Ujjain Smart City Limited

Request for Proposal for

Selection of System Integrator (SI) for

Establishment and O&M of Integrated Command & Control Centre (ICCC) for Simhastha Kumbh Mela 2028

Volume – 2: Detailed Scope of Work and Technical Specifications

NIT No. USCL/430

Tender ID: 2026_UAD_508730_1 **Ujjain Date: 20/05/2026**

……

Ujjain Smart City Limited
Simhastha Mela Office, Kothi Road,
Ujjain, Madhya Pradesh – 456010

Establishment and O&M of Integrated Command & Control Centre (ICCC) for Simhastha Kumbh Mela 2028

VOLUMES STRUCTURE OF RFP DOCUMENTS

Volume	Contents
Volume-I	Instructions to Bidders and Bid Process Management
Volume-II	Scope of Work & Technical Specifications
Volume-III	Draft Contract Agreement & SLA
Volume-IV	Financial Bid / BOQ

Volume – 2: Scope of Work & Technical Specifications

TABLE OF CONTENTS

Section 16	**Technical Specifications & Compliance Matrix**
Section 17	**Detailed Technical Specifications of Major Items**

SECTION 1: PROJECT BACKGROUND & OBJECTIVES

1. PROJECT BACKGROUND & OBJECTIVES

1.1 Background

Simhastha Kumbh Mela is one of the largest religious congregations in the world and is organized periodically at Ujjain on the banks of the holy river Shipra. Simhastha 2028 is scheduled to be held from 09 April 2028 to 08 May 2028 and is expected to witness an estimated cumulative footfall of approximately 30 crore pilgrims during the event period, including exceptionally high peak footfall during major Snan days.

The event shall involve extensive temporary and permanent infrastructure across approximately 3,000 hectares of Mela Area along with city-wide traffic, mobility, security, safety, emergency response, parking management, public information dissemination, and crowd management arrangements. The Mela Area includes ghats, roads, holding areas, parking areas, public congregation zones, temporary camps, transport corridors, and critical public infrastructure.

Considering the scale, complexity, and sensitivity of the event, Ujjain Smart City Limited (USCL), in coordination with Simhastha Mela Authority, District Administration, Police Department, and other stakeholder agencies, intends to establish an advanced Integrated Command & Control Centre (ICCC) ecosystem for integrated surveillance, crowd management, situational awareness, predictive monitoring, emergency coordination, and operational decision support.

The proposed ICCC ecosystem shall leverage advanced technologies including:

- AI-based video analytics,
- GIS-based operational dashboards,
- Digital Twin and simulation platform,
- integrated communication systems,
- radio/wireless communication systems,
- intelligent surveillance systems,
- traffic and parking analytics,
- drone surveillance,
- cybersecurity systems,
- and real-time field intelligence integration.

The project is envisaged as a hybrid infrastructure model comprising:

- Permanent city-level infrastructure assets for long-term smart governance and surveillance, and
- Temporary/rental infrastructure for event-specific surge deployment during Simhastha 2028.

The proposed system shall serve as a centralized operational platform for multi-agency coordination and management before, during, and after the event.

1.2 Project Vision

To establish a secure, scalable, intelligent, and integrated ICCC ecosystem for Simhastha 2028 that enables proactive crowd management, real-time situational awareness, efficient emergency response, and coordinated multi-agency operations through advanced digital technologies.

1.3 Project Objectives

The key objectives of the project are as follows:

1.3.1 Crowd Management & Public Safety

- Real-time monitoring and management of crowd movement across ghats, roads, holding areas, parking areas, and congregation zones.
- Detection of overcrowding, congestion, reverse flow, abnormal movement, and potential risk situations.
- Enabling predictive crowd management using AI and Digital Twin technologies.

1.3.2 Integrated Surveillance & Security

- Establishment of a comprehensive IP-based surveillance network across critical locations.
- Integration of CCTV, PTZ, panoramic, thermal, ANPR, drone, body-worn, underwater, and selected private CCTV feeds into a unified ICCC platform.
- Enhancement of law enforcement, monitoring, and incident response capabilities.

1.3.3 AI-Based Situational Awareness

- Deployment of AI-enabled video analytics for:
    - crowd density estimation,
    - heatmaps,
    - queue analysis,
    - people counting,
    - vehicle analytics,
    - fire and smoke detection,
    - intrusion detection,
    - and other operational intelligence functions.

1.3.4 Digital Twin & Predictive Decision Support

- Establishment of a GIS-enabled Digital Twin platform for:
    - real-time visualization,
    - crowd simulation,
    - congestion forecasting,
    - evacuation planning,
    - diversion planning,
    - and emergency scenario modelling.

1.3.5 Traffic & Parking Management

- Monitoring and management of traffic movement on major roads leading to Ujjain, city roads, Mela Area roads, parking areas, and holding zones.
- Integration of ANPR systems and parking analytics for operational efficiency.

1.3.6 Multi-Agency Coordination

- Enabling coordinated operations among:
    - District Administration,
    - Police,
    - Health Department,
    - SDRF/NDRF,
    - Fire Services,
    - Transport Agencies,
    - Municipal Authorities,
    - and other stakeholder agencies.

1.3.7 Emergency Response & Disaster Management

- Real-time incident monitoring and alerting.
- Integration of SOP-driven response workflows.
- Support for emergency evacuation, medical response, disaster management, and public communication.

1.3.8 Citizen Services & Information Dissemination

- Support for public information dissemination through Variable Message Displays (VMDs), public address systems, mobile applications, and other communication platforms.
- Facilitation of lost & found support and emergency communication systems.

1.3.9 Cybersecurity & Operational Resilience

- Establishment of a secure and resilient ICCC ecosystem with:
    - cybersecurity controls,
    - network security,
    - SOC/SIEM integration,
    - disaster recovery mechanisms,
    - and business continuity measures.

1.3.10 Long-Term Smart City Asset Creation

- Creation of scalable permanent infrastructure assets for continued use beyond Simhastha 2028 for:
    - city surveillance,

- public safety,
- traffic management,
- and future smart city initiatives.

1.4 Project Scope Overview

The scope of the project broadly includes:

- Survey, planning, design, engineering, supply, installation, integration, testing, commissioning, trial runs, training, operations and maintenance of ICCC infrastructure and associated systems.
- Deployment of hybrid permanent and rental infrastructure.
- Establishment of communication network backbone.
- AI analytics and Digital Twin implementation.
- ICCC setup and operations.
- Field infrastructure deployment.
- Integration with existing and third-party systems.
- Operations and maintenance for permanent and temporary infrastructure.

Detailed scope of work and technical requirements are specified in subsequent sections of this RFP.

1.5 Guiding Principles

The proposed solution architecture and implementation approach shall adhere to the following guiding principles:

- Scalability
- Interoperability
- Open standards
- High availability
- Cybersecurity by design
- Modular architecture
- Operational resilience
- Low latency and real-time responsiveness
- Multi-agency integration
- Future readiness and expandability

1.6 Implementation Approach

The project shall be implemented through a phased approach including:

- Detailed survey and design,
- procurement and deployment,

- integration and testing,
- trial runs and Go-Live,
- event-period operations,
- and long-term operations & maintenance.

The selected System Integrator (SI) shall be fully responsible for end-to-end implementation and operationalization of the complete ICCC ecosystem in accordance with the requirements of this RFP.

SECTION 2: SCOPE OF WORK

2. SCOPE OF WORK

2.1 Overview

Ujjain Smart City Limited (USCL) intends to appoint a System Integrator (SI) for design, engineering, supply, installation, integration, testing, commissioning, operations and maintenance of an Integrated Command & Control Centre (ICCC) ecosystem for Simhastha 2028, Ujjain.

The project shall include establishment of an integrated surveillance, crowd management, communication, analytics, Digital Twin, cybersecurity, and decision-support ecosystem through a hybrid deployment model comprising:

- Permanent infrastructure (CAPEX),
- Temporary/rental infrastructure for event-period surge deployment,
- and Operations & Maintenance (O&M).

The selected SI shall be responsible for complete end-to-end implementation and operationalization of all components under the project scope.

2.2 Broad Scope of Services

The scope of work shall broadly include, but not be limited to, the following:

1. Detailed site survey, planning, design and engineering
2. Supply, installation and commissioning of field devices and infrastructure
3. Establishment of ICCC and associated facilities
4. Deployment of surveillance and crowd management systems
5. Deployment of AI analytics and Digital Twin platform
6. Communication network establishment and integration
7. Cybersecurity implementation
8. Integration with existing and third-party systems
9. Testing, training, trial runs and Go-Live support
10. Operations and maintenance support
11. Documentation and knowledge transfer

2.3 Detailed Scope of Work

2.3.1 Survey, Planning & Detailed Design

The SI shall undertake detailed field survey, planning, engineering, and preparation of all required design documents including but not limited to:

a) Site Survey

- Physical survey of all proposed locations
- Route survey for OFC/network infrastructure

- Identification of installation points
- Power availability assessment
- Feasibility assessment for camera placement and coverage

b) Design & Engineering

- Preparation of detailed architecture and network design
- Camera placement plans
- GIS mapping
- Bandwidth sizing
- Storage sizing
- Power and UPS sizing
- Rack and infrastructure layouts
- ICCC design layouts
- Integration architecture

c) Documentation

- Detailed Project Implementation Plan
- Method Statements
- Deployment Strategy
- Risk Mitigation Plan
- Quality Assurance Plan
- Cybersecurity Plan
- Acceptance Testing Plan

The detailed design and implementation plan shall be submitted to USCL for approval prior to execution.

2.3.2 Supply, Installation & Commissioning of Surveillance Infrastructure

The SI shall supply, install, configure, integrate, test and commission all surveillance infrastructure including but not limited to:

a) Camera Systems

- Fixed IP Cameras
- PTZ Cameras
- Panoramic / 360° Cameras
- Thermal Cameras
- ANPR Cameras
- Underwater Cameras

- Boat-mounted Cameras
- Body-Worn Cameras
- Dash Cameras

b) Deployment Areas

- Major roads leading to Ujjain
- City roads and intersections
- Mela Area roads and sectors
- Ghats and congregation areas
- Entry/exit points
- Parking areas
- Holding areas
- Critical public infrastructure
- Emergency corridors
- Transport hubs

c) Private CCTV Integration

The SI shall provide secure integration capability for selected private/institutional CCTV feeds into ICCC.

2.3.3 ICCC Establishment

The SI shall establish and operationalize the ICCC ecosystem including:

a) Main ICCC

- Video wall
- Operator consoles
- Workstations
- AV systems
- Display systems
- Control room furniture
- Incident management systems

b) Secondary / Backup ICCC

- Integration with existing Smart City ICCC infrastructure, wherever applicable

c) War Room

- Temporary/rental war room setup during event period

d) Viewing Centres

- Remote viewing centres at designated locations

2.3.4 AI-Based Video Analytics Platform

The SI shall deploy and operationalize an AI-enabled analytics platform integrated with surveillance systems.

The analytics platform shall support:

- Crowd density analytics
- Heatmap generation
- Queue analytics
- Reverse flow detection
- People counting
- Intrusion detection
- Fire and smoke detection
- Vehicle analytics
- Parking analytics
- Incident analytics
- Configurable AI-based alerts

The AI platform shall support centralized management, real-time alerting, auditability, and scalability.

2.3.5 Digital Twin & Decision Intelligence Platform

The SI shall establish a GIS-enabled Digital Twin platform integrated with ICCC systems.

The platform shall include:

- Real-time GIS visualization
- Crowd simulation
- Congestion forecasting
- Traffic simulation
- Evacuation modelling
- Scenario planning
- Predictive analytics
- SOP-driven decision support
- Event correlation and situational awareness

The platform shall ingest data from:

- CCTV systems
- AI analytics
- GPS systems
- IoT devices

- ANPR systems
- Mobile applications
- Traffic systems
- Public information systems
- Other integrated platforms

2.3.6 Communication Network Infrastructure

The SI shall design, establish, integrate and maintain the communication network infrastructure including:

a) OFC Backbone

- OFC laying
- HDPE ducting
- Splicing
- Termination
- Redundant ring architecture

b) Active Network Components

- Core switches
- Aggregation switches
- Edge switches
- Routers
- Wi-Fi infrastructure
- RF/microwave links

c) Network Requirements

- High availability
- Low latency
- Scalability
- QoS for video traffic
- Secure architecture

The network shall support all surveillance and ICCC operations.

2.3.7 Field Infrastructure

The SI shall provide complete field-level infrastructure including:

- Poles and mounting structures
- Junction boxes
- UPS systems

- Power cabling
- Electrical infrastructure
- Earthing
- Lightning protection
- Outdoor enclosures
- Civil works
- Foundation works

2.3.8 Data Center, Storage & Disaster Recovery

The SI shall provide and operationalize:

- Centralized storage systems
- Backup systems
- Compute infrastructure
- Virtualization infrastructure
- Disaster Recovery integration
- Redundancy and failover systems

The architecture shall support:

- minimum 60 days video retention,
- extendable to 90 days for critical feeds.

2.3.9 Video Management System (VMS)

The SI shall deploy an enterprise-grade centralized Video Management System (VMS) supporting:

- Multi-camera monitoring
- Live view
- Playback
- Incident tagging
- Video archival
- Forensic search
- AI integration
- GIS integration
- Role-based access control
- Multi-site support

2.3.10 Cybersecurity Implementation

The SI shall implement comprehensive cybersecurity measures including:

- Firewall systems
- IDS/IPS
- SIEM integration
- SOC support
- Secure authentication
- Device hardening
- Encryption
- Secure remote access
- Security monitoring
- VAPT support
- CERT-In compliance

2.3.11 Limited Enterprise Event Communication System (Radio/Wireless Communication)

The SI shall provide and/or integrate enterprise-grade field communication systems including wireless handheld communication devices, command dispatch consoles, and associated communication infrastructure required for coordinated field operations, emergency response, crowd management, parking operations, and multi-agency event management during Simhastha 2028.

2.3.12 Public Communication & Citizen Interface Systems

The SI shall integrate and operationalize:

- Variable Message Displays (VMDs)
- Public Address Systems
- Citizen information systems
- Emergency alert systems
- Lost & Found integration
- Mobile application interfaces

2.3.13 Drone Surveillance Integration

The SI shall deploy and integrate drone surveillance systems for:

- aerial monitoring,
- crowd assessment,
- emergency response support,
- and situational awareness.

Drone feeds shall be integrated into ICCC dashboards and GIS systems.

2.3.14 Integration with Existing and Third-Party Systems

The SI shall provide seamless integration with:

- existing ICCC systems,
- city surveillance systems,
- ATCS systems,
- GIS systems,
- emergency systems,
- mobile applications,
- police systems,
- and approved third-party platforms.

The system shall support open APIs and interoperable architecture.

2.3.15 Testing, Trial Runs & Acceptance

The SI shall conduct:

- Factory Acceptance Test (FAT)
- Site Acceptance Test (SAT)
- User Acceptance Test (UAT)
- Integrated system testing
- Peak-load simulation testing
- Failover testing
- Cybersecurity testing
- Trial runs prior to Go-Live

2.3.16 Training & Capacity Building

The SI shall provide comprehensive training to:

- ICCC operators
- administrators
- technical teams
- police personnel
- field personnel
- and authorized stakeholders.

Training shall include:

- system operations,
- incident handling,
- troubleshooting,
- cybersecurity awareness,

- and reporting.

2.3.17 Operations & Maintenance (O&M)

The SI shall provide comprehensive O&M support for all project components including:

- preventive maintenance,
- corrective maintenance,
- software support,
- upgrades,
- spare management,
- helpdesk support,
- field support,
- and ICCC operational support.

The SI shall ensure compliance with prescribed SLAs throughout the contract period.

2.3.17.1 Utility Power Supply & Electricity Charges

The System Integrator (SI) shall be responsible for obtaining/coordinating temporary and permanent electricity connections, wherever required, for operation of ICCC infrastructure, field devices, surveillance systems, communication equipment, control rooms, war rooms, viewing centres, and associated project infrastructure during the contract period.

The SI shall initially pay all electricity consumption charges, meter charges, demand charges, temporary connection charges, and other recurring electricity-related operational expenses to the concerned utility authorities/agencies to ensure uninterrupted operations.

Such actual recurring electricity charges paid by the SI shall be reimbursed by USCL on a monthly basis, subject to:

- submission of original bills/invoices/receipts,
- certification by the Authorized Representative of USCL,
- submission of consumption details and supporting documents,
- and verification of actual deployment and operational status.

No additional administrative charges, overheads, penalties arising due to delayed payment by the SI, or interest liabilities shall be payable by USCL.

2.3.18 Documentation & Knowledge Transfer

The SI shall provide:

- As-built drawings
- Asset inventory
- Network diagrams
- Configuration documents

- User manuals
- SOP documents
- Training manuals
- O&M manuals
- Cybersecurity documentation
- Backup and recovery procedures

All project-related intellectual property, documentation, configurations, and records shall be handed over to USCL upon completion or termination of the contract.

2.4 Responsibility of the SI

The SI shall be solely responsible for:

- End-to-end execution,
- system integration,
- interoperability,
- performance compliance,
- SLA adherence,
- coordination with OEMs,
- statutory compliances,
- safety compliance,
- and timely completion of the project.

2.5 Exclusions

Unless explicitly specified otherwise, the following shall generally remain outside the scope of the SI:

- Land acquisition
- Permanent utility shifting by external agencies
- External statutory approvals from third-party authorities
- Existing civil structures not directly related to the project

However, the SI shall assist USCL in coordination and technical support related to such activities wherever required.

2.6 General Requirements

The proposed solution shall:

- Support open standards and interoperability
- Avoid vendor lock-in
- Be scalable up to minimum 30% additional load
- Support multi-agency operations

- Be resilient and fault-tolerant
- Be compliant with applicable Government guidelines and standards
- Support future expansion and integration requirements

SECTION 3: ICCC ARCHITECTURE

3. ICCC Architecture

The ICCC will follow a **six-layer enterprise architecture**.

3.1 Overall Architectural Philosophy

The ICCC architecture shall be designed as a multi-layered Predictive Command Platform comprising data acquisition, AI analytics, Digital Twin simulation, and decision support layers enabling proactive crowd management and real-time operational control.

The System Integrator shall have demonstrable capability in implementing AI-driven analytics platforms and Digital Twin or simulation-based systems, either directly or through OEM partnerships.

The proposed ICCC architecture integrates permanent city infrastructure with temporary event-specific systems through a unified platform. It is built to ensure:

- Real-time Situational Awareness: Immediate visibility across all mela and city zones.
- Predictive Analytics: Using data to forecast crowd density and traffic congestion.
- High Availability: A dual-site configuration (Primary DC + Disaster Recovery) for continuous operations.
- Inter-agency Coordination: A central hub for Police, Health, Revenue, and Municipal departments.

3.2 The Six-Layer Architecture

The ICCC system is structured into six functional layers, progressing from field-level data acquisition to centralized command, predictive analytics, and decision-making. Each layer has a distinct role to ensure clarity, scalability, and seamless integration.

3.2.1 Layer 1: Field Data Acquisition Layer

This layer comprises the physical “eyes and ears” deployed across Ujjain city and the Simhastha Mela area.

Components include:

- The field layer shall include scalable deployment of surveillance systems across mela area, city roads, and parking/holding zones based on risk and coverage requirements.
- Surveillance Systems: Fixed, PTZ, thermal, panoramic (360°), Facial Recognition (FRS), drone-based, underwater cameras, and body-worn cameras
- Mobility Systems: ANPR cameras, adaptive traffic signals, parking sensors
- Public Safety Systems: Emergency call boxes, Public Address Systems (PAS), Variable Message Displays (VMDs)
- Environmental Sensors: AQI, weather, and water quality monitoring systems
- Optional LiDAR-based sensors may be deployed at select critical locations for high-accuracy pedestrian and traffic movement detection, particularly in high-density or low-visibility conditions.

- The system shall support integration of CCTV feeds from selected private and institutional premises (e.g., temples, hotels, commercial establishments) subject to consent and technical feasibility.

3.2.2 Layer 2: Edge Processing & Connectivity Layer

This layer ensures real-time data transmission and preliminary processing with minimal latency.

Key components:

- Network Backbone: OFC-based high-speed network supplemented with RF/microwave links and outdoor Wi-Fi
- Private CCTV feeds shall be onboarded through secure connectivity mechanisms (VPN/secure RTSP/edge gateways) ensuring network isolation and bandwidth optimization.
- Edge Processing: AI-enabled cameras and edge devices for:
    - Preliminary crowd density estimation
    - Event filtering and compression
    - Reduced load on central systems

3.2.3 Layer 3: Integration & Data Management Layer

This layer acts as the central data exchange and storage backbone.

Components:

- Integration Middleware:
    - Enterprise Service Bus (ESB)
    - API Gateway
    - Message queues (Kafka / RabbitMQ)
    - The integration layer shall support ingestion of LiDAR point-cloud or processed data streams through standard APIs for unified processing alongside video analytics.
    - The system shall support ingestion of external data sources, including publicly available social media feeds, through secure APIs. Only publicly available data shall be used, in compliance with applicable legal and privacy frameworks.
    - The platform shall support standardized onboarding, authentication, and management of third-party CCTV feeds through APIs and secure device registration mechanisms
- Enterprise Data Lake:
    - Storage of structured and unstructured data
    - Includes video metadata, density maps, incidents, traffic data, SOS alerts
    - Technologies: Distributed storage (Hadoop), Spark/Flink processing

Function:

- Standardizes data formats
- Enables real-time data ingestion and historical data storage

- Serves as input for analytics and simulation

3.2.4 Layer 4: AI Analytics & Digital Twin Layer

This is the core intelligence layer of the ICCC system. AI analytics in the proposed system shall be based on pre-trained models calibrated to local conditions and continuously refined using real-time data, achieving high accuracy for crowd monitoring and predictive decision support during the event.

Key functionalities:

AI Analytics:

- Real-time crowd density estimation
- Heatmaps and hotspot detection
- Reverse flow and anomaly detection
- Traffic analytics and incident detection

Digital Twin & Simulation:

- Real-time virtual representation of the Mela area
- Simulation of crowd movement and flow
- Prediction of congestion (15–30 minutes in advance)
- Scenario modelling:
    - Route diversion
    - Emergency evacuation
- Ghat load monitoring and balancing
- Where deployed, LiDAR data shall be used to enhance and validate AI-based crowd analytics and improve accuracy of Digital Twin simulations in high-density zones.
- Where integrated, private CCTV feeds may be utilized for supplementary analytics and Digital Twin inputs to enhance situational awareness in identified zones.

3.2.5 Layer 5: Decision Support & Application Layer

This layer converts analytics into actionable decisions and operational control.

Components:

- Decision Support System (DSS):
    - Generates automated alerts
    - Recommends actions (diversion, restriction, routing)
    - Maps alerts to predefined SOPs
- Application Platforms:
    - GIS-based dashboards
    - Video Management System (VMS)
    - Traffic Management System (ITMS)

- Emergency response modules
- Lost & Found system

Function:

- Enables predictive and prescriptive decision-making
- Supports multi-agency coordination

Inputs from

- social media monitoring may be used as supplementary inputs for alert generation and situational awareness.
- third-party CCTV feeds may be used for alert generation and decision support, subject to data quality and reliability.

3.2.6 Layer 6: Command & Control Layer (ICCC)

This is the operational nerve centre for monitoring, coordination, and response.

Key facilities:

- Primary ICCC (Mela Office):
  - 9,000–10,000 sq. ft. command centre
  - Large video wall
  - 40+ operator workstations
  - 50-seat War Room
- Secondary ICCC (USCL / Police):
  - Backup and redundancy
  - City-wide integration
- Local War Room (Ranoji ki Chhatri):
  - 20-seat temporary command centre (event period)
  - Zone-level coordination and rapid response
- Remote Viewing Centres (10 Nos):
  - Collectorate, Police HQ, Bhopal State Command, enroute districts
- Authorized private CCTV feeds shall be viewable within ICCC with appropriate tagging, prioritization, and access control.

Function:

- Real-time monitoring
- Decision execution
- Inter-agency coordination

3.3 CROSS-CUTTING LAYERS (APPLICABLE TO ALL)

Cybersecurity Framework

- Next-generation firewalls
- IDS/IPS systems
- Data encryption
- SIEM monitoring
- Compliance with CERT-In guidelines

Operational Governance

- Standard Operating Procedures (SOPs)
- Incident Response System (IRS)-based command
- Multi-agency coordination (Police, Health, SDRF, Municipal)

Citizen Interface: "Simhastha Saarathi"

A unified mobile application providing:

- Navigation & Parking: Real-time routing and availability
- Safety: Crowd heatmaps, alerts, SOS
- Recovery: Lost & Found integrated with FRS

3.4 Architecture Flow

This architecture ensures that after Simhastha 2028, these infrastructure will remain as a permanent, scalable command platform for Ujjain's future smart city operations.

Architecture Flow

Field Layer
↓
Network & Edge Layer
↓
Data Lake &
Integration Layer
↓
AI Analytics &
Digital Twin Layer
↓
Decision Support System &
& Application Layer
↓
ICCC Command Layer
↓
Field Execution

Advanced sensing technologies such as LiDAR shall remain optional enhancements and shall be integrated within the existing data and analytics framework without altering the core system architecture.

SECTION 4: SURVEILLANCE & CROWD MANAGEMENT SYSTEM

4. SURVEILLANCE & CROWD MANAGEMENT SYSTEM

4.1 Overview

The System Integrator (SI) shall design, supply, install, integrate, test, commission, operate and maintain a comprehensive AI-enabled Surveillance & Crowd Management System for Simhastha 2028.

The system shall provide real-time situational awareness, crowd monitoring, traffic monitoring, incident detection, operational intelligence, and emergency response support across:

- Mela Area,
- Ghats,
- Major roads leading to Ujjain,
- City roads and intersections,
- Parking areas,
- Holding areas,
- Public congregation zones,
- Emergency corridors,
- Critical infrastructure locations,
- and other identified strategic locations.

The surveillance system shall operate as an integrated component of the ICCC ecosystem and shall support interoperability with AI analytics, Digital Twin, GIS, VMS, emergency response systems, and other integrated platforms.

The overall surveillance architecture shall support:

- centralized monitoring,
- distributed operations,
- edge intelligence,
- predictive analytics,
- scalability,
- and high availability.

4.2 Camera Systems

4.2.1 General Requirements

The SI shall provide enterprise-grade IP-based surveillance systems compliant with open standards and suitable for continuous outdoor operations under varying environmental conditions.

The camera ecosystem shall include:

- Fixed/Bullet/Box Cameras,

- PTZ Cameras,
- Panoramic Cameras,
- Thermal Cameras,
- Specialized Cameras,
- Edge AI-enabled Cameras,
- and associated accessories.

The proposed surveillance system shall:

- support ONVIF compliance,
- support centralized VMS integration,
- support AI analytics integration,
- support GIS integration,
- support secure communication protocols,
- and support centralized health monitoring.

The system shall be designed for approximately 2,600–2,800 cameras initially and scalable up to minimum 4,000 cameras without major redesign.

4.2.2 Coverage Requirements

The surveillance deployment shall cover, but not be limited to, the following categories of locations:

a) Regional Approach Corridors

- Highways and major roads leading to Ujjain

b) City Surveillance

- Major roads,
- intersections,
- traffic junctions,
- transport hubs

c) Mela Area

- Ghats,
- Akhadas,
- congregation areas,
- internal circulation routes,
- sector roads,
- temporary camps

d) Parking & Holding Areas

- Satellite parking zones,

- holding areas,
- peripheral parking

e) Critical Infrastructure

- Bridges,
- emergency routes,
- temporary structures,
- control points,
- public utility areas

4.2.3 Fixed / Bullet / Box Cameras

The SI shall deploy fixed surveillance cameras for continuous monitoring of designated areas.

Minimum Functional Requirements:

- Minimum 5 MP resolution
- H.265/H.265+ compression
- IR illumination
- WDR support
- Low-light performance
- Motion detection
- Tamper detection
- Day/Night operation
- IP66/IP67 outdoor rating
- IK10 vandal resistance

Deployment Areas:

- Roads
- Corridors
- Parking zones
- Internal routes
- Entry/exit areas
- Public congregation areas

4.2.4 PTZ Cameras

The SI shall deploy PTZ cameras at strategic locations requiring dynamic surveillance and wide-area monitoring.

Minimum Functional Requirements:

- Minimum 25x optical zoom

- 360° continuous rotation
- Auto-tracking capability
- Preset tours
- Patrol functionality
- Intelligent tracking
- Low-light operation
- IR support

Deployment Areas:

- Ghats
- Major junctions
- Entry/exit points
- Critical public locations
- Large congregation zones

4.2.5 Panoramic / 360° Cameras

The SI shall deploy panoramic cameras at high-density crowd locations.

Minimum Functional Requirements:

- 180° or 360° coverage
- Multi-sensor stitching
- De-warping functionality
- Simultaneous multi-view support
- Crowd density support

Deployment Areas:

- Major ghats
- Public congregation areas
- Choke points
- Queue areas

4.2.6 Thermal Cameras

The SI shall deploy thermal cameras at critical locations requiring low-visibility monitoring.

Minimum Functional Requirements:

- Thermal + optical dual sensor preferred
- Fire/smoke detection support
- Night operation capability

- Long-range monitoring
- Perimeter monitoring support

Deployment Areas:

- River banks
- Critical infrastructure
- Perimeter zones
- Emergency corridors

4.2.7 Edge AI Enabled Cameras

Selected cameras shall support edge analytics capability including:

- people counting,
- intrusion detection,
- queue analytics,
- object detection,
- and event triggering.

Edge analytics shall reduce bandwidth consumption and support real-time local event processing.

4.2.8 Camera Deployment Philosophy

The surveillance system shall follow a:

- risk-based,
- density-driven,
- and zone-based deployment strategy.

Higher camera density shall be deployed in:

- ghats,
- high-footfall areas,
- entry/exit corridors,
- and critical congregation zones.

The final deployment plan shall be approved by USCL after detailed survey and simulation assessment.

4.2.9 Video Retention

The system shall support:

- minimum 60 days video retention,
- extendable up to 90 days for critical feeds.

The architecture shall support centralized and edge recording mechanisms.

4.2.10 Camera Health Monitoring

The SI shall provide centralized monitoring for:

- camera health,
- storage status,
- connectivity,
- power status,
- recording status,
- and fault alerts.

4.3 Automatic Number Plate Recognition (ANPR)

4.3.1 Scope

The SI shall deploy and integrate ANPR systems for vehicle monitoring, traffic analytics, and operational intelligence.

4.3.2 Functional Requirements

The ANPR system shall support:

- automatic vehicle number recognition,
- vehicle classification,
- blacklist/whitelist matching,
- speed analytics,
- route tracking,
- and vehicle movement analytics.

4.3.3 Deployment Areas

ANPR systems shall be deployed at:

- city entry points,
- highways,
- parking areas,
- holding areas,
- major intersections,
- and critical traffic corridors.

4.3.4 Performance Requirements

The system shall support:

- minimum 95% recognition accuracy during daytime,
- minimum 90% accuracy during night conditions,
- multi-lane support,
- and real-time alerting.

4.3.5 Integration

The ANPR system shall integrate with:

- VMS,
- ICCC dashboards,
- AI analytics,
- traffic management systems,
- and GIS platform.

4.4 Body Cameras and Dash Cameras

4.4.1 Scope

The SI shall deploy body-worn cameras and vehicle-mounted dash cameras for field operations, law enforcement support, and incident recording.

4.4.2 Body-Worn Cameras

Functional Requirements:

- Full HD recording
- GPS tagging
- Audio recording
- Night vision support
- Docking station support
- Secure upload capability
- Tamper resistance

Usage Areas:

- Police personnel
- Field enforcement teams
- Emergency response teams
- Crowd management teams

4.4.3 Dash Cameras

Functional Requirements:

- Continuous recording
- GPS support
- Low-light support
- Secure storage
- Real-time upload capability preferred

Deployment Areas:

- Police vehicles
- Emergency vehicles
- Patrol vehicles
- Field operation vehicles

4.4.4 Integration

Body-worn and dash camera systems shall integrate with:

- ICCC,
- VMS,
- evidence management systems,
- and authorized playback systems.

4.5 Drone Integration

4.5.1 Scope

The SI shall deploy and integrate drone surveillance systems for aerial situational awareness and dynamic surveillance.

4.5.2 Functional Requirements

The drone system shall support:

- live video streaming,
- aerial monitoring,
- crowd assessment,
- emergency response support,
- route assessment,
- and situational visualization.

4.5.3 Drone Requirements

Minimum Requirements:

- Flight time ≥ 30 minutes
- HD/4K camera
- Stabilized gimbal
- Real-time streaming
- GPS support
- Night operation support preferred

4.5.4 Integration

Drone feeds shall integrate with:

- ICCC,

- GIS platform,
- Digital Twin,
- and VMS.

4.5.5 Regulatory Compliance

The SI shall ensure compliance with:

- DGCA regulations,
- aviation guidelines,
- no-fly zone restrictions,
- and other statutory requirements.

4.6 Water Surveillance

4.6.1 Scope

The SI shall provide integrated river and water surveillance systems for monitoring activities at ghats and river stretches.

4.6.2 Components

The water surveillance system may include:

- underwater cameras,
- boat-mounted cameras,
- thermal surveillance,
- floating surveillance systems,
- and associated communication infrastructure.

4.6.3 Deployment

Approximately 35–45 underwater and boat-mounted surveillance cameras shall be deployed in hybrid mode (permanent and rental) focusing on:

- high-risk ghats,
- major bathing locations,
- and critical river stretches.

4.6.4 Functional Requirements

The system shall support:

- real-time river monitoring,
- crowd monitoring near water zones,
- emergency response support,
- low-light monitoring,
- and integration with rescue operations.

4.6.5 Integration

The water surveillance system shall integrate with:

- ICCC,
- GIS platform,
- VMS,
- AI analytics,
- and emergency response systems.

4.7 Private CCTV Integration

4.7.1 Scope

The surveillance architecture shall support integration of selected private/institutional CCTV feeds for enhanced situational awareness.

4.7.2 Eligible Sources

Feeds may be integrated from

- temples,
- hotels,
- dharamshalas,
- commercial establishments,
- educational institutions,
- hospitals,
- and other identified locations.

4.7.3 Integration Requirements

The integration framework shall support:

- secure API/VPN-based integration,
- role-based access control,
- tagging and categorization,
- audit logging,
- and selective feed onboarding.

4.7.4 Security & Privacy

Private CCTV integration shall be:

- consent-based,
- secure,
- access-controlled,
- and compliant with applicable cybersecurity and privacy requirements.

4.7.5 Scalability

The system shall support integration of minimum 600–800 external CCTV feeds without major redesign.

SECTION 5: VIDEO MANAGEMENT SYSTEM (VMS)

5. VIDEO MANAGEMENT SYSTEM (VMS)

5.1 Overview

The System Integrator (SI) shall design, supply, install, configure, integrate, test, commission, operate and maintain an enterprise-grade centralized Video Management System (VMS) for Simhastha 2028.

The VMS shall function as the centralized video monitoring, recording, management, playback, event handling, and operational intelligence platform for the ICCC ecosystem.

The VMS shall support integration with:

- CCTV systems,
- AI analytics engines,
- Digital Twin platform,
- GIS systems,
- ANPR systems,
- Drone surveillance,
- Body-worn cameras,
- Dash cameras,
- Water surveillance systems,
- Public communication systems,
- and other integrated platforms.

The proposed VMS shall support centralized and distributed operations with high availability, scalability, and interoperability.

5.2 General Requirements

5.2.1 Architecture

The proposed VMS shall:

- be enterprise-grade and scalable,
- support centralized and distributed deployment,
- support multi-site architecture,
- support edge and centralized recording,
- support failover architecture,
- support redundant operation,
- and support open standards and interoperability.

The VMS shall not be based on standalone DVR/NVR-centric architecture and shall support centralized enterprise video management.

5.2.2 Open Standards & Interoperability

The VMS shall:

- support ONVIF compliance,
- support integration with multi-OEM cameras,
- support standard APIs,
- support third-party integrations,
- and avoid vendor lock-in.

The VMS shall support integration with:

- existing surveillance systems,
- future surveillance systems,
- and approved third-party platforms.

5.2.3 Scalability

The proposed VMS shall:

- initially support approximately 2,600–2,800 cameras,
- be scalable up to minimum 4,000 cameras,
- support future expansion without major redesign,
- and support additional recording and analytics load.

5.3 Functional Requirements

5.3.1 Live Monitoring

The VMS shall support:

- real-time live video monitoring,
- simultaneous multi-camera viewing,
- customizable layouts,
- dynamic camera grouping,
- operator-based view configuration,
- and multi-monitor support.

The system shall support viewing of:

- live feeds,
- recorded feeds,
- AI alerts,
- and GIS-linked video streams.

5.3.2 Recording Management

The VMS shall support:

- continuous recording,
- scheduled recording,
- event-triggered recording,
- edge recording,
- centralized recording,
- failover recording,
- and recording synchronization.

The system shall support:

- minimum 60 days retention,
- extendable to 90 days for critical feeds.

5.3.3 Playback & Forensic Investigation

The VMS shall support:

- synchronized playback,
- timeline-based playback,
- forensic search,
- event search,
- bookmark tagging,
- smart playback,
- frame-by-frame analysis,
- and evidence export.

The system shall support investigation workflows for authorized users.

5.3.4 Event & Alarm Management

The VMS shall support:

- real-time alarm handling,
- event prioritization,
- event acknowledgement,
- event escalation,
- incident tagging,
- and configurable alarm workflows.

The VMS shall support alarms generated from:

- AI analytics,

- ANPR systems,
- intrusion detection,
- motion events,
- camera tampering,
- storage failures,
- network failures,
- and other integrated systems.

5.3.5 Camera Management

The VMS shall support:

- centralized camera provisioning,
- remote camera configuration,
- firmware management,
- health monitoring,
- camera grouping,
- camera maps,
- and user-based camera access.

5.3.6 User & Role Management

The VMS shall support:

- Role-Based Access Control (RBAC),
- user authentication,
- granular permissions,
- operator-level access,
- multi-level authorization,
- audit trails,
- and activity logging.

5.3.7 GIS Integration

The VMS shall support integration with:

- GIS platform,
- Digital Twin platform,
- geospatial dashboards,
- and location-based camera visualization.

Operators shall be able to:

- view camera locations on maps,
- trigger camera feeds from GIS interface,
- and correlate incidents geographically.

5.3.8 AI Analytics Integration

The VMS shall support integration with AI/video analytics systems including:

- crowd density analytics,
- heatmaps,
- people counting,
- reverse flow detection,
- intrusion analytics,
- fire/smoke analytics,
- queue analytics,
- traffic analytics,
- and incident detection systems.

AI-generated alerts shall be:

- auditable,
- operator-verifiable,
- and configurable.

5.3.9 ANPR Integration

The VMS shall support:

- ANPR event visualization,
- vehicle search,
- vehicle tracking,
- blacklist/whitelist alerts,
- and integration with traffic dashboards.

5.3.10 Drone & Mobility Integration

The VMS shall support integration of:

- drone feeds,
- body-worn camera feeds,
- dash camera feeds,
- and mobile surveillance systems.

5.3.11 Incident Management

The VMS shall support:

- incident creation,
- incident tracking,
- event correlation,
- incident escalation,
- and incident closure workflows.

The system shall support incident linkage with:

- GIS,
- AI analytics,
- Digital Twin,
- and emergency response systems.

5.4 Technical Requirements

5.4.1 Compression & Streaming

The VMS shall support:

- H.264,
- H.265,
- adaptive streaming,
- multicast/unicast streaming,
- and bandwidth optimization.

5.4.2 Performance

The VMS shall support:

- low-latency operations,
- simultaneous multi-user access,
- large-scale video ingestion,
- and high-volume event handling.

Critical alerts shall be processed within acceptable operational timelines.

5.4.3 Redundancy & High Availability

The VMS architecture shall support:

- server redundancy,
- failover clustering,
- database redundancy,
- storage redundancy,

- and uninterrupted operations.

The system shall support automatic failover mechanisms.

5.4.4 Edge Recording Support

The VMS shall support:

- edge recording on cameras,
- recording synchronization,
- automatic recovery after connectivity restoration,
- and centralized archival.

5.4.5 Time Synchronization

The system shall support centralized time synchronization through:

- NTP,
- GPS synchronization,
- or equivalent mechanisms.

5.5 Video Storage & Archival

5.5.1 Storage Architecture

The VMS shall support:

- centralized storage,
- distributed storage,
- edge storage,
- RAID configuration,
- archival management,
- and storage scalability.

5.5.2 Retention Policy

The VMS shall support:

- minimum 60 days retention,
- extendable to 90 days for critical feeds,
- policy-based retention,
- and selective archival.

5.5.3 Evidence Export

The system shall support:

- encrypted export,
- watermarking,

- chain-of-custody support,
- and tamper-evident evidence handling.

5.6 Health Monitoring & Diagnostics

The VMS shall provide centralized monitoring of:

- camera status,
- recording status,
- storage health,
- network connectivity,
- server health,
- and application health.

Automated alerts shall be generated for:

- device failures,
- storage failures,
- camera tampering,
- recording failures,
- and connectivity loss.

5.7 Cybersecurity Requirements

The VMS shall support:

- secure authentication,
- password policies,
- encryption,
- secure communication,
- audit logs,
- session management,
- and cybersecurity hardening.

The system shall comply with:

- CERT-In guidelines,
- applicable Government cybersecurity requirements,
- and industry best practices.

5.8 Reporting & Analytics

The VMS shall support:

- operational reports,

- alarm reports,
- incident reports,
- audit reports,
- user activity reports,
- and customizable dashboards.

Reports shall support export in standard formats including:

- PDF,
- CSV,
- XLSX.

5.9 Mobile & Remote Access

The VMS shall support:

- secure web access,
- mobile/tablet access,
- remote monitoring,
- and secure remote administration.

Remote access shall be role-based and securely authenticated.

5.10 Integration Requirements

The VMS shall support seamless integration with:

- ICCC systems,
- AI platforms,
- Digital Twin platform,
- GIS systems,
- ANPR systems,
- drone systems,
- public communication systems,
- emergency systems,
- and other approved third-party systems.

The system shall support:

- REST APIs,
- SDK support,
- and standard integration interfaces.

5.11 Testing & Acceptance

The SI shall demonstrate:

- live monitoring,
- recording functionality,
- playback functionality,
- failover operations,
- analytics integration,
- GIS integration,
- and alert handling

during:

- FAT,
- SAT,
- UAT,
- and trial run stages.

5.12 OEM & Support Requirements

The proposed VMS solution shall:

- be OEM-backed,
- have proven enterprise deployments,
- support long-term updates,
- and provide technical support for the contract period.

OEM authorization and support commitment shall be mandatory.

5.13 SLA Requirements

The VMS shall support:

- minimum 99.5% uptime during event period,
- defined incident response timelines,
- fault monitoring,
- and performance tracking.

Peak snan days shall be treated as critical operational periods requiring enhanced SLA compliance.

5.14 Future Readiness

The proposed VMS architecture shall:

- support future expansion,
- support additional analytics modules,
- support additional camera onboarding,

- support integration with future city systems,
- and support evolving smart city requirements without major redesign.

SECTION 6: AI ANALYTICS PLATFORM

6. AI ANALYTICS PLATFORM

6.1 Overview

The System Integrator (SI) shall design, supply, install, configure, integrate, test, commission, operate and maintain an enterprise-grade AI Analytics Platform for Simhastha 2028.

The AI Analytics Platform shall function as the intelligent operational analytics layer of the ICCC ecosystem and shall provide real-time situational awareness, crowd intelligence, traffic intelligence, predictive analytics, event detection, operational alerts, and decision support.

The platform shall process and analyze data from:

- CCTV systems,
- PTZ cameras,
- panoramic cameras,
- thermal cameras,
- ANPR systems,
- drone feeds,
- body-worn cameras,
- dash cameras,
- water surveillance systems,
- IoT devices,
- GIS systems,
- and other integrated platforms.

The AI platform shall support:

- real-time analytics,
- centralized event management,
- predictive intelligence,
- GIS correlation,
- Digital Twin integration,
- and automated operational workflows.

6.2 Objectives

The objectives of the AI Analytics Platform include:

- proactive crowd management,
- congestion prediction,
- incident detection,

- operational intelligence generation,
- automated alerting,
- enhanced situational awareness,
- traffic and parking analytics,
- emergency response support,
- and data-driven operational decision making.

6.3 General Requirements

6.3.1 Architecture

The proposed AI Analytics Platform shall be enterprise-grade, modular, scalable, API-driven, and support distributed processing architecture.

The platform shall support centralized analytics, edge analytics, hybrid processing, GPU-enabled processing, and high availability architecture.

6.3.2 Open Standards & Interoperability

The AI platform shall support integration with multi-OEM systems, support ONVIF-compliant video systems, support REST APIs, support SDK integration, and avoid vendor lock-in.

The platform shall support integration with:

- VMS,
- Digital Twin platform,
- GIS systems,
- ANPR systems,
- traffic systems,
- emergency systems,
- and approved third-party applications.

6.3.3 Scalability

The platform shall:

- initially support analytics processing for approximately 2,800–3,000 cameras,
- support future scaling up to minimum 4,000 cameras,
- support additional analytics modules,
- and support future onboarding of additional data sources without major redesign.

6.4 Core Functional Modules

6.4.1 Crowd Density Analytics

The AI platform shall support:

- real-time crowd density estimation,

- density threshold monitoring,
- dynamic crowd heatmaps,
- crowd intensity classification,
- and high-density alert generation.

The system shall support:

- configurable density thresholds,
- GIS-linked visualization,
- and automated operational alerts.

6.4.2 Crowd Flow Analytics

The platform shall support:

- crowd movement tracking,
- directional flow analysis,
- pedestrian flow monitoring,
- abnormal movement detection,
- and crowd flow visualization.

6.4.3 Reverse Flow Detection

The system shall support:

- reverse crowd movement detection,
- abnormal directional flow alerts,
- and configurable operational thresholds.

The analytics engine shall generate real-time alerts for:

- counter-direction movement,
- congestion buildup,
- and abnormal crowd behaviour.

6.4.4 Queue Analytics

The AI platform shall support:

- queue detection,
- queue length estimation,
- waiting time estimation,
- queue overflow alerts,
- and queue trend analysis.

6.4.5 People Counting

The system shall support:

- real-time people counting,
- zone-wise occupancy monitoring,
- entry/exit counting,
- and crowd accumulation analytics.

6.4.6 Heatmap Generation

The platform shall support:

- dynamic heatmaps,
- temporal heatmaps,
- movement heatmaps,
- and GIS-based visualization.

Heatmaps shall support:

- crowd monitoring,
- traffic monitoring,
- and incident hotspot identification.

6.4.7 Intrusion & Perimeter Analytics

The platform shall support:

- intrusion detection,
- line crossing detection,
- zone intrusion alerts,
- virtual fencing,
- and perimeter breach analytics.

6.4.8 Fire & Smoke Detection

The AI system shall support:

- fire detection,
- smoke detection,
- abnormal heat detection,
- and automated alert generation.

The system shall support integration with:

- thermal cameras,
- emergency systems,
- and incident management systems.

6.4.9 Vehicle Analytics

The platform shall support:

- vehicle counting,
- vehicle classification,
- traffic density estimation,
- congestion analytics,
- and route utilization analysis.

6.4.10 Parking Analytics

The system shall support:

- parking occupancy analytics,
- parking utilization analytics,
- inflow/outflow analytics,
- and parking congestion alerts.

6.4.11 Incident Analytics

The AI platform shall support:

- suspicious activity detection,
- abnormal event detection,
- crowd anomaly detection,
- unattended object detection,
- and configurable operational event analytics.

6.4.12 Water Surveillance Analytics

The system shall support analytics for:

- riverbank monitoring,
- water-zone crowd monitoring,
- restricted zone detection,
- and emergency event alerts.

6.5 Predictive Analytics & Decision Support

6.5.1 Predictive Intelligence

The AI platform shall support:

- predictive congestion analytics,
- trend analysis,
- behavioural analytics,

- and event forecasting.

The system shall support forecasting of:

- crowd buildup,
- congestion formation,
- traffic accumulation,
- and operational risk indicators.

6.5.2 Forecast Window

The system shall support predictive analysis for:

- 15–30 minute operational forecasting,
- configurable forecasting windows,
- and trend-based operational recommendations.

6.5.3 Decision Support Integration

The AI platform shall support:

- SOP-based alerting,
- automated operational recommendations,
- escalation workflows,
- and integration with Digital Twin simulations.

6.6 GIS & Digital Twin Integration

6.6.1 GIS Integration

The platform shall support:

- GIS-based visualization,
- map-based event plotting,
- geospatial correlation,
- and location-based alert visualization.

6.6.2 Digital Twin Integration

The AI platform shall integrate with the Digital Twin platform for:

- simulation-driven analytics,
- predictive crowd modelling,
- congestion forecasting,
- and evacuation scenario support.

6.7 Alert Management System

6.7.1 Alert Generation

The AI platform shall generate:

- real-time alerts,
- threshold-based alerts,
- predictive alerts,
- event-based alerts,
- and escalated alerts.

6.7.2 Alert Prioritization

Alerts shall support:

- severity classification,
- location tagging,
- incident categorization,
- and configurable escalation hierarchy.

6.7.3 Alert Channels

Alerts shall support:

- ICCC dashboards,
- video wall integration,
- SMS,
- email,
- mobile application notifications,
- and other configured communication channels.

6.8 AI Model Requirements

6.8.1 AI Model Characteristics

The AI models shall:

- be configurable,
- support retraining and tuning,
- support operational calibration,
- and support contextual optimization.

6.8.2 AI Explainability

The platform shall support:

- operator-verifiable alerts,
- auditability of AI-generated events,
- explainable event triggers,

- and operational review capability.

6.8.3 Accuracy Requirements

The AI platform shall provide high operational accuracy under varied environmental conditions.

The bidder shall specify:

- expected accuracy levels,
- environmental limitations,
- and operational dependencies.

6.9 Performance Requirements

6.9.1 Processing Latency

The AI platform shall support:

- near real-time analytics processing,
- low-latency event generation,
- and rapid operational alerting.

Critical alerts shall preferably be generated within operationally acceptable timelines.

6.9.2 Concurrent Processing

The system shall support:

- simultaneous multi-camera analytics,
- high-density event processing,
- and large-scale event handling during peak snan periods.

6.9.3 High Availability

The AI platform shall support:

- redundant architecture,
- failover capability,
- load balancing,
- and uninterrupted analytics operations.

6.10 Dashboard & Visualization

6.10.1 Operational Dashboard

The platform shall provide centralized dashboards for:

- crowd monitoring,
- traffic analytics,
- event monitoring,
- predictive alerts,

- and operational intelligence.

6.10.2 Customizable Views

The system shall support:

- role-based dashboards,
- configurable widgets,
- customizable analytics views,
- and multi-screen operations.

6.10.3 Reporting

The platform shall support:

- operational reports,
- incident reports,
- trend reports,
- crowd analytics reports,
- traffic reports,
- and exportable reports.

Reports shall support:

- PDF,
- XLSX,
- CSV,
- and GIS-compatible exports.

6.11 Cybersecurity & Data Protection

6.11.1 Security Requirements

The AI platform shall support:

- secure authentication,
- encrypted communication,
- audit logging,
- access control,
- and cybersecurity hardening.

6.11.2 Compliance

The platform shall comply with:

- CERT-In guidelines,
- applicable Government cybersecurity requirements,

- and industry best practices.

6.12 Integration Requirements

The AI platform shall support seamless integration with:

- VMS,
- ICCC,
- Digital Twin platform,
- GIS systems,
- ANPR systems,
- emergency systems,
- public communication systems,
- and approved third-party systems.

The platform shall support:

- REST APIs,
- SDK support,
- and standard integration mechanisms.

6.13 Testing & Acceptance

The SI shall demonstrate the following during FAT/SAT/UAT/PoC:

- crowd density analytics,
- queue analytics,
- heatmaps,
- reverse flow detection,
- predictive alerts,
- GIS integration,
- Digital Twin integration,
- and alert workflows.

Peak-load simulation and operational stress testing shall be carried out before Go-Live.

6.14 Training & Knowledge Transfer

The SI shall provide training for:

- ICCC operators,
- administrators,
- police personnel,
- and authorized users

covering:

- analytics interpretation,
- incident management,
- dashboard operations,
- and operational workflows.

6.15 OEM & Support Requirements

The AI Analytics Platform shall:

- be OEM-backed,
- have proven large-scale deployment experience,
- support enterprise-grade operations,
- and provide updates and support during the contract period.

OEM authorization and support commitment shall be mandatory.

6.16 SLA Requirements

The AI platform shall support:

- minimum 99.5% uptime during event period,
- defined alert response timelines,
- performance monitoring,
- and fault reporting.

Major snan days shall be treated as critical operational periods requiring enhanced SLA compliance.

6.17 Future Readiness

The proposed AI platform shall:

- support future analytics modules,
- support additional integrations,
- support future smart city use cases,
- and support evolving operational requirements without major redesign.

SECTION 7: DIGITAL TWIN & DECISION INTELLIGENCE PLATFORM

7. DIGITAL TWIN & DECISION INTELLIGENCE PLATFORM

7.1 Overview

The System Integrator (SI) shall design, supply, install, configure, integrate, test, commission, operate and maintain an enterprise-grade Digital Twin & Decision Intelligence Platform for Simhastha 2028.

The platform shall function as the predictive intelligence, simulation, operational visualization, and decision-support layer of the ICCC ecosystem and shall enable:

- real-time situational awareness,
- predictive crowd management,
- traffic intelligence,
- congestion forecasting,
- emergency response planning,
- simulation-driven operational decisions,
- and coordinated multi-agency management.

The platform shall create a dynamic digital representation of:

- the Mela Area,
- city infrastructure,
- ghats,
- roads,
- parking areas,
- holding zones,
- public facilities,
- transport corridors,
- and integrated operational assets.

The platform shall ingest and correlate real-time operational data from:

- surveillance systems,
- AI analytics,
- ANPR systems,
- IoT devices,
- drones,
- GPS systems,
- public communication systems,

- traffic systems,
- weather systems,
- social media monitoring systems,
- and other integrated platforms.

7.2 Objectives

The objectives of the Digital Twin & Decision Intelligence Platform include:

- predictive crowd management,
- proactive congestion mitigation,
- simulation-based planning,
- operational decision support,
- multi-agency coordination,
- emergency response optimization,
- and enhanced situational intelligence.

7.3 General Requirements

7.3.1 Architecture

The proposed platform shall:

- be enterprise-grade,
- GIS-enabled,
- modular,
- scalable,
- API-driven,
- and based on open architecture principles.

The platform shall support:

- centralized operations,
- distributed operations,
- hybrid cloud/on-premise deployment,
- and high availability architecture.

7.3.2 Open Standards & Interoperability

The platform shall:

- support standard APIs,
- support multi-OEM integration,
- support open GIS standards,

- support integration with third-party systems,
- and avoid vendor lock-in.

The platform shall support seamless integration with:

- ICCC,
- VMS,
- AI Analytics Platform,
- GIS systems,
- ANPR systems,
- ATCS,
- emergency systems,
- and approved external systems.

7.3.3 Scalability

The proposed platform shall:

- initially support operations for approximately 2,600–2,800 cameras,
- support future expansion up to minimum 4,000 cameras,
- support onboarding of additional IoT devices and systems,
- and support future smart city integrations without major redesign.

7.4 GIS & Geospatial Visualization

7.4.1 GIS-Based Visualization

The platform shall provide:

- real-time GIS visualization,
- map-based situational awareness,
- multi-layer operational dashboards,
- and geospatial incident correlation.

7.4.2 GIS Layers

The platform shall support configurable GIS layers including:

- roads,
- ghats,
- sectors,
- parking areas,
- holding areas,
- utilities,

- emergency infrastructure,
- surveillance infrastructure,
- public facilities,
- transport infrastructure,
- and operational assets.

7.4.3 2D & 3D Visualization

The platform shall support:

- 2D GIS visualization,
- 3D visualization,
- object-level navigation,
- zoom/pan/rotate functionality,
- and layered operational visualization.

7.4.4 Asset Visualization

The platform shall support visualization of:

- cameras,
- drones,
- vehicles,
- public infrastructure,
- field personnel,
- and operational assets on GIS interface.

7.5 Real-Time Data Ingestion & Correlation

7.5.1 Data Ingestion

The platform shall ingest real-time data from:

- CCTV systems,
- AI analytics engines,
- ANPR systems,
- drones,
- IoT devices,
- GPS systems,
- parking systems,
- traffic systems,
- public communication systems,

- and approved third-party platforms.

7.5.2 Data Correlation

The platform shall support:

- multi-source event correlation,
- GIS-linked operational intelligence,
- incident correlation,
- and unified operational visualization.

7.5.3 Data Refresh Rate

The platform shall support near real-time operational updates with minimal latency suitable for operational decision making.

7.6 Crowd Simulation & Predictive Analytics

7.6.1 Crowd Simulation

The platform shall support:

- crowd movement simulation,
- pedestrian flow modelling,
- density forecasting,
- and crowd accumulation analysis.

7.6.2 Congestion Forecasting

The platform shall support:

- predictive congestion analytics,
- hotspot forecasting,
- queue buildup prediction,
- and movement trend analysis.

The platform shall support operational forecasting for:

- 15–30 minute predictive windows.

7.6.3 Crowd Diversion Support

The system shall support:

- crowd diversion planning,
- alternate route identification,
- crowd balancing strategies,
- and operational recommendations.

7.6.4 Reverse Flow Risk Analysis

The platform shall support:

- reverse flow simulation,
- abnormal movement modelling,
- and risk zone identification.

7.7 Traffic & Mobility Intelligence

7.7.1 Traffic Simulation

The platform shall support:

- traffic movement simulation,
- congestion analysis,
- route utilization analytics,
- and diversion planning.

7.7.2 Parking Intelligence

The platform shall support:

- parking occupancy visualization,
- parking utilization analytics,
- holding area analytics,
- and inflow/outflow estimation.

7.7.3 Route Optimization

The system shall support:

- emergency route optimization,
- traffic rerouting recommendations,
- and dynamic mobility planning.

7.8 Emergency Response & Disaster Management

7.8.1 Emergency Simulation

The platform shall support:

- emergency scenario simulation,
- evacuation modelling,
- crowd evacuation planning,
- disaster response planning,
- and operational stress simulation.

7.8.2 Evacuation Modelling

The platform shall support:

- evacuation route analysis,

- safe-zone planning,
- exit capacity assessment,
- and response time estimation.

7.8.3 Incident Correlation

The system shall support:

- incident visualization,
- multi-agency coordination support,
- incident escalation,
- and real-time operational decision support.

7.9 Decision Intelligence Engine

7.9.1 Decision Support

The platform shall support:

- automated operational recommendations,
- SOP-based response workflows,
- incident prioritization,
- and escalation support.

7.9.2 Workflow Automation

The platform shall support:

- configurable workflows,
- rule-based automation,
- escalation workflows,
- and incident lifecycle management.

7.9.3 Alert Prioritization

The system shall support:

- severity-based alerts,
- geography-based alerts,
- impact-based prioritization,
- and configurable escalation matrix.

7.9.4 Multi-Agency Coordination

The platform shall support coordinated operational workflows for:

- Police,
- Administration,

- Health Department,
- Fire Services,
- SDRF/NDRF,
- Transport Agencies,
- and other stakeholders.

7.10 Social Media & External Intelligence Integration

7.10.1 Social Media Monitoring

The platform shall support integration with approved social media monitoring systems for:

- public sentiment analysis,
- event monitoring,
- rumor detection,
- incident reporting,
- and operational alerts.

7.10.2 External Data Sources

The platform shall support integration with:

- weather systems,
- AQI systems,
- river/water monitoring systems,
- GPS systems,
- and approved external operational data sources.

7.11 Dashboard & Visualization

7.11.1 Unified Dashboard

The platform shall provide:

- centralized operational dashboard,
- GIS-based operational view,
- incident dashboard,
- predictive analytics dashboard,
- and executive dashboards.

7.11.2 Role-Based Dashboards

The platform shall support:

- operator dashboards,
- supervisory dashboards,

- command dashboards,
- field dashboards,
- and agency-specific views.

7.11.3 Video Integration

The platform shall support:

- live video overlays,
- GIS-linked video streams,
- camera trigger from GIS map,
- and synchronized operational visualization.

7.12 Reporting & Analytics

7.12.1 Reporting

The platform shall support:

- operational reports,
- simulation reports,
- incident reports,
- trend analysis reports,
- and predictive analytics reports.

7.12.2 Export Capability

Reports and dashboards shall support export in:

- PDF,
- XLSX,
- CSV,
- GIS-compatible formats.

7.13 Performance Requirements

7.13.1 Processing Performance

The platform shall support:

- simultaneous multi-source ingestion,
- real-time visualization,
- and large-scale event processing.

7.13.2 High Availability

The platform shall support:

- redundant architecture,

- failover mechanisms,
- load balancing,
- and uninterrupted operations.

7.13.3 Operational Latency

Critical alerts and operational recommendations shall be generated within operationally acceptable timelines suitable for real-time command operations.

7.14 Cybersecurity & Data Protection

7.14.1 Security Requirements

The platform shall support:

- secure authentication,
- encrypted communication,
- audit logging,
- secure APIs,
- access control,
- and cybersecurity hardening.

7.14.2 Compliance

The platform shall comply with:

- CERT-In guidelines,
- applicable Government cybersecurity standards,
- and industry best practices.

7.15 Integration Requirements

The platform shall support seamless integration with:

- ICCC,
- VMS,
- AI Analytics Platform,
- ANPR systems,
- GIS systems,
- ATCS,
- public communication systems,
- emergency systems,
- and approved third-party systems.

The platform shall support:

- REST APIs,

- SDKs,
- WebSocket/MQTT support where applicable,
- and standard integration frameworks.

7.16 Testing & Acceptance

The SI shall demonstrate during FAT/SAT/UAT/PoC:

- GIS visualization,
- crowd simulation,
- congestion forecasting,
- predictive alerts,
- evacuation modelling,
- dashboard functionality,
- workflow automation,
- and multi-system integration.

Peak-load simulation and operational stress testing shall be carried out prior to Go-Live.

7.17 Training & Capacity Building

The SI shall provide comprehensive training for:

- ICCC operators,
- administrators,
- technical teams,
- field personnel,
- and stakeholder agencies.

Training shall include:

- platform operations,
- simulation workflows,
- incident management,
- dashboard operations,
- and operational decision support usage.

7.18 OEM & Support Requirements

The proposed platform shall:

- be OEM-backed,
- have proven enterprise deployment experience,
- support long-term upgrades,

- and provide technical support during the contract period.

OEM authorization and support commitment shall be mandatory.

7.19 SLA Requirements

The platform shall support:

- minimum 99.5% uptime during event period,
- real-time operational responsiveness,
- defined alert timelines,
- and operational continuity during major snan days.

7.20 Future Readiness

The proposed platform shall:

- support future smart city integrations,
- support onboarding of additional sensors and systems,
- support future analytics modules,
- and support evolving operational requirements without major redesign.

SECTION 8: COMMUNICATION NETWORK

8. COMMUNICATION NETWORK

8.1 Overview

The System Integrator (SI) shall design, engineer, supply, install, integrate, test, commission, operate and maintain a highly available, resilient, scalable, and secure communication network infrastructure for Simhastha 2028.

The communication network shall serve as the backbone infrastructure for:

- surveillance systems,
- ICCC operations,
- AI analytics,
- Digital Twin platform,
- public communication systems,
- emergency response systems,
- traffic systems,
- and all integrated field infrastructure.

The network shall support uninterrupted transmission of:

- video feeds,
- analytics data,
- operational data,
- voice/data traffic,
- and command & control communication.

The proposed architecture shall follow:

- ring-based redundancy,
- hybrid OFC + RF architecture,
- distributed aggregation,
- low-latency communication,
- and high availability design principles.

8.2 Objectives

The objectives of the communication network include:

- high-speed data connectivity,
- resilient network operations,
- low-latency video transmission,

- uninterrupted ICCC operations,
- scalable future-ready infrastructure,
- and secure communication architecture.

8.3 Network Architecture

8.3.1 Overall Architecture

The communication network shall comprise:

- OFC backbone network,
- RF/microwave backup network,
- field aggregation network,
- core network infrastructure,
- edge connectivity infrastructure,
- and network management systems.

The architecture shall support centralized monitoring, distributed field operations, failover capability, and network redundancy.

8.3.2 Ring Topology

The OFC backbone shall preferably be designed in ring topology, dual-ring topology, or equivalent resilient architecture.

The network shall support automatic failover, alternate routing, and minimal service interruption in case of fiber/network failure.

8.3.3 Redundancy Requirements

The network shall support redundancy at core level, aggregation level, power level, communication path level, and critical field locations.

8.3.4 Hybrid Connectivity

The network architecture shall support OFC as primary communication medium, RF/microwave/ wireless links as backup, and alternate communication paths for critical infrastructure.

8.4 OFC Backbone Infrastructure

8.4.1 Scope

The SI shall survey, design, lay, terminate, splice, test, commission, and maintain the OFC backbone infrastructure.

8.4.2 OFC Deployment Areas

The OFC backbone shall cover ICCC, Mela Area, ghats, roads, parking areas, holding areas, major intersections, control points, viewing centres, and critical operational locations.

8.4.3 OFC Specifications

The OFC network shall support high-bandwidth video transmission, support future scalability, support redundant routing, and comply with applicable standards.

The SI shall use outdoor armoured OFC, HDPE ducting, and industrial-grade accessories suitable for outdoor deployment.

8.4.4 OFC Laying Methodology

The SI shall undertake trenching, HDD (where required), duct laying, reinstatement, route marking, and restoration works.

The SI shall ensure minimal disruption to public infrastructure, traffic management during execution, and compliance with applicable standards and permissions.

8.4.5 Splicing & Termination

The SI shall undertake proper OFC splicing, provide OFDFs, undertake route testing, and maintain acceptable optical loss parameters.

8.4.6 OFC Protection Measures

The SI shall provide route markers, warning tapes, protection pipes, chamber protection, and mechanical protection for OFC routes.

8.4.7 OFC Testing

The SI shall conduct OTDR testing, optical power testing, continuity testing, and acceptance testing.

Test reports shall be submitted to USCL.

8.5 Active Network Infrastructure

8.5.1 Scope

The SI shall supply, install, configure and maintain all active network components including core switches, aggregation switches, edge switches, routers, wireless equipment, network security appliances, and associated accessories.

8.5.2 Core Network

The core network shall support high-throughput operations, support redundant architecture, support low latency, and support centralized management.

The core network shall support high-capacity video traffic, analytics traffic, and operational data traffic.

8.5.3 Aggregation Network

The aggregation layer shall aggregate field traffic, support resilient routing, support ring architecture, and support QoS mechanisms.

8.5.4 Edge Network

The edge network shall support camera connectivity, field device connectivity, edge analytics, and distributed field operations.

8.5.5 Industrial Network Components

All field-level network equipment shall be industrial-grade, support outdoor deployment, support extended operating temperatures, and support surge protection.

8.6 Wireless & RF Infrastructure

8.6.1 Scope

The SI shall provide wireless/RF connectivity infrastructure wherever OFC connectivity is infeasible, temporary, or required as backup.

8.6.2 RF/Microwave Links

The wireless infrastructure shall support point-to-point connectivity, point-to-multipoint connectivity, backup communication, and resilient network architecture.

8.6.3 Outdoor Wi-Fi Infrastructure

The SI may provide outdoor Wi-Fi infrastructure for field operations, operational connectivity, temporary operational areas, and approved public utility applications.

8.7 Enterprise Radio / Wireless Communication System

The scope shall also include integration/provisioning of enterprise field communication systems including wireless handheld communication devices, command communication consoles, and interoperable radio communication support for coordinated field operations during Simhastha.

This will cover:

- digital wireless communication,
- handheld radios,
- command communication consoles,
- repeater/base stations,
- interoperability,
- emergency communication,
- GPS-enabled radios (optional),
- group communication,
- and integration with ICCC.

8.8 Network Performance Requirements

8.8.1 Bandwidth

The network shall support adequate bandwidth for HD video streams, AI analytics, Digital Twin operations, and concurrent ICCC operations.

The SI shall undertake detailed bandwidth sizing during design stage.

8.8.2 Latency

The network shall support low-latency video transmission, real-time analytics communication, and operational responsiveness suitable for ICCC operations.

8.8.3 Quality of Service (QoS)

The network shall support QoS policies for video traffic, critical alerts, operational data, and emergency communication.

8.8.4 Network Availability

The communication network shall support high availability architecture, failover mechanisms, and uninterrupted operations during peak event periods.

8.9 Network Management System (NMS)

8.9.1 Scope

The SI shall provide centralized Network Management System (NMS) for monitoring and management of network devices, bandwidth utilization, connectivity status, link health, and network events.

8.9.2 Functional Requirements

The NMS shall support topology visualization, fault monitoring, event correlation, alert generation, reporting, and centralized diagnostics.

8.9.3 Monitoring

The NMS shall support real-time monitoring, bandwidth monitoring, link monitoring, device health monitoring, and network utilization analytics.

8.10 Cybersecurity Requirements

8.10.1 Secure Network Architecture

The communication network shall support network segmentation, VLAN architecture, secure routing, secure remote access, and controlled network access.

8.10.2 Security Controls

The SI shall implement firewalls, IDS/IPS, secure authentication, secure device configuration, and cybersecurity hardening.

8.10.3 Compliance

The network architecture shall comply with:

- CERT-In guidelines,
- Government cybersecurity advisories,
- and applicable standards.

8.11 Power & Environmental Requirements

8.11.1 Power Backup

Critical network infrastructure shall support UPS backup, surge protection, and stable operations during power fluctuations.

8.11.2 Environmental Protection

Field network infrastructure shall support outdoor operations, dust protection, weather protection, and thermal protection.

8.12 Integration Requirements

The communication network shall support seamless integration with:

- ICCC systems,

- surveillance systems,
- AI analytics,
- Digital Twin platform,
- emergency systems,
- public communication systems,
- and approved third-party systems.

8.13 Testing & Acceptance

8.13.1 Testing Requirements

The SI shall conduct:

- OFC testing,
- bandwidth testing,
- failover testing,
- redundancy testing,
- latency testing,
- and operational stress testing.

8.13.2 Acceptance Testing

Acceptance testing shall include:

- network performance validation,
- failover validation,
- operational load testing,
- and integrated system testing.

8.14 Restoration & Maintenance

8.14.1 Fault Restoration

The SI shall maintain defined restoration timelines for OFC cuts, network device failures, connectivity loss, and critical communication failures.

8.14.2 Preventive Maintenance

The SI shall undertake preventive maintenance, route inspection, cleaning, firmware upgrades, and proactive monitoring.

8.15 Documentation Requirements

The SI shall provide network architecture diagrams, route maps, OFC layouts, IP addressing plans, rack layouts, configuration documents, and as-built drawings.

8.16 SLA Requirements

The communication network shall support:

- minimum 99.5% uptime during event period,
- low-latency operations,
- rapid fault restoration,
- and uninterrupted operations during major snan days.

Peak snan days shall be treated as critical operational periods requiring enhanced SLA compliance.

8.17 Future Readiness

The proposed communication network shall support future scalability, support onboarding of additional cameras and devices, support future smart city applications, and support evolving operational requirements without major redesign.

SECTION 9: CYBERSECURITY FRAMEWORK

9. CYBERSECURITY FRAMEWORK

9.1 Overview

The System Integrator (SI) shall design, implement, integrate, operate and maintain a comprehensive cybersecurity framework for the ICCC ecosystem of Simhastha 2028.

The cybersecurity framework shall ensure confidentiality, integrity, availability, resilience, and secure operation of all project infrastructure including surveillance systems, communication network, ICCC infrastructure, AI Analytics Platform, Digital Twin Platform, VMS, storage systems, applications, APIs, databases, cloud/on-prem infrastructure, and integrated third-party systems.

The cybersecurity architecture shall follow defense-in-depth principles, zero-trust security concepts, layered security controls, secure access mechanisms, continuous monitoring, and proactive threat management.

9.2 Objectives

The objectives of the cybersecurity framework include:

- protection of critical infrastructure,
- prevention of unauthorized access,
- secure transmission of operational data,
- cyber threat detection,
- incident response readiness,
- operational continuity,
- and compliance with Government cybersecurity guidelines.

9.3 General Requirements

9.3.1 Security by Design

The entire ICCC ecosystem shall follow secure-by-design principles, least privilege access, secure configuration practices, and layered security architecture.

Cybersecurity shall be integrated at network layer, application layer, endpoint layer, device layer, and operational layer.

9.3.2 Standards & Compliance

The cybersecurity framework shall comply with:

- CERT-In guidelines,
- applicable Government of India cybersecurity advisories,
- MeitY guidelines,
- ISO 27001 principles,
- and applicable industry best practices.

9.3.3 Security Governance

The SI shall establish cybersecurity governance mechanisms, security policies, operational security procedures, incident response procedures, and access management procedures.

9.4 Network Security

9.4.1 Secure Network Architecture

The network shall support segmented architecture, VLAN-based isolation, secure routing, network zoning, and controlled communication pathways.

Critical systems shall be logically segregated including ICCC systems, surveillance systems, AI systems, Digital Twin platform, and external/public networks.

9.4.2 Firewall Systems

The SI shall deploy enterprise-grade firewall systems supporting traffic filtering, application control, policy management, threat prevention, and secure access control.

9.4.3 IDS/IPS

The SI shall implement Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), anomaly detection, and threat monitoring mechanisms.

9.4.4 Secure Remote Access

Remote access mechanisms shall support secure VPN connectivity, multi-factor authentication, encrypted sessions, and role-based access control.

9.4.5 Secure Communication

All communication channels shall support encrypted transmission, secure protocols, secure API communication, and secure data exchange mechanisms.

9.5 Endpoint & Device Security

9.5.1 Endpoint Protection

The SI shall implement endpoint protection mechanisms for servers, workstations, operator consoles, field devices, and other connected systems.

9.5.2 Device Hardening

All systems and devices shall be securely configured, hardened against vulnerabilities, stripped of unnecessary services, and protected against unauthorized access.

9.5.3 Camera Security

The surveillance ecosystem shall support secure camera authentication, encrypted communication, firmware security, password management, and secure onboarding.

9.5.4 IoT Security

IoT and field devices shall support secure device communication, device authentication, secure provisioning, and controlled network access.

9.6 Identity & Access Management (IAM)

9.6.1 User Authentication

The system shall support secure authentication, centralized user management, password policies, and configurable authentication mechanisms.

9.6.2 Multi-Factor Authentication (MFA)

Critical administrative and remote access functions shall support multi-factor authentication, secure login mechanisms, and enhanced access security.

9.6.3 Role-Based Access Control (RBAC)

The system shall support granular RBAC, least privilege access, department-wise access, operator-level permissions, and hierarchical authorization.

9.6.4 Audit Logging

The system shall maintain user activity logs, access logs, configuration change logs, administrative logs, and security event logs.

9.7 Security Monitoring & Incident Management

9.7.1 Security Monitoring

The SI shall implement centralized security monitoring for network traffic, devices, applications, user activities, and security events.

9.7.2 SIEM Integration

The cybersecurity framework shall support SIEM integration, event correlation, centralized log management, and security analytics.

9.7.3 Security Operations Support

The SI shall provide security monitoring support, threat alerting, incident reporting, and escalation mechanisms.

9.7.4 Incident Response

The SI shall establish cybersecurity incident response procedures, incident classification, escalation workflows, containment procedures, and recovery mechanisms.

9.8 Application Security

9.8.1 Secure Application Architecture

All applications and platforms shall support secure coding practices, secure APIs, secure authentication, session security, and input validation.

9.8.2 API Security

All APIs shall support authentication, authorization, encryption, rate limiting, and audit logging.

9.8.3 Web Security

Web-based platforms shall support protection against unauthorized access, injection attacks, session hijacking, cross-site scripting, and other common web vulnerabilities.

9.9 Data Security & Privacy

9.9.1 Data Protection

The SI shall implement mechanisms for data confidentiality, integrity protection, secure storage, secure backup, and controlled access.

9.9.2 Encryption

Sensitive data shall support encryption in transit, encryption at rest, and secure key management mechanisms.

9.9.3 Privacy Controls

The system shall support controlled access to surveillance data, privacy-aware operational access, auditability, and secure data handling practices.

9.9.4 Data Retention

Data retention policies shall comply with project requirements, operational policies, and applicable Government guidelines.

9.10 Vulnerability Assessment & Security Testing

9.10.1 Vulnerability Assessment

The SI shall conduct periodic vulnerability assessments, security audits, and remediation activities.

9.10.2 Penetration Testing

The SI shall conduct VAPT, network penetration testing, application security testing, and remediation verification.

9.10.3 Security Hardening Validation

The SI shall validate device hardening, server hardening, application hardening, and network hardening.

9.11 Backup, Recovery & Business Continuity

9.11.1 Backup Mechanisms

The SI shall implement data backup systems, configuration backups, secure backup storage, and backup verification mechanisms.

9.11.2 Disaster Recovery

The cybersecurity framework shall support disaster recovery integration, failover mechanisms, operational continuity, and recovery procedures.

9.11.3 Business Continuity

The SI shall establish business continuity procedures, recovery workflows, and operational continuity planning.

9.12 Third-Party & Integration Security

9.12.1 Third-Party Integration Security

All third-party integrations shall support secure API integration, controlled access, auditability, and cybersecurity compliance.

9.12.2 Private CCTV Integration Security

Private CCTV integration shall support consent-based onboarding, secure connectivity, access control, and segregated operational access.

9.13 Security Logging & Audit Trails

9.13.1 Logging Requirements

The system shall maintain logs for user activity, access attempts, administrative actions, security events, system failures, and operational incidents.

9.13.2 Log Retention

Security logs shall support configurable retention and archival policies.

9.13.3 Auditability

The system shall support audit trails, forensic investigation support, and event traceability.

9.14 Training & Awareness

9.14.1 Security Training

The SI shall provide cybersecurity awareness and operational security training for:

- ICCC operators,
- administrators,
- technical teams,
- and authorized stakeholders.

9.14.2 Incident Handling Training

Training shall include cyber incident reporting, response workflows, escalation procedures, and operational best practices.

9.15 Documentation Requirements

The SI shall provide cybersecurity architecture documents, security policies, incident response plans, hardening guidelines, access control procedures, VAPT reports, and audit documentation.

9.16 Testing & Acceptance

9.16.1 Security Testing

The SI shall conduct security validation, access control testing, failover testing, penetration testing, and incident response validation.

9.16.2 Acceptance Criteria

Cybersecurity acceptance shall include successful VAPT closure, security configuration validation, audit compliance, and operational security verification.

9.16.3 SLA Requirements

The cybersecurity framework shall support continuous monitoring, defined response timelines, incident escalation, and operational security support during event period.

Major snan days shall be treated as critical operational periods requiring enhanced security monitoring.

9.17 OEM & Support Requirements

All cybersecurity components shall be OEM-backed, support enterprise-grade deployment, provide updates and patches, and support long-term operational maintenance.

OEM authorization and support commitment shall be mandatory.

9.18 Future Readiness

The proposed cybersecurity architecture shall support future expansion, support additional integrations, support evolving cyber threat landscapes, and support future smart city operational requirements without major redesign.

SECTION 10: DATA CENTER / DISASTER RECOVERY / STORAGE

10. DATA CENTER / DISASTER RECOVERY / STORAGE

10.1 Overview

The System Integrator (SI) shall design, supply, install, configure, integrate, test, commission, operate and maintain a secure, scalable, resilient, and high-availability Data Center (DC), Disaster Recovery (DR), and Storage infrastructure for the ICCC ecosystem of Simhastha 2028.

The DC/DR infrastructure shall support:

- surveillance systems,
- Video Management System (VMS),
- AI Analytics Platform,
- Digital Twin & Decision Intelligence Platform,
- ICCC applications,
- GIS systems,
- databases,
- communication systems,
- reporting systems,
- and integrated operational platforms.

The architecture shall support:

- uninterrupted operations,
- centralized data management,
- high-volume video ingestion,
- failover capability,
- disaster recovery,
- operational continuity,
- cybersecurity compliance,
- and future scalability.

The proposed infrastructure shall follow:

- hybrid architecture principles,
- virtualization-based deployment,
- centralized management,
- and enterprise-grade redundancy mechanisms.

10.2 Objectives

The objectives of the DC/DR infrastructure include:

- reliable data storage,
- secure operational data management,
- uninterrupted ICCC operations,
- high-performance video recording,
- disaster resilience,
- business continuity,
- and future-ready scalable infrastructure.

10.3 Architecture Requirements

10.3.1 Deployment Model

The proposed architecture may support on-premise deployment, cloud-assisted deployment, hybrid deployment, or equivalent enterprise architecture,

subject to approval of USCL and applicable Government guidelines.

10.3.2 Hybrid Architecture

The proposed solution shall support centralized data center architecture, edge recording capability, distributed field storage where required, and centralized archival and analytics processing.

10.3.3 Scalability

The infrastructure shall:

- initially support operations for approximately 2,600–2,800 cameras,
- support future expansion up to minimum 4,000 cameras,
- support additional AI workloads,
- support additional applications,
- and support future smart city integrations without major redesign.

10.3.4 High Availability

The architecture shall support redundant compute infrastructure, redundant storage architecture, redundant networking, failover mechanisms, and uninterrupted operations.

No single point of failure shall exist for critical systems.

10.4 Data Center Infrastructure

10.4.1 Scope

The SI shall provide compute infrastructure, virtualization infrastructure, storage infrastructure, networking infrastructure, rack infrastructure, power infrastructure, and management systems required for ICCC operations.

10.4.2 Compute Infrastructure

The compute infrastructure shall support VMS operations, AI analytics workloads, Digital Twin platform, GIS applications, databases, operational applications, and future expansion.

The compute architecture shall support virtualization, clustering, GPU-enabled processing where required, and high-performance operations.

10.4.3 Virtualization Infrastructure

The SI shall provide enterprise-grade virtualization infrastructure supporting server virtualization, resource pooling, workload balancing, failover capability, and centralized management.

10.4.4 Rack Infrastructure

The SI shall provide standard enterprise racks, cable management, structured power distribution, environmental management, and organized equipment layouts.

10.4.5 Environmental Controls

The data center environment shall support cooling systems, temperature management, humidity control, fire suppression, access control, and environmental monitoring.

10.5 Storage Infrastructure

10.5.1 Scope

The SI shall provide centralized storage infrastructure supporting:

- surveillance video storage,
- AI analytics data,
- Digital Twin data,
- operational databases,
- application data,
- backups,
- and archival storage.

10.5.2 Storage Architecture

The storage architecture shall support centralized storage, scalable storage expansion, RAID protection, high-throughput video recording, and enterprise-grade storage management.

The architecture shall support structured data, unstructured data, video data, analytics metadata, and archival data.

10.5.3 Video Retention

The storage infrastructure shall support:

- minimum **60 days** video retention,
- extendable up to 90 days for critical feeds,
- configurable retention policies,
- and selective archival mechanisms.

10.5.4 Edge Recording

The architecture shall support edge recording at camera level where required, recording synchronization, automatic recovery, and centralized archival.

10.5.5 Storage Performance

The storage system shall support simultaneous recording, playback, analytics processing, and concurrent multi-user access.

The storage shall support high write throughput, rapid retrieval, and operational responsiveness.

10.5.6 Data Protection

The storage infrastructure shall support RAID protection, redundancy, snapshots, backup integration, and data integrity mechanisms.

10.6 Disaster Recovery (DR)

10.6.1 Scope

The SI shall provide Disaster Recovery (DR) infrastructure and operational mechanisms for ensuring continuity of critical ICCC operations.

10.6.2 DR Architecture

The DR architecture shall support failover operations, replication, redundancy, backup systems, and continuity of critical services.

10.6.3 DR Site

The DR setup may utilize cloud-based DR, secondary DC integration, or equivalent approved architecture.

The DR architecture shall comply with operational resilience requirements, cybersecurity requirements, and Government guidelines.

10.6.4 Replication

The DR architecture shall support data replication, application replication, configuration replication, and recovery workflows.

10.6.5 Recovery Objectives

The SI shall propose suitable:

- Recovery Point Objective (RPO),
- and Recovery Time Objective (RTO)

for critical systems.

Critical operational systems shall support rapid recovery mechanisms.

10.6.6 DR Testing

The SI shall conduct DR drills, failover testing, recovery validation, and operational continuity testing.

10.7 Backup Infrastructure

10.7.1 Backup Mechanisms

The SI shall provide automated backup systems, backup scheduling, backup monitoring, and backup verification mechanisms.

10.7.2 Backup Scope

The backup system shall support application backups, configuration backups, database backups, operational data backups, and critical video archival.

10.7.3 Backup Retention

The backup architecture shall support configurable backup retention policies as per operational requirements.

10.8 Database Infrastructure

10.8.1 Database Support

The infrastructure shall support operational databases, analytics databases, GIS databases, metadata storage, and application databases.

10.8.2 Database High Availability

The database architecture shall support redundancy, failover, replication, and backup mechanisms.

10.9 Network Integration

The DC/DR infrastructure shall integrate seamlessly with ICCC systems, surveillance systems, AI Analytics Platform, Digital Twin platform, GIS systems, communication network, and approved third-party systems.

10.10 Cybersecurity Requirements

10.10.1 Secure Architecture

The DC/DR infrastructure shall support secure access, network segregation, secure management, and controlled administrative access.

10.10.2 Security Controls

The SI shall implement firewalls, access controls, SIEM integration, logging, encryption, and security monitoring.

10.10.3 Compliance

The DC/DR architecture shall comply with:

- CERT-In guidelines,
- MeitY advisories,
- Government cybersecurity policies,
- and industry best practices.

10.11 Monitoring & Management

10.11.1 10.11.1 Infrastructure Monitoring

The SI shall provide centralized monitoring for compute infrastructure, storage infrastructure, network infrastructure, backup systems, virtualization systems, and environmental systems.

10.11.2 Alerting

The system shall support automated alerts, fault notifications, capacity alerts, performance alerts, and operational health monitoring.

10.11.3 Reporting

The infrastructure shall support utilization reports, storage reports, backup reports, operational health reports, and audit reports.

10.12 Testing & Acceptance

10.12.1 Testing

The SI shall conduct performance testing, storage testing, failover testing, DR testing, backup validation, and stress testing.

10.12.2 Acceptance Criteria

Acceptance testing shall include operational validation, storage validation, DR validation, failover validation, and integrated system testing.

10.13 Documentation Requirements

The SI shall provide architecture diagrams, storage sizing documents, backup procedures, DR procedures, rack layouts, IP addressing plans, operational manuals, and as-built documentation.

10.14 SLA Requirements

The DC/DR infrastructure shall support:

- minimum 99.5% uptime during event period,
- uninterrupted recording operations,
- rapid recovery capability,
- and operational continuity during major snan days.

Peak snan days shall be treated as critical operational periods requiring enhanced operational readiness.

10.15 Training & Knowledge Transfer

The SI shall provide training for administrators, ICCC operators, technical teams, and authorized personnel

covering infrastructure operations, backup management, DR operations, storage administration, and troubleshooting.

10.16 OEM & Support Requirements

All DC/DR/storage components shall be OEM-backed, support enterprise-grade operations, support long-term upgrades, and provide technical support during the contract period.

OEM authorization and support commitment shall be mandatory.

10.17 Future Readiness

The proposed DC/DR/storage infrastructure shall support future expansion, support onboarding of additional systems, support future smart city applications, and support evolving operational requirements without major redesign.

SECTION 11: ICCC, MINI WAR-ROOM & VIEWING CENTERS

11. ICCC, MINI WAR-ROOM & VIEWING CENTERS

11.1 Overview

The System Integrator (SI) shall design, supply, install, integrate, test, commission, operationalize and maintain an enterprise-grade Integrated Command & Control Centre (ICCC) ecosystem for Simhastha 2028.

The ICCC ecosystem shall comprise:

- Primary ICCC,
- Secondary/Backup ICCC integration,
- Mini War-Room at Ranoji ki Chhatri,
- Remote Viewing Centers,
- and associated operational infrastructure.

The ICCC ecosystem shall function as the centralized operational platform for surveillance monitoring, crowd management, traffic monitoring, emergency coordination, incident management, AI-driven operational intelligence, Digital Twin operations, and multi-agency command & coordination.

The ICCC architecture shall support real-time operations, multi-agency coordination, high availability, operational scalability, redundancy, cybersecurity, and future smart city integrations.

11.2 Objectives

The objectives of the ICCC ecosystem include:

- centralized operational monitoring,
- integrated event management,
- predictive operational intelligence,
- rapid incident response,
- coordinated emergency management,
- operational decision support,
- and enterprise-grade command operations.

11.3 ICCC Architecture

11.3.1 Enterprise ICCC Model

The ICCC ecosystem shall follow centralized command architecture, distributed viewing capability, integrated data visualization, multi-agency operational workflows, and scalable enterprise architecture.

11.3.2 Components

The ICCC ecosystem shall broadly include Primary ICCC, Secondary/Backup ICCC integration, Mini War-Room, Viewing Centers, Video Wall systems, Operator consoles, Collaboration systems, AV systems, Incident Management Systems, Decision Support Systems, dispatcher console, communication gateway, emergency communication integration and associated infrastructure.

11.4 Primary ICCC

11.4.1 Scope

The SI shall establish and operationalize the Primary ICCC at designated location(s) identified by USCL.

The ICCC shall function as the principal operational command center for Simhastha 2028.

11.4.2 Functional Areas

The ICCC shall support surveillance monitoring, AI analytics monitoring, Digital Twin operations, GIS operations, traffic monitoring, emergency coordination, multi-agency coordination, and executive decision support.

11.4.3 ICCC Infrastructure

The SI shall provide operator consoles, supervisory consoles, video wall systems, workstations, AV systems, display systems, collaboration systems, communication systems, and associated infrastructure.

11.4.4 Operator Capacity

The Primary ICCC shall support approximately 40+ operator positions, supervisory workstations, and executive monitoring positions.

The final seating plan shall be approved by USCL/ Mela Authority.

11.4.5 Video Wall System

The ICCC shall include enterprise-grade video wall infrastructure supporting:

- multi-source visualization,
- dynamic layouts,
- AI alert visualization,
- GIS integration,
- and centralized operational monitoring.

The video wall system shall support:

- redundant controllers,
- centralized management,
- and uninterrupted operations.

11.4.6 Dashboard Integration

The ICCC shall support integrated dashboards for surveillance, AI analytics, Digital Twin, traffic management, incident management, and emergency response operations.

11.4.7 Collaboration Facilities

The ICCC shall support inter-agency collaboration, video conferencing, briefing facilities, incident coordination, and operational review meetings.

11.5 Secondary / Backup ICCC

11.5.1 Scope

The SI shall integrate and operationalize Secondary/Backup ICCC functionality utilizing existing Smart City ICCC infrastructure or other designated facilities, wherever applicable.

11.5.2 Functional Requirements

The Secondary ICCC shall support operational redundancy, failover operations, backup monitoring, emergency operational continuity, and alternate command capability.

11.5.3 Synchronization

The Secondary ICCC shall support real-time synchronization, mirrored operational capability, and continuity of critical operational systems.

11.6 Mini War-Room at Ranoji ki Chhatri

11.6.1 Scope

The SI shall establish and operationalize a temporary/rental Mini War-Room at Ranoji ki Chhatri during the event period.

The Mini War-Room shall function as a localized field coordination and rapid response command facility.

11.6.2 Seating Capacity

The Mini War-Room shall support:

- approximately 20 operational seats,
- supervisory seating,
- and collaborative operational coordination.

11.6.3 Functional Requirements

The Mini War-Room shall support localized surveillance monitoring, field coordination, rapid incident management, emergency response coordination, and operational communication.

11.6.4 Infrastructure

The SI shall provide operator workstations, display systems, communication systems, AV systems, networking, collaboration facilities, and temporary operational infrastructure.

11.6.5 Integration

The Mini War-Room shall integrate seamlessly with Primary ICCC, AI Analytics Platform, Digital Twin platform, GIS systems, and communication systems.

11.6.6 Rental Model

The Mini War-Room may be deployed on rental basis, temporary deployment basis, or equivalent operational model

for approximately **9 months** or as directed by USCL/Mela Authority.

11.7 Viewing Centers

11.7.1 Scope

The SI shall establish and operationalize approximately 10 Viewing Centers at locations identified by USCL.

11.7.2 Purpose

Viewing Centers shall support distributed monitoring, executive monitoring, agency coordination, situational awareness, and operational review.

11.7.3 Proposed Locations

Viewing Centers may be established at:

- Collectorate,
- Police Control Room,
- State-level monitoring centers (2 Nos),
- enroute district monitoring centers,
- and other approved locations.

Final locations shall be approved by USCL.

11.7.4 Infrastructure

Each Viewing Center shall support display systems, operator workstations, video feeds, dashboard access, communication systems, and secure network connectivity.

11.7.5 Integration

Viewing Centers shall integrate with ICCC, VMS, AI Analytics Platform, Digital Twin, and operational dashboards.

11.8 Control Room Design & Interiors

11.8.1 Design Standards

The ICCC ecosystem shall follow:

- enterprise-grade control room standards,
- ergonomic design principles,
- operational efficiency principles,
- and safety standards.

The design may align with:

- ISO 11064 principles,
- industry best practices,

- and approved operational standards.

11.8.2 Interior Infrastructure

The SI shall provide modular interiors, acoustic treatment, anti-static flooring, cable management, lighting systems, HVAC integration, and operator-friendly layouts.

11.8.3 Material Requirements

The SI shall use fire-resistant materials, durable industrial-grade materials, and operationally suitable infrastructure.

11.9 Workstations & Operator Consoles

11.9.1 Operator Consoles

The SI shall provide enterprise-grade operator consoles supporting:

- 24×7 operations,
- ergonomic usage,
- cable management,
- and integrated operational workflows.

11.9.2 Workstations

The workstations shall support VMS operations, AI analytics, Digital Twin visualization, GIS operations, dashboard monitoring, and operational applications.

11.9.3 Display Systems

The ICCC ecosystem shall support large display systems, multi-monitor operations, and high-resolution operational visualization.

11.10 Audio-Visual & Collaboration Systems

11.10.1 AV Infrastructure

The SI shall provide AV systems, presentation systems, audio systems, and collaboration systems.

11.10.2 Video Conferencing

The ICCC ecosystem shall support multi-agency video conferencing, operational briefings, and remote coordination.

11.11 Communication Systems

The ICCC ecosystem shall support secure communication, operational coordination, voice/data integration, and emergency communication workflows.

11.12 Operational Software & Dashboards

The ICCC ecosystem shall support unified operational dashboards, GIS-based operational visualization, incident management, AI-driven alerts, Digital Twin operations, and decision support workflows.

11.13 Power & Environmental Infrastructure

11.13.1 Power Backup

Critical ICCC infrastructure shall support UPS backup, surge protection, and uninterrupted operations.

11.13.2 Environmental Controls

The ICCC shall support cooling systems, environmental monitoring, fire suppression, and operational safety systems.

11.14 Security & Access Control

11.14.1 Physical Security

The ICCC ecosystem shall support access control, visitor management, surveillance, and operational security.

11.14.2 Cybersecurity

The ICCC ecosystem shall comply with cybersecurity policies, secure access mechanisms, and operational security requirements.

11.15 Integration Requirements

The ICCC ecosystem shall support seamless integration with VMS, AI Analytics Platform, Digital Twin platform, GIS systems, communication systems, emergency systems, and approved third-party platforms.

11.16 Testing & Acceptance

11.16.1 Testing

The SI shall conduct operational testing, AV testing, failover testing, integrated dashboard testing, and operational simulation testing.

11.16.2 Acceptance Criteria

Acceptance testing shall include functionality validation, visualization validation, integration validation, and operational readiness verification.

11.17 Documentation Requirements

The SI shall provide seating layouts, rack layouts, AV architecture, network diagrams, operational manuals, SOP documents, and as-built drawings.

11.18 SLA Requirements

The ICCC ecosystem shall support:

- minimum 99.5% uptime during event period,
- uninterrupted operational monitoring,
- rapid incident handling,
- and operational continuity during major snan days.

Major snan days shall be treated as critical operational periods requiring enhanced operational readiness.

11.19 Training & Capacity Building

The SI shall provide training for ICCC operators, administrators, police personnel, and stakeholder agencies covering:

- ICCC operations,
- dashboard usage,
- incident management,
- collaboration workflows,
- and operational coordination.

11.20 OEM & Support Requirements

All ICCC components shall be OEM-backed, support enterprise-grade operations, support long-term upgrades, and provide technical support during the contract period.

OEM authorization and support commitment shall be mandatory.

11.21 Future Readiness

The ICCC ecosystem shall support future expansion, support additional integrations, support future smart city applications, and support evolving operational requirements without major redesign.

SECTION 12: FIELD INFRASTRUCTURE

12. FIELD INFRASTRUCTURE

12.1 Overview

The System Integrator (SI) shall design, engineer, supply, install, integrate, test, commission, operate and maintain all field infrastructure required for deployment and operation of the ICCC ecosystem for Simhastha 2028.

The field infrastructure shall support surveillance systems, communication network, AI analytics, Digital Twin operations, public communication systems, field connectivity, and associated operational infrastructure.

The field infrastructure shall include, but not be limited to poles and mounting structures, OFC infrastructure, field network infrastructure, power infrastructure, UPS systems, outdoor cabinets, junction boxes, civil works, earthing, lightning protection, temporary deployment infrastructure, and associated accessories.

The infrastructure shall support permanent deployment, temporary/rental deployment, high availability, operational safety, scalability, and harsh outdoor operational conditions.

12.2 Objectives

The objectives of the field infrastructure include reliable field deployment, stable communication backbone, uninterrupted surveillance operations, resilient outdoor infrastructure, rapid deployment capability, operational safety, and scalable infrastructure support.

12.3 General Requirements

12.3.1 Deployment Philosophy

The field infrastructure shall support hybrid deployment model, permanent infrastructure, temporary event-period infrastructure, modular deployment, and scalable architecture.

12.3.2 Environmental Suitability

All field infrastructure shall be suitable for outdoor operations, dust-prone conditions, high-temperature conditions, temporary event environments, and continuous operations during Simhastha period.

12.3.3 Structural Safety

All field infrastructure shall comply with structural safety requirements, electrical safety requirements, applicable standards, and operational safety practices.

12.4 Poles & Mounting Infrastructure

12.4.1 Scope

The SI shall provide poles, mounting structures, brackets, foundations, and associated accessories required for installation of cameras, communication devices, RF equipment, public communication systems, and associated field infrastructure.

12.4.2 Pole Types

The deployment may include permanent poles, temporary poles, portable poles, telescopic poles, and customized mounting structures.

12.4.3 Pole Specifications

The poles shall be industrial-grade, weather-resistant, corrosion-resistant, structurally stable, and suitable for outdoor deployment.

12.4.4 Temporary Pole Infrastructure

Temporary/rental poles shall support rapid deployment, easy relocation, stable installation, and operational flexibility during event period.

The temporary pole infrastructure shall preferably support non-intrusive or minimal civil foundation works, modular assembly, and quick dismantling after event period.

12.4.5 Pole Height & Placement

Pole heights and placement shall be based on coverage requirements, camera field of view, crowd management requirements, traffic visibility, and site conditions.

Final placement shall be approved by USCL after detailed survey.

12.4.6 Mounting Structures

The SI shall provide camera mounting brackets, PTZ mounting structures, RF antenna mounts, equipment mounting accessories, and vibration-resistant supports.

12.5 OFC Field Infrastructure

12.5.1 Scope

The SI shall provide all field-level OFC infrastructure required for connectivity of cameras, field devices, aggregation points, viewing centers, and operational nodes.

12.5.2 OFC Components

The SI shall provide OFC cables, HDPE ducts, OFC chambers, OFDFs, patch cords, splice enclosures, and associated accessories.

12.5.3 OFC Protection

The SI shall provide warning tapes, protection pipes, route markers, cable protection mechanisms, and route protection systems.

12.5.4 OFC Route Restoration

The SI shall restore roads, footpaths, pavements, and affected infrastructure after OFC deployment as per applicable standards and directions of authorities.

12.6 Field Network Infrastructure

12.6.1 Scope

The SI shall provide field-level networking infrastructure including edge switches, industrial switches, field routers, wireless devices, RF equipment, and associated connectivity infrastructure.

12.6.2 Outdoor Network Equipment

All field network devices shall be industrial-grade, weatherproof, surge-protected, and suitable for outdoor deployment.

12.6.3 Field Connectivity

The field connectivity architecture shall support OFC connectivity, RF connectivity, microwave connectivity, wireless backup, and hybrid communication architecture.

12.6.4 Redundancy

Critical field nodes shall support communication redundancy, failover capability, and alternate connectivity paths.

12.7 Power Infrastructure

12.7.1 Scope

The SI shall provide complete field-level power infrastructure required for operation of surveillance systems, field network infrastructure, public communication systems, and associated field devices.

12.7.2 Components

The power infrastructure shall include power cabling, distribution systems, field power panels, SMPS systems, protection systems, and associated accessories.

12.7.3 Power Source Coordination

The SI shall coordinate with relevant authorities/agencies for power availability, temporary power arrangements, and operational power connectivity.

12.7.4 Surge Protection

All field infrastructure shall support surge protection, voltage protection, and electrical protection mechanisms.

12.8 UPS & Backup Power Systems

12.8.1 Scope

The SI shall provide UPS and backup power infrastructure for critical field devices and systems.

12.8.2 Functional Requirements

The backup power systems shall support uninterrupted operations, temporary power failure handling, controlled shutdown, and operational continuity.

12.8.3 Backup Duration

Critical field infrastructure shall support minimum backup duration as per operational requirements and approved design.

12.8.4 Field UPS Infrastructure

The SI shall provide outdoor UPS systems, industrial batteries, enclosure protection, and monitoring capability.

12.9 Outdoor Cabinets & Junction Boxes

12.9.1 Scope

The SI shall provide outdoor cabinets and junction boxes for field deployment.

12.9.2 Requirements

The outdoor cabinets shall support equipment protection, cable management, power distribution, environmental protection, and operational safety.

12.9.3 Environmental Rating

Outdoor cabinets and junction boxes shall support weather protection, dust protection, water resistance, and operational suitability for outdoor conditions.

12.10 Earthing & Lightning Protection

12.10.1 Scope

The SI shall provide complete earthing and lightning protection systems for all field infrastructure.

12.10.2 Earthing Requirements

The earthing system shall support equipment protection, personnel safety, surge protection, and stable operations.

12.10.3 Lightning Protection

Critical field infrastructure shall support lightning arrestors, surge suppressors, and protection mechanisms.

12.11 Civil & Foundation Works

12.11.1 Scope

The SI shall undertake all civil works required for pole foundations, equipment installation, OFC route works, mounting infrastructure, and associated field deployment.

12.11.2 Restoration

The SI shall restore all affected infrastructure after completion of work.

12.11.3 Safety During Execution

The SI shall ensure barricading, public safety, traffic management, warning signage, and safe execution practices.

12.12 Temporary/Rental Infrastructure

12.12.1 Scope

The SI shall provide temporary/rental field infrastructure for event-specific deployment, temporary surveillance locations, temporary parking areas, holding areas, and surge operational zones.

12.12.2 Temporary Deployment Requirements

The temporary infrastructure shall support rapid deployment, modularity, scalability, easy relocation, and operational flexibility.

12.12.3 Dismantling & Restoration

The SI shall dismantle temporary infrastructure after completion of event period and restore affected locations.

12.13 Field Asset Management

12.13.1 Asset Tagging

The SI shall maintain asset inventory, GIS-tagged asset records, and asset management database.

12.13.2 Health Monitoring

The SI shall support monitoring of field devices, power systems, UPS systems, network connectivity, and operational status.

12.14 Integration Requirements

The field infrastructure shall support seamless integration with ICCC, VMS, AI Analytics Platform, Digital Twin platform, communication network, and approved third-party systems.

12.15 Testing & Acceptance

12.15.1 Testing

The SI shall conduct structural testing, electrical testing, OFC testing, network testing, power testing, and integrated operational testing.

12.15.2 Acceptance Criteria

Acceptance testing shall include infrastructure validation, connectivity validation, power validation, and operational readiness verification.

12.16 Documentation Requirements

The SI shall provide pole layout drawings, OFC route drawings, electrical diagrams, field infrastructure drawings, as-built documentation, GIS-tagged infrastructure records, and maintenance manuals.

12.17 SLA Requirements

The field infrastructure shall support uninterrupted operations, defined restoration timelines, rapid fault resolution, and operational continuity during major snan days.

Critical operational zones shall receive priority maintenance support during peak event periods.

12.18 Training & Knowledge Transfer

The SI shall provide training for field teams, maintenance personnel, technical teams, and authorized stakeholders covering infrastructure maintenance, fault handling, power systems, and operational safety.

12.19 OEM & Support Requirements

All field infrastructure components shall be OEM-backed where applicable, support enterprise-grade deployment, support long-term operations, and provide technical support during the contract period.

12.20 Future Readiness

The proposed field infrastructure shall support future expansion, support onboarding of additional systems, support future smart city applications, and support evolving operational requirements without major redesign.

SECTION 13: SLA & OPERATIONS AND MAINTENANCE (O&M)

13. SLA & OPERATIONS AND MAINTENANCE (O&M)

13.1 Overview

The System Integrator (SI) shall provide comprehensive Operations & Maintenance (O&M) services for all project components deployed under the ICCC ecosystem.

The O&M obligations shall include preventive maintenance, corrective maintenance, field support, application support, software support, cybersecurity support, operational support, manpower deployment, monitoring services, reporting, and SLA compliance management.

The O&M services shall cover:

- Permanent Infrastructure (CAPEX Assets),
- Temporary/Rental Infrastructure,
- ICCC operations,
- communication network,
- surveillance systems,
- AI Analytics Platform,
- Digital Twin platform,
- and all integrated systems.

13.2 O&M Period

13.2.1 Permanent Infrastructure

The SI shall provide comprehensive O&M support for all permanent infrastructure for **60 months (5 years).**

from the date of successful Go-Live / Final Acceptance Certificate (FAC), unless otherwise specified.

13.2.2 Temporary/Rental Infrastructure

The SI shall provide comprehensive O&M support for all temporary/rental infrastructure for approximately **9 months** or as directed by USCL, including:

- deployment period,
- operational period,
- peak snan operations,
- and dismantling support period.

13.3 Scope of O&M Services

13.3.1 General Scope

The SI shall provide end-to-end O&M services including monitoring, maintenance, repairs, replacement, software support, updates, fault management, incident management, and operational assistance.

13.3.2 Coverage

The O&M scope shall include:

- surveillance systems,
- VMS,
- AI Analytics Platform,
- Digital Twin platform,
- ICCC infrastructure,
- communication network,
- OFC infrastructure,
- power systems,
- UPS systems,
- field infrastructure,
- viewing centers,
- war-room infrastructure,
- and associated software/hardware systems.

13.4 O&M Responsibilities of SI

The SI shall be fully responsible for system uptime, operational continuity, preventive maintenance, fault rectification, spare management, manpower deployment, OEM coordination, cybersecurity monitoring, reporting, and SLA compliance.

13.5 Preventive Maintenance

13.5.1 Scope

The SI shall undertake scheduled preventive maintenance for all project components.

13.5.2 Activities

Preventive maintenance shall include equipment inspection, cleaning, firmware updates, health checks, configuration verification, calibration, battery inspection, and network diagnostics.

13.5.3 Maintenance Schedule

The SI shall prepare preventive maintenance schedules, inspection schedules, and maintenance records.

Preventive maintenance shall not disrupt critical operations.

13.6 Corrective Maintenance

13.6.1 Scope

The SI shall provide corrective maintenance for hardware failures, software failures, communication failures, field equipment failures, and operational incidents.

13.6.2 Replacement Responsibility

The SI shall replace defective hardware, faulty components, failed devices, and damaged equipment without additional cost during applicable O&M period, except in cases attributable to force majeure or wilful damage by third parties.

13.7 ICCC Operations Support

13.7.1 Operational Assistance

The SI shall provide operational support for ICCC operations, dashboard monitoring, surveillance operations, AI alert management, Digital Twin operations, and incident management.

13.7.2 Event-Period Operations

The SI shall ensure:

- 24×7 operational support,
- enhanced manpower deployment,
- rapid escalation,
- and operational continuity during major snan days.

13.8 Manpower Deployment

13.8.1 Manpower Requirement

The System Integrator (SI) shall deploy qualified, competent, experienced, and adequately trained personnel for successful implementation, operations, maintenance, cybersecurity management, AI analytics operations, Digital Twin operations, network management, and overall project execution.

The manpower deployed by the SI shall be dedicated for the Project and shall possess qualifications and relevant experience commensurate with the complexity and criticality of the ICCC ecosystem for Simhastha 2028.

The minimum qualification and experience requirements specified below are indicative minimum requirements and the SI shall ensure deployment of adequately skilled personnel necessary for successful and uninterrupted operation of the Project.

13.8.2 Minimum Qualification & Experience Requirements for Key Personnel

SNo.	Position	Minimum Qualification	Minimum Experience	Key Responsibilities
1	Project Director	B.E./B.Tech/MCA/M.Tech	15 Years	Overall Project Oversight
2	Project Manager	B.E./B.Tech + PMP/Prince2 preferred	10 Years	End-to-End Project Management
3	ICCC Operations Manager	Graduate/Engineer	8 Years	ICCC Operations & Coordination
4	Network & Communication Lead	B.E./B.Tech + CCNP equivalent preferred	8 Years	Network & OFC Management
5	Cybersecurity Lead	B.E./B.Tech + CEH/CISSP preferred	8 Years	Security Operations & Compliance

6	AI Analytics Lead	AI/ML/Data Science qualification	7 Years	AI Analytics Operations
7	Digital Twin/GIS Expert	GIS/Geo-Informatics qualification	7 Years	Digital Twin & GIS Operations
8	VMS Expert	Relevant certification preferred	5 Years	VMS Administration
9	Data Center/Cloud Expert	Cloud/Virtualization certification preferred	7 Years	DC/DR Operations
10	Field Deployment Lead	Diploma/B.E./B.Tech	5 Years	Field Deployment & Maintenance
11	Helpdesk/Support Engineers	Diploma/Graduate	3 Years	Incident Management
12	Field Technicians	ITI/Diploma	2 Years	Field Support
13	Shift Supervisors	Graduate/Diploma	5 Years	Shift Coordination

Authority reserves the right to interview, verify, accept, reject, or seek replacement of any proposed Key Personnel during evaluation or implementation stage.

The Authority reserves the right to seek replacement of any personnel deployed by the SI who is found incompetent, underperforming, lacking required qualifications, involved in misconduct, or unsuitable for Project operations. The SI shall replace such personnel within timelines specified by the Authority without additional cost implication.

The SI shall ensure continuity of key personnel during critical implementation and operational phases including major snan days and high-footfall periods.

13.8.3 Shift Operations

During operational period, especially major snan days, the SI shall provide:

- 24×7 shift operations,
- adequate standby manpower,
- rapid-response teams,
- and escalation support.

13.8.4 Government/User Personnel

USCL and stakeholder agencies may deploy supervisory personnel, monitoring personnel, police representatives, emergency coordinators, and operational officers for integrated operations.

The SI shall provide necessary operational support and system access to authorized personnel.

13.9 Network & OFC Maintenance

13.9.1 OFC Maintenance

The SI shall maintain OFC network, duct infrastructure, splicing, route integrity, and communication continuity.

13.9.2 OFC Restoration

The SI shall maintain dedicated restoration teams for OFC cuts, communication failures, and critical link restoration.

13.9.3 Network Monitoring

The SI shall provide centralized network monitoring, fault diagnostics, bandwidth monitoring, and proactive fault management.

13.10 Spare Management

13.10.1 Spare Inventory

The SI shall maintain adequate spare inventory for cameras, switches, storage systems, UPS systems, communication equipment, and critical components.

13.10.2 Critical Spares

Critical spares shall be maintained locally during event period for rapid restoration.

13.11 Cybersecurity Operations

13.11.1 Security Monitoring

The SI shall provide cybersecurity monitoring, threat detection, security alerting, and incident escalation.

13.11.2 Patch Management

The SI shall ensure firmware updates, security patches, vulnerability remediation, and system hardening.

13.12 Helpdesk & Support System

13.12.1 Helpdesk

The SI shall establish centralized helpdesk support for fault reporting, escalation, incident management, and operational coordination.

13.12.2 Ticketing System

The SI shall provide ticket logging, fault tracking, escalation tracking, closure records, and SLA monitoring.

13.13 SLA Parameters

13.13.1 General

The SI shall comply with all SLA requirements specified in the RFP and Contract Agreement.

SLA compliance shall be monitored continuously.

13.14 Availability Requirements

Component	Minimum Availability Requirement
ICCC Core Systems	99.5%
VMS Platform	99.5%

AI Analytics Platform	99.5%
Digital Twin Platform	99.5%
Communication Network	99.5%
Video Wall System	99.0%
Core Storage Systems	99.5%
Critical Cameras (Major Ghats)	98%
Overall Surveillance Network	97%

13.15 Incident Classification

Severity	Description	Examples
Critical	Complete failure impacting major operations	ICCC outage, major network failure
Major	Partial operational impact	Video wall failure, analytics failure
Minor	Limited operational impact	Individual camera/device failure
Low	Cosmetic/non-critical issues	Dashboard formatting issues

13.16 Response & Resolution Timelines

Severity	Response Time	Resolution Time
Critical	5 Minutes	1 Hours
Major	15 Minutes	2 Hours
Minor	2 Hours	12 Hours
Low	1 Business Day	3 Business Days

13.17 OFC Restoration SLA

Type	Restoration Timeline
Critical OFC Route	Within 2 Hours
Non-Critical OFC Route	Within 6 Hours

13.18 Peak Snan Day SLA

13.18.1 Critical Operations Period

Major snan days shall be treated as critical operational periods, zero-compromise operational windows, and enhanced SLA enforcement periods.

13.18.2 Enhanced Deployment

The SI shall deploy additional manpower, standby devices, mobile maintenance teams, rapid response teams, and OEM escalation support during major snan days.

13.19 Penalty Mechanism

13.19.1 SLA Penalties

Non-compliance with SLA requirements shall attract penalties.

The penalty framework may include uptime penalties, delayed restoration penalties, operational failure penalties, and repeated incident penalties.

13.19.2 Severe Operational Failure

Repeated critical failures, major outages, or operational negligence may attract enhanced penalties, recovery from payments, performance security invocation, or termination actions.

13.20 Reporting Requirements

13.20.1 Operational Reports

The SI shall submit daily reports, incident reports, uptime reports, maintenance reports, and SLA compliance reports.

13.20.2 Event Reports

Special operational reports shall be submitted during major snan days, emergency situations, and peak operational periods.

13.21 Asset Management

The SI shall maintain asset inventory, GIS-tagged asset records, maintenance history, warranty records, and operational logs.

13.22 Knowledge Transfer & Handover

At completion/termination of contract, the SI shall hand over configurations, documentation, licenses, operational records, asset records, and system knowledge to USCL or authorized agency.

13.23 Documentation Requirements

The SI shall maintain maintenance logs, incident records, configuration records, backup records, and operational documentation.

13.24 Audit & Performance Review

USCL may conduct operational audits, SLA audits, security audits, infrastructure inspections, and performance reviews.

The SI shall provide full cooperation during such reviews.

13.25 Exit Management

The SI shall support smooth transition, operational continuity, data migration, and knowledge transfer during contract completion or termination.

13.26 Future Readiness

The O&M framework shall support future expansion, onboarding of additional systems, evolving operational requirements, and future smart city integration needs.

SECTION 14: IMPLEMENTATION SCHEDULE & DELIVERABLES

14. IMPLEMENTATION SCHEDULE & DELIVERABLES

14.1 Overview

The System Integrator (SI) shall undertake end-to-end implementation of the ICCC ecosystem for Simhastha 2028 within the timelines prescribed in this RFP and subsequent Contract Agreement.

The implementation shall include survey, planning, design, supply, installation, integration, testing, commissioning, trial runs, Go-Live, operations, and maintenance.

The implementation schedule shall be designed to ensure:

- timely operational readiness,
- adequate stabilization period before Simhastha 2028,
- successful peak-load readiness,
- and uninterrupted operations during event period.

14.2 Implementation Philosophy

The implementation approach shall follow:

- milestone-based execution,
- phased deployment,
- integrated testing,
- operational validation,
- and progressive commissioning methodology.

The SI shall ensure:

- parallel execution of activities wherever feasible,
- coordination with multiple agencies,
- and minimal disruption to public infrastructure and city operations.

14.3 Overall Project Timelines

14.3.1 Project Duration

The implementation timeline shall broadly comprise:

- implementation phase,
- stabilization phase,
- operational phase,
- and O&M phase.

14.3.2 Tentative Timeline

The tentative implementation schedule may broadly include:

Sl. No.	Milestone	Tentative Timeline
1	Letter of Award (LoA)	T
2	Contract Agreement Signing	T + 15 Days
3	Project Kick-Off	T + 15 Days
4	Detailed Survey & Design	T + 60 Days
5	Submission of Detailed Design Documents	T + 75 Days
6	Approval of Design Documents	T + 90 Days
7	Procurement & Supply Commencement	T + 90 Days
8	Field Infrastructure Deployment	T + 180 Days
9	OFC & Network Deployment	T + 210 Days
10	ICCC Infrastructure Readiness	T + 240 Days
11	Surveillance System Deployment	T + 270 Days
12	AI & Digital Twin Integration	T + 300 Days
13	Integrated System Testing	T + 330 Days
14	Trial Runs & Operational Simulation	T + 360 Days
15	Go-Live & Operational Readiness	As directed by USCL prior to Simhastha 2028
16	O&M Commencement	Post Go-Live

The timelines may be revised by USCL depending upon project requirements and operational considerations.

14.4 Implementation Phases

14.4.1 Phase-I: Survey & Planning

The SI shall undertake:

- site surveys,
- route surveys,
- infrastructure assessment,
- camera planning,
- bandwidth assessment,
- power assessment,
- GIS mapping,
- and deployment planning.

14.4.2 Phase-II: Detailed Design & Engineering

The SI shall prepare:

- detailed architecture,
- network design,

- OFC layouts,
- field deployment plans,
- ICCC layouts,
- integration architecture,
- cybersecurity architecture,
- and implementation methodology.

14.4.3 Phase-III: Procurement & Supply

The SI shall:

- procure all approved components,
- ensure OEM authorization,
- ensure quality compliance,
- and maintain delivery schedules.

14.4.4 Phase-IV: Field Deployment

The SI shall undertake:

- OFC deployment,
- field infrastructure installation,
- pole installation,
- power infrastructure deployment,
- camera installation,
- and communication infrastructure deployment.

14.4.5 Phase-V: ICCC & Platform Deployment

The SI shall:

- establish ICCC infrastructure,
- deploy VMS,
- deploy AI Analytics Platform,
- deploy Digital Twin platform,
- and establish operational dashboards.

14.4.6 Phase-VI: Integration & Testing

The SI shall undertake:

- system integration,
- interoperability testing,
- failover testing,

- cybersecurity testing,
- and integrated operational testing.

14.4.7 Phase-VII: Trial Run & Simulation

The SI shall conduct:

- mock drills,
- operational simulation,
- crowd simulation,
- peak-load simulation,
- and emergency response testing.

14.4.8 Phase-VIII: Go-Live & Stabilization

The SI shall:

- operationalize the system,
- provide enhanced support,
- monitor stabilization,
- and rectify deficiencies before event operations.

14.5 Detailed Deliverables

14.5.1 Survey Deliverables

The SI shall submit:

- site survey reports,
- OFC route survey reports,
- GIS-tagged deployment plans,
- power availability assessment,
- and infrastructure feasibility reports.

14.5.2 Design Deliverables

The SI shall submit:

- High-Level Design (HLD),
- Low-Level Design (LLD),
- network architecture,
- cybersecurity architecture,
- storage sizing,
- compute sizing,
- rack layouts,

- and integration design documents.

14.5.3 Field Infrastructure Deliverables

The SI shall deliver:

- OFC infrastructure,
- poles and mounting structures,
- power systems,
- UPS systems,
- field cabinets,
- and associated infrastructure.

14.5.4 Surveillance Deliverables

The SI shall deploy:

- fixed cameras,
- PTZ cameras,
- panoramic cameras,
- thermal cameras,
- ANPR systems,
- drone integration,
- body cameras,
- and water surveillance systems.

14.5.5 ICCC Deliverables

The SI shall deliver:

- ICCC infrastructure,
- video wall systems,
- operator consoles,
- AV systems,
- viewing centers,
- and mini war-room infrastructure.

14.5.6 Platform Deliverables

The SI shall deliver:

- VMS platform,
- AI Analytics Platform,
- Digital Twin platform,

- GIS integration,
- dashboards,
- reporting systems,
- and workflow systems.

14.5.7 Cybersecurity Deliverables

The SI shall deliver:

- firewall systems,
- IDS/IPS,
- security configurations,
- SIEM integration,
- VAPT reports,
- and cybersecurity documentation.

14.5.8 Documentation Deliverables

The SI shall provide:

- architecture documents,
- as-built drawings,
- asset inventory,
- SOP documents,
- operational manuals,
- maintenance manuals,
- training manuals,
- and backup/DR procedures.

14.6 Project Management & Governance

14.6.1 Project Management Office (PMO)

The SI shall establish a dedicated PMO for implementation management, stakeholder coordination, schedule management, risk management, and reporting.

14.6.2 Project Manager

The SI shall deploy a dedicated Project Manager responsible for overall execution, coordination, milestone achievement, and escalation management.

14.6.3 Review Meetings

The SI shall participate in:

- weekly review meetings,
- milestone review meetings,

- coordination meetings,
- and progress review meetings.

14.7 Progress Reporting

14.7.1 Reports

The SI shall submit

- weekly progress reports,
- monthly progress reports,
- issue logs,
- risk registers,
- and mitigation reports.

14.7.2 Dashboards

The SI shall maintain project monitoring dashboards showing progress status, milestone status, risks, delays, and corrective actions.

14.8 Dependency & Coordination Management

The SI shall coordinate with USCL, District Administration, Police, utility agencies, transport agencies, and other stakeholder departments for smooth execution.

14.9 Quality Assurance & Quality Control

14.9.1 QA/QC Framework

The SI shall establish QA/QC procedures for material inspection, installation quality, testing procedures, and operational validation.

14.9.2 Inspection Rights

USCL or authorized representatives may inspect equipment, deployment sites, documentation, and testing activities at any stage.

14.10 Delay & Recovery Mechanism

14.10.1 Delay Responsibility

The SI shall be responsible for timely completion of all milestones.

14.10.2 Recovery Plan

In case of delay, the SI shall submit recovery plans, accelerated deployment plans, and corrective action measures.

14.10.3 Liquidated Damages

Delay in milestone completion may attract liquidated damages, milestone payment withholding, and other contractual remedies.

14.11 Testing & Acceptance Milestones

14.11.1 FAT

The SI shall conduct Factory Acceptance Testing (FAT) before deployment wherever applicable.

14.11.2 SAT

The SI shall conduct Site Acceptance Testing (SAT) after installation.

14.11.3 UAT

The SI shall conduct User Acceptance Testing (UAT) with USCL and authorized stakeholders.

14.11.4 Integrated Operational Testing

The SI shall conduct integrated platform testing, peak-load simulation, failover testing, and emergency response simulation.

14.12 Training Deliverables

The SI shall provide operator training, administrator training, cybersecurity awareness training, field maintenance training, and operational SOP training.

14.13 Go-Live Criteria

Go-Live shall be subject to:

- successful completion of testing,
- operational readiness validation,
- resolution of critical deficiencies,
- and approval by USCL.

14.14 Stabilization Support

The SI shall provide enhanced stabilization support after Go-Live including dedicated manpower, rapid response teams, OEM support, and operational monitoring.

14.15 Asset Handover

The SI shall submit asset inventory, GIS-tagged asset database, warranty records, license details, and ownership transfer documentation.

14.16 Exit Deliverables

Upon completion/termination of contract, the SI shall provide final documentation, operational records, backups, configurations, and transition support.

14.17 Future Scalability

The implementation architecture and deliverables shall support future expansion, onboarding of additional systems, future smart city integration, and evolving operational requirements without major redesign.

SECTION 15: ACCEPTANCE TESTING

15. ACCEPTANCE TESTING

15.1 Overview

The System Integrator (SI) shall undertake comprehensive testing, validation, simulation, trial runs, operational readiness assessment, and acceptance procedures for all components of the ICCC ecosystem before Go-Live.

Acceptance testing shall ensure that:

- all systems perform as per specifications,
- all integrations function seamlessly,
- operational objectives are achieved,
- resilience and failover mechanisms function correctly,
- and the overall ICCC ecosystem is fully prepared for large-scale event operations during Simhastha 2028.

Acceptance testing shall include:

- Factory Acceptance Testing (FAT),
- Site Acceptance Testing (SAT),
- User Acceptance Testing (UAT),
- Integrated System Testing,
- Cybersecurity Testing,
- Failover Testing,
- Stress Testing,
- Peak-Load Simulation,
- Mock Drills,
- and Operational Trial Runs.

15.2 Objectives

The objectives of acceptance testing include:

- validation of functional requirements,
- validation of technical specifications,
- operational readiness verification,
- integration validation,
- resilience validation,
- cybersecurity validation,
- and multi-agency operational preparedness.

15.3 General Requirements

15.3.1 Responsibility

The SI shall be fully responsible for preparation of test plans, test execution, coordination, rectification of defects, re-testing, documentation, and demonstration of compliance.

15.3.2 Approval

All testing procedures, simulation plans, and acceptance criteria shall be approved by USCL prior to execution.

15.3.3 Stakeholder Participation

Acceptance testing may involve participation from USCL, District Administration, Police Department, Mela Authority, Fire Department, SDRF/NDRF, Transport Authorities, and other designated agencies.

15.4 Testing Stages

15.4.1 Factory Acceptance Testing (FAT)

The SI shall conduct FAT for critical components prior to deployment wherever applicable.

15.4.2 Site Acceptance Testing (SAT)

The SI shall conduct SAT after installation and integration of systems at site.

15.4.3 User Acceptance Testing (UAT)

The SI shall conduct UAT in coordination with USCL and authorized stakeholders to validate functionality, operational workflows, dashboards, alerts, reporting, and integrated operations.

15.4.4 Integrated System Testing

The SI shall conduct end-to-end integrated testing of surveillance systems, ICCC, AI Analytics Platform, Digital Twin platform, communication network, cybersecurity systems, and all integrated applications.

15.5 Test Documentation

15.5.1 Test Plans

The SI shall prepare detailed test plans, test procedures, acceptance criteria, simulation plans, and execution methodology.

15.5.2 Test Reports

The SI shall submit test reports, defect logs, rectification reports, simulation reports, and compliance reports.

15.6 Functional Testing

15.6.1 Surveillance Testing

The SI shall test camera functionality, PTZ operations, panoramic visualization, thermal imaging, ANPR functionality, underwater surveillance, drone integration, and video quality.

15.6.2 VMS Testing

The SI shall test live monitoring, playback, recording, failover, event handling, GIS integration, and alarm workflows.

15.6.3 AI Analytics Testing

The SI shall validate crowd density analytics, people counting, reverse flow detection, queue analytics, heatmaps, intrusion detection, fire/smoke detection, and predictive alerts.

15.6.4 Digital Twin Testing

The SI shall validate GIS visualization, simulation engine, crowd forecasting, congestion prediction, evacuation modelling, and operational dashboards.

15.6.5 ICCC Testing

The SI shall validate video wall operations, operator consoles, viewing centers, mini war-room, AV systems, dashboards, and collaboration systems.

15.7 Communication Network Testing

15.7.1 OFC Testing

The SI shall conduct OTDR testing, link testing, optical loss testing, and route validation.

15.7.2 Network Testing

The SI shall validate bandwidth, latency, packet loss, redundancy, QoS, and network failover.

15.7.3 Wireless/RF Testing

The SI shall validate RF links, microwave links, wireless failover, and operational continuity.

15.8 Cybersecurity Testing

15.8.1 Vulnerability Assessment

The SI shall conduct vulnerability assessment, hardening validation, and remediation verification.

15.8.2 Penetration Testing

The SI shall conduct network penetration testing, application penetration testing, API testing, and access control validation.

15.8.3 Security Validation

The SI shall validate RBAC, MFA, encryption, secure access, audit logging, and cybersecurity monitoring.

15.9 Failover & Redundancy Testing

15.9.1 Failover Simulation

The SI shall conduct failover simulations for network failure, storage failure, server failure, communication failure, and ICCC operational failure.

15.9.2 Redundancy Validation

The SI shall validate redundancy mechanisms, automatic failover, data replication, and operational continuity.

15.10 Performance & Stress Testing

15.10.1 Load Testing

The SI shall conduct high-load testing, concurrent video stream testing, analytics load testing, and storage stress testing.

15.10.2 Peak Event Simulation

The SI shall simulate peak snan-day load conditions, surge crowd conditions, high-alert operational conditions, and emergency operational scenarios.

15.10.3 Scalability Validation

The SI shall validate scalability, concurrent user operations, system responsiveness, and operational stability under peak load.

15.11 Operational Trial Runs

15.11.1 Mandatory Trial Runs

The SI shall conduct rigorous operational trial runs prior to Go-Live.

The trial runs shall include field operations, ICCC operations, integrated monitoring, emergency workflows, and multi-agency coordination.

15.11.2 Duration

The trial run period shall be of sufficient duration as determined by USCL to validate operational readiness.

15.11.3 Operational Validation

The SI shall demonstrate uninterrupted operations, stable monitoring, operational responsiveness, and coordinated command workflows.

15.12 Simulation Exercises

15.12.1 Crowd Surge Simulation

The SI shall conduct crowd surge simulation for major ghats, congregation zones, and high-density routes.

15.12.2 Stampede-Risk Simulation

The SI shall simulate:

- reverse flow conditions,
- crowd bottlenecks,
- congestion buildup,
- and crowd diversion workflows.

15.12.3 Traffic Congestion Simulation

The SI shall simulate:

- traffic buildup,
- parking overflow,

- holding area congestion,
- and diversion planning.

15.12.4 Emergency Evacuation Simulation

The SI shall conduct evacuation drills, route optimization validation, emergency corridor testing, and safe-zone simulations.

15.12.5 Disaster Response Simulation

The SI shall simulate fire incidents, communication failures, flooding/water emergencies, infrastructure failures, and multi-location emergencies.

15.12.6 Multi-Agency Mock Drills

The SI shall coordinate and support mock drills involving:

- Police,
- Fire Services,
- SDRF/NDRF,
- Health Department,
- Administration,
- and other agencies.

15.13 AI & Digital Twin Simulation Testing

15.13.1 Predictive Analytics Validation

The SI shall validate congestion forecasting, crowd trend prediction, and predictive alert generation.

15.13.2 Simulation Accuracy

The SI shall demonstrate operational usefulness of simulations, event correlation, and actionable operational outputs.

15.13.3 Decision Workflow Validation

The SI shall validate SOP-driven alerts, escalation workflows, and automated operational recommendations.

15.14 Acceptance Criteria

15.14.1 General Criteria

Acceptance shall be based on successful completion of tests, compliance with specifications, operational readiness, and satisfactory performance during simulations.

15.14.2 Defect Rectification

All identified defects shall be rectified by the SI before final acceptance.

15.14.3 Re-Testing

USCL may require re-testing after rectification of deficiencies.

15.15 Go-Live Approval

Go-Live approval shall be granted only after successful completion of acceptance testing, successful operational simulations, satisfactory trial runs, and approval by USCL.

15.16 Final Acceptance Certificate (FAC)

FAC shall be issued only after successful completion of all testing, stabilization, operational validation, and compliance with contractual obligations.

15.17 Documentation Deliverables

The SI shall submit test reports, simulation reports, failover reports, VAPT reports, operational readiness reports, defect closure reports, and acceptance compliance documents.

15.18 Independent Verification

USCL reserves the right to appoint third-party auditors, conduct independent validation, witness simulations, and verify operational readiness.

15.19 Penalty for Failed Acceptance

Failure to achieve acceptance criteria may result in:

- delayed Go-Live approval,
- re-testing requirements,
- milestone payment withholding,
- penalties,
- or other contractual remedies.

15.20 Future Readiness Validation

The SI shall demonstrate that the system architecture supports future scalability, onboarding of additional devices, future integrations, and operational expansion without major redesign.

SECTION 16: TECHNICAL SPECIFICATIONS

16. TECHNICAL SPECIFICATIONS

16.1 Overview

This section defines the minimum functional and technical requirements for the ICCC ecosystem for Simhastha 2028.

The specifications provided herein are:

- indicative minimum requirements,
- functional in nature,
- technology-neutral wherever feasible,
- and intended to ensure interoperability, scalability, operational resilience, and enterprise-grade performance.

The bidder may propose:

- equivalent or higher specifications,
- enhanced enterprise features,
- and future-ready architecture,

subject to compliance with the minimum requirements of this RFP.

16.2 General Technical Requirements

16.2.1 Open Architecture

The proposed solution shall:

- support open standards,
- support interoperability,
- support multi-OEM integration,
- avoid vendor lock-in,
- and support future expansion.

16.2.2 Scalability

The proposed architecture shall support minimum 30% future scalability, onboarding of additional devices, onboarding of additional applications, and future smart city integrations without major redesign.

16.2.3 Environmental Suitability

All field devices and outdoor infrastructure shall be industrial-grade, weather-resistant, dust-resistant, and suitable for continuous outdoor operations.

16.2.4 Power Protection

All critical field infrastructure shall support surge protection, voltage protection, earthing, and power backup mechanisms.

16.2.5 Cybersecurity

All systems shall support secure authentication, encrypted communication, access control, audit logging, and cybersecurity hardening.

16.3 Master Compliance Matrix

16.3.1 Compliance Requirement

The bidder shall submit a detailed compliance matrix against each specification in the following format:

SNo	Specification Reference	Requirement	Compliance (Yes/No)	Offered Specification	Deviation, if any	Supporting Document Reference
1						
2						
3						
.						
.						

16.3.2 Supporting Documents

The bidder shall submit:

- OEM datasheets,
- architecture documents,
- brochures,
- certificates,
- and technical compliance documents

supporting the offered solution.

16.4 Surveillance System Specifications

16.4.1 Fixed/Bullet/Box IP Cameras

Parameter	Minimum Requirement
Camera Type	Enterprise-grade IP Camera
Resolution	Minimum 4 MP
Compression	H.264/H.265 or better
Day/Night	Supported
WDR	Supported
IR Illumination	Supported
Low-Light Performance	Supported
Analytics Support	Motion/Tamper/Event support

Protection	IP66/IP67 and IK-rated
Protocol Support	ONVIF compliant
Mounting	Outdoor suitable

16.4.2 PTZ Cameras

Parameter	Minimum Requirement
Resolution	Minimum 4 MP
Optical Zoom	Minimum 25x
Rotation	360° continuous
Auto Tracking	Supported
Preset/Tour	Supported
IR Support	Supported
Low-Light Support	Supported
Analytics Integration	Supported
Protocol Support	ONVIF compliant

16.4.3 Panoramic Cameras

Parameter	Minimum Requirement
Coverage	180°/360°
Multi-Sensor	Supported
De-Warping	Supported
Simultaneous Views	Supported
Crowd Monitoring	Supported
ONVIF Support	Mandatory

16.4.4 Thermal Cameras

Parameter	Minimum Requirement
Thermal Imaging	Supported
Optical + Thermal	Preferred
Fire/Smoke Detection	Supported
Long Range Monitoring	Supported
Outdoor Rating	Industrial grade

16.4.5 ANPR Cameras

Parameter	Minimum Requirement
Vehicle Recognition	Supported
Multi-Lane Support	Supported

Day/Night Recognition	Supported
Blacklist/Whitelist	Supported
Integration Support	VMS/GIS/AI integration
Recognition Accuracy	Enterprise-grade operational accuracy

16.4.6 Underwater & Boat Surveillance Cameras

Parameter	Minimum Requirement
Water-Resistant Operation	Mandatory
Low-Light Monitoring	Supported
Real-Time Streaming	Supported
ICCC Integration	Mandatory
Outdoor/Marine Suitability	Required

16.4.7 Body-Worn Cameras

Parameter	Minimum Requirement
Recording	Full HD
Audio Recording	Supported
GPS Tagging	Supported
Docking Support	Supported
Secure Upload	Supported
Tamper Resistance	Supported

16.4.8 Dash Cameras

Parameter	Minimum Requirement
Recording	Full HD
GPS Support	Supported
Night Recording	Supported
Storage	Secure local storage
ICCC Integration	Preferred

16.5 Video Management System (VMS)

Parameter	Minimum Requirement
Architecture	Enterprise-grade centralized VMS
Camera Scalability	Minimum 4,000 cameras
Multi-OEM Support	Mandatory
ONVIF Support	Mandatory

Live Monitoring	Supported
Playback	Supported
Edge Recording	Supported
GIS Integration	Supported
AI Integration	Supported
Failover Support	Supported
Role-Based Access	Supported
Mobile Access	Supported
Redundancy	Supported

16.6 AI Analytics Platform

Parameter	Minimum Requirement
Crowd Density Analytics	Supported
Heatmaps	Supported
Reverse Flow Detection	Supported
Queue Analytics	Supported
Intrusion Detection	Supported
Fire/Smoke Detection	Supported
Predictive Analytics	Supported
Dashboard	Supported
GIS Integration	Supported
Digital Twin Integration	Mandatory
Alert Management	Supported
API Support	Supported

16.7 Digital Twin Platform

Parameter	Minimum Requirement
GIS Visualization	2D & 3D
Real-Time Data Ingestion	Supported
Crowd Simulation	Supported
Traffic Simulation	Supported
Congestion Forecasting	Supported
Evacuation Modelling	Supported
Scenario Planning	Supported
Dashboard	Supported
API Integration	Supported

Scalability	Enterprise-grade

16.8 Communication Network Specifications

16.8.1 OFC Infrastructure

Parameter	Minimum Requirement
Fiber Type	Outdoor armoured OFC
Architecture	Ring/Dual Ring
Redundancy	Mandatory
Protection	HDPE ducts & protection
Testing	OTDR testing mandatory

16.8.2 Network Switches

Parameter	Minimum Requirement
Architecture	Enterprise-grade managed switches
Layer Support	L2/L3 as required
Redundancy	Supported
QoS	Supported
VLAN	Supported
SNMP Monitoring	Supported
Industrial Grade	For field devices

16.8.3 Wireless/RF Infrastructure

Parameter	Minimum Requirement
Point-to-Point Support	Mandatory
Redundancy Support	Mandatory
Outdoor Deployment	Supported
Secure Communication	Supported

16.8.4 Enterprise Radio / Wireless Communication System

Parameter	Minimum Requirement
digital VHF/UHF radios	Mandatory
LTE/PTT radios (optional),	Mandatory
Repeaters, base stations	Supported
dispatch console	Supported
recording	Supported
emergency SOS	Supported
battery backup	Mandatory

ruggedized handhelds	Mandatory

16.9 Data Center / Storage / DR Specifications

16.9.1 Compute Infrastructure

Parameter	Minimum Requirement
Virtualization Support	Mandatory
High Availability	Supported
GPU Support	For AI workloads
Scalability	Enterprise-grade

16.9.2 Storage Infrastructure

Parameter	Minimum Requirement
Video Retention	Minimum 60 Days
RAID Protection	Mandatory
Scalability	Supported
Redundancy	Supported
High Throughput	Supported

16.9.3 DR Infrastructure

Parameter	Minimum Requirement
Replication	Supported
Failover	Supported
Backup Integration	Supported
Recovery Workflow	Supported

16.10 ICCC Specifications

16.10.1 Video Wall

Parameter	Minimum Requirement
Enterprise Video Wall	Mandatory
Multi-Source Visualization	Supported
Redundant Controller	Supported
Dynamic Layout	Supported

16.10.2 Operator Consoles

Parameter	Minimum Requirement
24×7 Operational Suitability	Mandatory
Ergonomic Design	Mandatory

Multi-Monitor Support	Supported

16.10.3 Viewing Centers

Parameter	Minimum Requirement
Secure Connectivity	Mandatory
Dashboard Access	Supported
Live Monitoring	Supported

16.11 Cybersecurity Specifications

Parameter	Minimum Requirement
Firewall	Enterprise-grade
IDS/IPS	Supported
SIEM Integration	Supported
MFA	Supported
Encryption	Supported
Audit Logging	Supported
VAPT	Mandatory
CERT-In Compliance	Mandatory

16.12 Field Infrastructure Specifications

16.12.1 Poles & Mounting Structures

Parameter	Minimum Requirement
Outdoor Grade	Mandatory
Corrosion Resistant	Mandatory
Structural Stability	Mandatory
Temporary Deployment Support	Supported

16.12.2 Outdoor Cabinets

Parameter	Minimum Requirement
Weather Protection	Mandatory
Cable Management	Supported
Surge Protection	Supported

16.12.3 UPS Systems

Parameter	Minimum Requirement
Online UPS Preferred	Yes
Backup Support	As per approved design

Monitoring	Supported

16.13 Drone System Specifications

Parameter	Minimum Requirement
Flight Time	Minimum operational-grade duration
HD/4K Camera	Supported
GPS	Supported
Real-Time Streaming	Supported
ICCC Integration	Mandatory

16.14 GIS & Dashboard Specifications

Parameter	Minimum Requirement
GIS Dashboard	Supported
Real-Time Visualization	Supported
Multi-Layer GIS	Supported
Reporting	Supported
Mobile Compatibility	Supported

16.15 Public Communication Systems

Parameter	Minimum Requirement
VMD Integration	Supported
Public Address Integration	Supported
Emergency Alerts	Supported
Centralized Control	Supported

16.16 Environmental & Compliance Standards

All supplied systems shall comply with applicable BIS standards, safety standards, environmental standards, cybersecurity standards, and Government guidelines.

16.17 OEM Requirements

All critical systems/components shall:

- be OEM-backed,
- have proven enterprise deployments,
- support long-term support availability,
- and provide warranty/support commitments.

16.18 Warranty Requirements

The SI shall provide OEM warranty, software support, firmware updates, and technical support as per contract requirements.

16.19 Future Readiness

The proposed solution shall support future scalability, future integrations, additional analytics modules, additional devices, and evolving smart city operational requirements without major redesign.

SECTION 17: DETAILED TECHNICAL SPECIFICATIONS OF MAJOR ITEMS

The detailed technical specifications provided in this section have been prepared based on the current market assessment, prevailing industry standards, operational requirements, and envisaged technological requirements of the Ujjain Simhastha ICCC Project. The specifications primarily cover major and critical system components/items identified at this stage.

For ancillary, supporting, minor, or any other items/components for which detailed specifications are not explicitly provided in the RFP, the Selected Bidder/Implementation Agency (IA) shall propose appropriate, state-of-the-art, interoperable, and industry-standard specifications, duly aligned with the intended functional requirements, system performance, scalability, reliability, cybersecurity, and overall project objectives.

All such proposed specifications, makes/models, architecture, and technical configurations shall be submitted to Ujjain Smart City Limited (USCL) for review and approval prior to procurement, deployment, and implementation. USCL reserves the right to seek modifications, enhancements, or alternative specifications in the interest of overall system performance, standardization, future scalability, operational efficiency, and integration requirements. The decision of USCL in this regard shall be final and binding on the Implementation Agency.

Specification Precedence

In the event of any discrepancy, ambiguity, inconsistency, conflict, or variation between the brief specifications, indicative descriptions, bill of quantities, scope of work provisions, functional requirements, drawings, schedules, or any other references provided elsewhere in the RFP document and the Detailed Technical Specifications section, the specifications and requirements provided under the Detailed Technical Specifications shall prevail and be considered binding.

However, if any higher specification, functionality, performance parameter, interoperability requirement, statutory compliance, cybersecurity requirement, or operational requirement is mentioned elsewhere in the RFP, the same shall also be deemed applicable and shall be complied with by the Implementation Agency without any additional cost implication to Ujjain Smart City Limited (USCL). The decision of USCL in interpretation of such specifications and applicability shall be final and binding on the bidder/Implementation Agency.

Generic OEM Eligibility, Security Compliance & Government Procurement Restriction Clause

“Unless specifically exempted or otherwise stated, all OEMs proposed for hardware, software, networking, surveillance, cybersecurity, ICCC, communication, field infrastructure, cloud, data center, and associated ICT components under this project shall comply with the following minimum eligibility, security, and regulatory requirements:

1. OEMs shall be established and reputed manufacturers/developers with proven experience in supply, deployment, integration, commissioning, and support of similar technology solutions in India and/or globally.
2. OEMs shall preferably have direct presence in India through registered office/subsidiary/authorized support structure and shall provide adequate technical support, warranty, firmware/software updates, patches, and after-sales services during the entire contract period.

3. All supplied products/components shall be genuine, new, current-generation, interoperable, industry-standard, and compliant with applicable technical standards, cybersecurity requirements, and interoperability protocols mentioned in the RFP.
4. OEMs/products shall possess relevant quality, security, environmental, telecom, and manufacturing certifications, wherever applicable, such as ISO 9001, ISO 14001, ISO 27001, ISO 45001, CE, RoHS, BIS, STQC, TEC, FCC, UL, ONVIF, IEC standards, and other statutory certifications applicable for the respective product category.
5. All proposed ICT systems, applications, software, firmware, network devices, surveillance systems, servers, storage, cloud infrastructure, and cybersecurity solutions shall comply with applicable guidelines/advisories/frameworks issued by MeitY, CERT-In, National Critical Information Infrastructure Protection Centre (NCIIPC), Ministry of Home Affairs (MHA), and Government of India from time to time.
6. The proposed systems shall support secure architecture and cybersecurity best practices including, but not limited to:
    - Role-based access control (RBAC)
    - Secure authentication and password policies
    - Encryption for data in transit and at rest
    - Secure APIs and interoperability interfaces
    - Logging and audit trail mechanism
    - Patch and vulnerability management
    - Malware/ransomware protection
    - Secure remote access mechanisms
    - Time synchronization and log retention
    - Network segmentation and device hardening
    - Compliance with applicable CERT-In advisories and cybersecurity directions
7. All products/equipment/software shall be free from known malicious code, unauthorized remote access/backdoors, unsupported firmware, prohibited components, and cybersecurity vulnerabilities that may compromise national security, public safety, or ICCC operations.
8. The bidder/Implementation Agency shall submit OEM authorization certificates, technical datasheets, compliance sheets, cybersecurity compliance documents, test certificates, and other supporting documents as sought by Ujjain Smart City Limited (USCL) during technical evaluation or project implementation.
9. USCL reserves the right to seek additional certifications, security audit reports, proof of deployments, interoperability demonstrations, vulnerability assessment reports, source declarations, or replacement of OEM/products in case the proposed solution is found unsuitable from operational, cybersecurity, interoperability, performance, lifecycle support, or national security perspective.

10. Wherever detailed OEM-specific criteria are not separately mentioned for individual items/components, this generic OEM eligibility and compliance clause shall be considered applicable.
11. As per Rule 144 (XI) of General Financial Rules (GFR), 2017, notwithstanding anything contrary contained in these Rules, Department of Expenditure may, by order in writing, impose restrictions, including prior registration and/or screening, on procurement from bidders/OEMs/suppliers/third-party OEMs from a country or countries, or a class of countries, on grounds of defence of India, or matters directly or indirectly related thereto including national security; and no procurement shall be made in violation of such restrictions. The bidder shall ensure compliance with all such orders, guidelines, notifications, and amendments issued by Government of India from time to time.
12. The bidder/Implementation Agency shall ensure that all proposed OEMs, associated OEMs, cloud/service providers, software providers, and supply chain partners comply with prevailing Government of India procurement restrictions, cybersecurity directives, trusted source requirements, and national security related advisories applicable at the time of bidding as well as during the contract period."

Index for Ujjain Simhastha ICCC Specifications

SNo	Component
Group-1: Field Infrastructure & Passive Components	
1.	Junction Box with Chemical Earthing
2.	Cat-6 Cable (Armoured) Outdoor
3.	12 Core SM Outdoor Armoured Cable (Aerial Application)
4.	24 Core SM Outdoor Armoured Cable
5.	Fiber LIU for Fiber Termination Point
6.	Patch Cord, LC-LC Duplex SM
7.	19” 1U 24 Port Patch Panel
8.	Cat 6 UTP RJ45 Keystone Jack
9.	Cat 6 Patch Cord
10.	Cat6 UTP Field Termination Plug
11.	Poles
12.	42U Network Rack
13.	22U Network Rack
Group-2: Power Infrastructure & Electrical Systems	
14.	Field UPS
15.	Viewing Center UPS
16.	DC UPS
17.	DR UPS
18.	DG Set (250 kVA)
Group-3: Surveillance & Field Devices	
19.	Fixed Camera
20.	PTZ Camera
21.	ANPR Camera
22.	Panoramic Camera
23.	Thermal Camera
24.	Body Worn Camera Solution
25.	Dashboard Camera Solution
26.	Drones
27.	Local Processing Unit (LPU)
Group-4: Public Safety, Communication & Emergency Systems	
28.	Emergency Call Box (ECB)
29.	PAS Amplifier

30.	PAS Horn Speaker
31.	Digital Handheld Wireless Sets
32.	ECB & PA Control Desk Call Station
33.	IP Phones
34.	Public Address System (PAS)
35.	Dispatcher Subscription
Group-5: Network & Communication Infrastructure	
36.	Core Router
37.	Core Switches
38.	L3 Managed Distribution Switch
Group-6: Cyber Security Infrastructure	
39.	Firewall
40.	WAF & Server Load Balancer
41.	DDOS Protection
42.	Network Intrusion Detection System (IDS)
43.	Security Information & Event Management (SIEM)
Group-7: ICCC & Control Center Infrastructure	
44.	Integrated Command & Control Center (ICCC) Platform
45.	Enterprise Management System (EMS)
46.	Videowall
47.	Workstations
48.	Keyboard Joystick for PTZ
49.	LED TV 55”
Group-8: Data Center, Servers & Storage Infrastructure	
50.	Application & Failover Application Server
51.	Recording Server
52.	Analytics Server
53.	Data Lake Server
54.	Digital Twin & GIS Server
55.	PA System ECB Server
56.	ITSM Server
57.	Database Server
58.	SAN Storage
59.	NAS Storage

60.	Tape Library
61.	Backup Solution
Group-9: Video Management, Analytics & AI Applications	
62.	Video Management System (VMS)
63.	Video Summarization
64.	AI Based Video Analytics
65.	Facial Recognition System
66.	ANPR & Vehicle Detection
Group-10: Smart Mobility, GIS & Digital Platforms	
67.	ITMS Application
68.	Geographic Information System (GIS)
69.	Data Lake & Analytics
70.	Digital Twin for Kumbh Area
71.	Mobile App for Pilgrims / Visitors

Group 1: Field Infrastructure & Passive Components

SNo.	Parameter	Specifications	Compliance (Yes/No)
1.	**Junction Box Ground Mounted**		
1	Make		
2	Model	As per approved design & drawings	
3	Cabinet Material	CRCA Sheet, having thickness from 1.2mm to 1.6 mm, Surface Powder Coated with PP Powder.	
4	Structure	Rigid enclosure with base frame suitable for ground mounting on concrete foundation	
5	Rack Provision	20U rack with minimum load bearing capacity of 40 kg	
6	Protection	IP55 certified enclosure with protection against dust and water splashes	
7	Locking System	Heavy-duty compression lock, tamper-resistant, metal handle/lever	
8	Mounting	Ground mounted on concrete base with proper anchoring arrangement	
9	Mounting facilities	Integrated mounting provision for CCTV cameras, junction box for IT components, and meter box. Camera bracket to be adjustable for angle/focus.	
10	Internal Arrangement	DIN rail / rack mounting, cable management, earthing stud	
11	Cable Entry	Bottom/side entry with weatherproof cable glands	
12	Accessories	Earthing provision, cooling fan/ventilation, rain canopy (if required)	
13	Surface Finish	Outdoor grade anti-corrosive powder coating, UV resistant	
14	Logo/Marking	Customer logo embossed / sticker on front panel	
2.	**Cat 6 Outdoor Armoured Cable**		
1	Category	Suitable for 1GBASE-T with Min. 250Mhz of Bandwidth	
2	Cable	4 Twisted Pair alongside PE / PVC Cross Separator	
3	Conductor	Conductor: 23AWG Solid Annealed Bare Copper	
4	Insulation	Insulation: High Density Polyethylene, Diameter 1.0 ± 0.05mm	
5	Inner Jacket	LSZH	
6	Armour	Armor : ECCS Corrugated Tape, >= .125mm	
7	Outer Jacket	UV Resistant & Anti-Rodent HDPE Outer Jacket	
8	OD	Cable Outer Diameter: 10.0 ± 0.3 mm	
9	Temp	Operating Temperature: -20°C to +70°C	
10	Bend Radius	Bend Radius: 20 X Cable Diameter (Min.) or Better	

SNo.	Parameter	Specifications	Compliance (Yes/No)
11	Electrical	Conductor Resistance : £ 9.38 Ω /100m	
12	Electrical	Resistance Unbalance : 5% Max	
13	Electrical	Mutual Capacitance : ≤ 5.6nF/100m	
14	Pulling Force	Should have Pulling force of 50Kg.	
15	Standards	IEC 60332-1	
16		IEC 60754, IEC 61034	
17	ROHS	RoHS Complied	
3.	**12 Core SM outdoor Armoured Cable**		
1	Core	12F SM OFC (6 Tube x 4 Core F/T)	
2	ITU-T Standards	OFC Cables must be as per the ITU-T standard G.652D Fibre -Armoured Optical Fibre Cable.	
3	Attenuations	0.23 dB / KM @1550nm for each individual Fibre. AND 0.36 dB / KM @1310nm for each individual Fibre.	
4	Bending-loss performance of optical fiber @1310nm&1550nm	≤0.05dB (100 turns around a mandrel of 50mm diameter)	
5	Tensile strength:	The cable shall withstand a load of value ≤ 9.81 x 2.5 x W Newton, where 'W' is the weight of 1Km of the cable and the strain ≤ 0. 25 % (4000N)	
6	Construction	Fiber cable Single Mode Suitable for Arial application. Fiber optimized for operation at 1310 nm & at 1550 nm. Fiber type 9/125 / G.652D & Refractive Index 1.4670/1.4675. Cable will be with two Jacket - Inner HDPE Sheath (Thickness => 1.2mm and Outer HDPE sheath => 1.6mm	
7	Construction	Armouring with Aramid Yarn. Steel Tape Armoured in between Inner & Outer sheath with Thickness of 0.15mm. Jacket Material HDPE Black	
8	Central Strength Member	FRP Rod (2.0 +/- 0.1mm)	
9	Fiber count /Tube	12F - 6Tubes *2 Fiber	
10	Crush load:	The cable shall sustain a compressive load of 4 KN/100x100mm.	
11	Cable Diameter	<= 16.0 ± 3.0 mm	
12	Cable weight (kg/km)	200 ± 50 kg	
13	Water penetration:	IEC 60794-1-2 F5	
14	Operating Temperature	-20°C~+70°C	
15	Cable bend:	Minimum-bending radius will be 20D, where 'D' is outer dia of the cable.	
16	Standards	Standard ISO 11801, IEC 60793-1/60794-1-2 & ITU-T-REC G.652D	

SNo.	Parameter	Specifications	Compliance (Yes/No)
17	PMD & CD	The manufacturing PMD and CD values should be as per the standards.	
4.	**24 Core SM outdoor Armoured Cable**		
1	Core	24F SM OFC (6 Tube x 4 Core F/T)	
2	ITU-T Standards	OFC Cables must be as per the ITU-T standard G.652D Fibre -Armoured Optical Fibre Cable.	
3	Attenuations	0.23 dB / KM @1550nm for each individual Fibre. AND 0.36 dB / KM @1310nm for each individual Fibre.	
4	Bending-loss performance of optical fiber @1310nm&1550nm	≤0.05dB (100 turns around a mandrel of 50mm diameter)	
5	Tensile strength:	The cable shall withstand a load of value ≤ 9.81 x 2.5 x W Newton, where 'W' is the weight of 1Km of the cable and the strain ≤ 0. 25 % (4000N)	
6	Construction	Cable will be with two Jacket - Inner HDPE Sheath (Thickness => 1.2mm and Outer HDPE sheath => 1.6mm	
7	Construction	Steel Tape Armoured in between Inner & Outer sheath with Thickness of 0.15mm	
8	Central Strength Member	FRP Rod (2.0 +/- 0.1mm)	
9	Fiber count /Tube	24F - 6Tubes *4 Fiber	
10	Crush load:	The cable shall sustain a compressive load of 4 KN/100x100mm.	
11	Cable Diameter	<= 16.0 ± 3.0 mm	
12	Cable weight (kg/km)	200 ± 50 kg	
13	Water penetration:	IEC 60794-1-2 F5	
14	Operating Temperature	-20°C~+70°C	
15	Cable bend:	Minimum-bending radius will be 20D, where 'D' is outer dia of the cable.	
16	Standards	IEC60794-1 IEC11801 IEC60332-1-2	
17	PMD & CD	The manufacturing PMD and CD values should be as per the standards.	
5.	**Fiber LIU for Fiber termination**		
1	Panel	Fiber optic patch panel : Fiber optic patch panel should have provision for 48 fiber in 1U size.FMS Termination Drawer should have sufficient slots to accommodate 3 of 12/16 Port LC Adaptor Plates.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
2	Style	Should have Slide type drawer structure	
3	Height	Height: 1 U, 1.75 inches (12 and 48 Ports)	
4	Materail	Material: Cold Rolled Steel in surface coated by electrostatic epoxy powder	
5	Slots	Slots: FMS should have sufficient slots to accommodate adaptor plates	
6	Slots	Empty Slots of FMS should be covered with blank plates.	
7	Splice Tray	Splice Tray : Splice Tray of ABS, Comply with UL 94V2 material should be supplied with LIU.	
8	Port	24 Duplex LC Port for 48F (8Duplex per adapter Plate * 3)	
9	Adapter	The adaptor plate should be pre-loaded with LC/SC Type Single mode Duplex Adaptors.	
10	Density	Port Density :12/16 LC/SC Single mode Ports	
11	Adapter	All LC adapters should be duplex type with shutter for protection. Adapters should be snap mount for easy insertion and removal.	
12	Loss	Insertion Loss: <0.2 to <0.1 dB	
13	Compliant	Compliance RoHS Compliant	
14	Testing	Must be tested for Shall be tested for Corrosion as per ASTM B117: 2019. (Relevant Document to be shared) by NABL Lab	
6.	**Patch Cord, LC LC, Duplex, SM, Bend Insensitive G657, PC, LSZH**		
1	Cable	Cable : LC-LC 9/125µm OS2 Singlemode Duplex Patch Cord Length : 3mtrs	
2	Connectors	Connectors : The optical fiber patch leads shall comprise of Single mode 9/125µm fiber with 2XLC type fiber connectors terminated at each end of fiber patch cord.	
3	Insertion	Insertion loss should be better than 0.30 dB	
4	Jacket	Jacket Material : LSZH complying to IEC 61034-1 & 2,IEC-60332-3C, IEC-60754-2	
5	Attenuation	Attenuation: 1310/1550 : 0.36/0.22 dB/KM	
6	Connector	Connector Loss : 0.30dB(max)	
7	Temp	Operating Temperature : -40°C to +75°C	
8	Certificate	Tested by NBAL / BIS lab for LSZH and OEM Name shall be printed on the Patch Cord Cable.	
9	Length	Must be available in 3mtr / 5mtr and 10 mtr or as per BOQ required length	

SNo.	Parameter	Specifications	Compliance (Yes/No)
7.	**19" 1U 24 port unshielded Patch Panel**		
1	Panel	Patch panel should be modular design, populates up to 24 UTP keystone-type jacks in 1U	
2	Tray	Patch panel should be Enhanced with cable strain relief with retention tray; It should be single metal both front panel and rear tray	
3	Material	Material: sub-rack made of Aluminium with dimension 44.4 mm : 482.6 mm : 105 mm (h:w:d) tray	
4	IO	Information Outlet or connecting module should comply with the specification mentioned above in 2	
5	Standard	Standard : Conforms to IEC-60603-7 (603-7) for keystone-type, snap-on apertures	
6	RoHS	Should be RoHS complied	
7	UTP and STP	Panel must be able to fit UTP as well as STP jacks. Must have grounding provision / wire with the panel	
8	Testing	Must be tested for Shall be tested for Corrosion as per ASTM B117: 2019. (Relevant Document to be shared) by NABL Lab	
9	Certification	ETL 4 connector test report needed for 100mtr as well as for short ditance i.e 15mtr 4 connector test report by ETL. Must include Zero Bit error Test report.	
10	UL	Must be UL Listed	
8.	**Cat 6 UTP RJ 45 Keystone Jack**		
1	Jack	RJ45 Jack of Category 6, for the establishing of transmission channels of class E with up to 4 plugged connections, complies with Category 6 requirements of the standards ISO/IEC 11801:2nd edition, EN 50173-1, DIN EN 50173-1: 2002 as well as ANSI/TIA/EIA 568-B.2-1, de-embedded tested in acc. with IEC 60603-7 (603-7), interoperable and backwards compatible with Cat.5e and Cat.5.	
2	Application	Simple labor -saving termination using standard 110 Block termination and Krone tools	
3	Compatible	Compatible with RJ standard plugs (RJ11, RJ12, RJ45), PCB- and tool based connection of installation cables AWG 26 – 23 and flexible cables AWG 26/7 – AWG 24/7.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
4	IDC	IDC termination should feature nil crossover in acc. with EIA/TIA 568-A/B, gold-plated bronze contacts for >750 mating cycles, >200 insertion cycle	
5	Material	Material: RoHS complied	
6	Hosing	Housing material: Polycarbonate (UL-94-V0)	
7	Dust Protection	Should be available with or without dust protection feature	
8	Certification	ETL 4 connector test report needed for 100mtr as well as for short ditance i.e 15mtr 4 connector test report by ETL. Must include Zero Bit error Test report.	
9	UL	Must be UL Listed	
9.	**Patch Cord, U/UTP 4P, Cat.6, length 1/ 2**		
1	Standard	Standardization: Compliant with Cat.6, Class E requirements: ISO/IEC 11801 2nd Edition Compliant with Cat.6 component standards IEC 60603-7-4 and 60603-7-5	
2	Type	Cable shield: U/UTP	
3	Conductors	Number of conductors : 8	
4	Guage	Stranding: 7 x 0.19 mm (24 AWG)	
5	Jacket	Cable jacket characteristics: cable, metal-free	
6	OD	Cable overall diameter: 6.0 ±0.3 mm	
7	Wire	Tube / Wire type: stranded conductor	
8	Insulation	Insulation: solid polyolefin, 0.8 ±0.03 mm diameter	
9	Plug	Plug: Feature cable retension, with enhanced pull strength.	
10	Tensile Strength	Min. 1.6Kgf/mm²	
11	Type	Cat 6 patch cord plug to have round cable holder and strain relief boot to avoid bending.	
12	Jacket	Jacket: LSZH with 8 different color options	
13	Certificate	Jacket must be tseted by NABL/ BIS certfied Lab. Report Mandatory	
14	Plug	Plug should have high repeatability cross talk performance	
15	UL	Must be UL Listed	
16	Testing	Patch Cord must be tested for Anti Bacterial - NABL test report mandatory as per ISO 22196:2011	
17	Certification	ETL 4 connector test report needed for 100mtr as well as for short ditance i.e 15mtr 4 connector test report by ETL. Must include Zero Bit error Test report.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
10.	**Cat6 - UTP Field Termination Plug**		
1	Category	Standardization: Compliant with Cat.6 requirements: ISO/IEC 11801 2nd Edition backward Compliant with Cat.6 component standards IEC 60603-7-4 and 60603-7-5 . Rotatable Plug	
2	Type	Cable: UTP - Short plug with Rotation plug for better fitment.	
3	Conductors	Number of conductors : 8	
4	IDC	Termination: IDC type Tool less	
5	Contact Finish	Contact Finish: 50µ gold plated on plug contact area	
6	Contact	RJ45 Plug contacts: Phosphor bronze with 100µ nickel plated	
7	Wire	Plastic Wire Organizer: PC, Color: White, UL 94V-2	
8	Durability	IDC Durability: ≥20 Termination cycles	
9	Jack Durability	RJ45 Jack Durability: ≥750 Plug-Jack mating cycles per IEC 60603-7-81	
10	Temperature	Operating Temperature: -10 degree C to +60 degree C	
11	Cord retention	Patch Cord retention strength: 7.7 Kg Max. according to IEC 60603-7-5	
12	Plug Insertion	Rj45 Plug Insertion force: 3.1 Kg Max according to IEC 60603-7-81	
13	ROHS	RoHS Complied	
11.	**Poles**		
1	Make		
2	Model	As per approved design & drawings	
3	Pole type	Tubular pole with foundation bolts after fabrication, hot-dip galvanized.	
4	Height	For Surveillance: **6** meters (clear height) For ANPR: 7 meters (clear height)	
5	Pole Diameter	Diameter should be min 114.3 OD, with Min thkness 4mm	
6	Design	Pole and its accessories shall be designed in such a way that it should withstand a windspeed of 140/kmph. Structural stability certification to be provided by recognized third party consultant (to be Government approved by Purchaser)	
7	Cantilever Arm Length	1.5 meter / 3 meter as per site condition and approved drawing	
8	Base Plate & Foundation	Base plate minimum size **300 mm × 300 mm × 16mm** Thk	

SNo.	Parameter	Specifications	Compliance (Yes/No)
9	Galvanising	Hot Dip Galvanising on poles and cantilever should be as per IS:2629.1985 & IS 4759, Min DFT should be 80Mic.	
10	Mounting facilities	Integrated mounting provision for CCTV cameras, junction box for IT components, and meter box. Camera bracket to be adjustable for angle/focus.	
11	Cable Routing	All wiring must be Concealed/hidden, through HDPE/DWC/tubes/pipes. No wires shall be visible from outside.	
12	Foundation	Casting of Civil Foundation with foundation bolts, to ensure vibration free erection. Expected foundation depth as per site conditions.	
13	Protection	Lightning arrester shall be provided, to protect all field equipment mounted on pole.	
14	Earthing	Proper earthing provision shall be provided for pole and mounted equipment, Min depth of 1Mtr.	
15	Testing and certificati on	All poles shall be factory load tested and supplied with compliance certificates	
16	Sign Board & Number plates	A sign board describing words such as “This area under surveillance” and with serial number of the pole.	
17	Standards	Fabrication, welding, and coating as per relevant IS standards	
12.	**42U Network Rack**		
1.		Rack should be floor Mount 42U RACK (UL Certified or equivalent) (All Racks should be from same OEM)	
	Rack Size		
2.		Floor Mount 42U - 800 W x 1000 D for Network and 600 W x 1200 D or higher for large servers and storages.	
	Accessories		
3.		1U Horizontal Cable Manager	
4.		FHU with 4 FAN 360CFM	
5.		Vertical Power Distribution Unit with 12 x 5/15 sockets Round Pin, 230 Volts AC, 32 Amp with Plug	
6.		Mounting Hardware Kit (Pack of 20)	
7.		Vertical Cable Manager-42U-Loop	
8.		Casters Set of 4	
9.		Adjustable Levellers set of 4	
10.		19" Reduced Channel - Loop Type	
11.		Front side - Hexagonal Perforated Single Door-42U	

SNo.	Parameter	Specifications	Compliance (Yes/No)
12.		Rear side- Hexagonal Perforated Dual Door-42U	
13.		Side Panels - Vented Side Panels-42U (Set of 2)	
	Features		
14.		Conforms to Standards	
15.		Powder Coated Steel Frame Welded Construction	
16.		Equipment Mounting on DIN Standard 10sqmm Slots / Direct M6 Tap	
17.		Mounting Angle should be 19" Mounting angle made of formed steel	
18.		Vented and Cable entry/exit cut outs from Top & Bottom	
19.		Static Load should be 750 kgs or better.	
20.		Depth adjustable mounting slots	
21.		Provision to mount the cooling fans on the top panel.	
13.	22U Network Rack		
1		Rack should be Floor Mount 22U Rack (UL Certified or equivalent)	
	Rack Size		
2		Floor Mount 22U – 600 W x 800 D / 1000 D suitable for Network, Server and Storage applications	
	Accessories		
3		1U Horizontal Cable Manager	
4		FHU with 2 / 4 FAN Cooling Unit	
5		Vertical Power Distribution Unit with minimum 6 / 8 sockets, 230V AC	
6		Mounting Hardware Kit (Pack of 20)	
7		Vertical Cable Manager – 22U	
8		Casters Set of 4	
9		Adjustable Levellers Set of 4	
10		19" Mounting Channels	
11		Front Side – Hexagonal Perforated Lockable Door	
12		Rear Side – Perforated / Dual Split Rear Door	
13		Side Panels – Removable / Lockable Side Panels	
	Features		
14		Conforms to International Standards	
15		Powder Coated Steel Welded Construction	
16		Equipment Mounting on DIN Standard Slots / M6 Mounting	
17		Standard 19" Rack Mounting Angle	
18		Top & Bottom Cable Entry / Exit Provision	
19		Static Load Capacity minimum 300 kg or higher	

SNo.	Parameter	Specifications	Compliance (Yes/No)
20		Depth Adjustable Mounting Slots	
21		Provision to mount Cooling Fans on Top Panel	

Group 2: Power Infrastructure & Electrical Systems

SNo.	Parameter	Specifications	Compliance (Yes/No)
14.	**Field UPS (True Online)**		
1.	INPUT		
2.	Acceptable Input Voltage	100VAC-300VAC	
3.	Phase	Single phase with ground	
4.	Transfer Voltage Range (low load)	100VAC-300VAC (50% load)	
5.	Transfer Voltage Range (100% load)	160VAC-300VAC	
6.	-Line low loss	160VAC/100VAC (±3%)	
7.	-Line low comeback	170VAC/110VAC (±3%)	
8.	-Line high loss	300VAC (±3%)	
9.	-Line high comeback	290VAC (±3%)	
10.	Nominal input current (r.m.s) @ 230V input and battery fully recharged	3.95A	
11.	Inrush Current Limit	8*Irms	
12.	THDi	<9% with R full load @ 230V input	
13.	Input Power Factor	≥0.99(R FULL LOAD) @ 230V input	
14.	Input Frequency Range	45-55Hz / 54-66Hz	
15.	Input protection	Breaker	
16.	OVCD	Withstand 440Vac, 24Hours	
17.	Generator Set	2.2 x UPS Rating Power	
18.	OUTPUT		
19.	Output Power(VA) max	1000	
20.	Output Power(W) max	800	
21.	Output Power Factor	0.8	
22.	Output Waveform	Pure sine wave	
23.	Output nominal voltage	200VAC/208VAC/220VAC/230VAC/240VAC	
24.	Output Voltage Variation	± 1 %	
25.	Output Transient recovery	100ms (IEC 62040-3 Non-linear load)	
26.	Output Voltage distortion	< 3% THD, linear load@Line mode < 3% THD, linear load @ battery mode, battery voltage 12V / per battery	
27.		< 7% THD, non-linear load@line mode < 7% THD, non-linear load @ battery mode, battery voltage 12V / per battery	
28.	Output Frequnecy in inverter mode Synchronization range	45-55Hz / 54-66Hz	

SNo.	Parameter	Specifications	Compliance (Yes/No)
29.	Output Frequency Slew rate	1 Hz/s	
30.	Output Frequency in Battery mode	(50/60±0.05) Hz	
31.	Transfer time Inverter Mode to Battery Mode.	0ms	
32.	Transfer Time Inverter Mode to Bypass Mode.	4ms	
33.	Line mode efficiency @ full load with battery fully charged	>88%	
34.	ECO mode efficiency @ full load with battery fully charged	>97.35%	
35.	Battery mode efficiency @ full load 12Vdc/Battery	>85%	
36.	Overload Capability (Line mode)	100%～105% :Constant 105%~130% :60s 130%~150% :10s >150% :300ms	
37.	Overload Capability (Battery mode)	100%～105% :Constant 105%~130% :10s 130%~150% :1s >150% :300ms >105% and Vbat<10.5V: 300ms	
38.	BATTERY		
39.	DC Voltage	36VDC	
40.	Battery-Low Voltage(full load)	33.6VDC, 11.2V/pcs	
41.	Battery shutdown voltage @ 0 ～ 20% Load (for long run model) / 0~ 30% (for standard model)	33VDC, 11V/pcs	
42.	Battery shutdown voltage @ 20 ～ 70% Load (for long run model) / 30%~70% load (for standard model)	31.5VDC, 10.5/pcs	
43.	Battery shutdown voltage @ > 70% Load	30VDC, 10V/pcs	
44.	Charger Current	10A (2/4/6/8/10A adjustable)	
45.	Leakage current	<300uA	

SNo.	Parameter	Specifications	Compliance (Yes/No)
46.	FEATURES		
47.	ECO Mode	YES	
48.	EPO Function	NA	
49.	Battery Capacity Calculation	YES	
50.	Fan Speed Control	YES	
51.	Frequency Converter Mode(CVCF)	YES, 60% load	
52.	INTERFACE		
53.	RS232	Yes	
54.	USB	NA	
55.	COM Slot	YES	
56.	NMC card	Optional	
57.	AS400 card (Dry contact card)	Optional	
58.	Modbus card	Optional	
59.	Input connection	input powercord 6A	
60.	Outlet socket	3 x IEC 10A outlets	
61.	MECHANICAL		
62.	WxHxD (mm)	102X228X346	
63.	Net Weight	3.8Kg	
64.	Operating Temperature Range	0°C ~ 40 °C	
65.	Relative Humidity	0 ~ 95% (No condensing)	
66.	Audible Noise	≤45dB at front 1m	
67.	REGULATIONS		
68.	-ESD	IEC 61000-4-2 Level 3	
69.	-RS	IEC 61000-4-3 Level 3	
70.	-EFT	IEC 61000-4-4 Level 4	
71.	-Surge	IEC 61000-4-5 Level 4	
72.	-Safety	BIS	
73.	-Transportation	ISTA 2A	
74.	-Protection	IP20 (static)	
75.	ACCESSORIES		
76.	User manual	Yes	
77.	External battery power cord	NA	
78.	EMC		
79.	Conduction	NA	
80.	Radiation	NA	

SNo.	Parameter	Specifications	Compliance (Yes/No)
81.	Low frequency conducted disturbances	Criteria A Ref Std : IEC61000-2-2:2002	
82.	Harmonic current	Class A Ref Std :IEC 61000-3-2:2014	
83.	ESD	Criteria B, Level 3 Ref Std : IEC 61000-4-2:2008	
84.	RS	Criteria A, Level 3 Ref Std IEC 61000-4-3:2006+AMD1:2007+AMD2:2010 CSV	
85.	EFT	Criteria B ,Level 4 Ref Std :IEC 61000-4-4:2012	
86.	Surge	Criteria B, DM Level 3: 2KV, CM Level 4: 4KV Ref Std : IEC 61000-4-5:2014	
87.	C/S	Criteria A, level 3 Ref Std : IEC61000-4-6:2013	
88.	M/S	Criteria B, level 4 Ref Std : IEC61000-4-8:2009	
89.	Voltage Dips, short interruptions and voltage variations	Criteria B ,Level 4 Ref Std : IEC61000-4-11: 2004	
90.	Certificate	BIS	
15.	**Viewing Center UPS**		
1	Capacity (in kVA)	3kVA Online UPS, 1-Phase Input / 1-Phase Output	
2	Technology and Capability	True Online Double Conversion UPS Technology	
		DSP / Microprocessor controlled architecture	
		IGBT based inverter technology	
		Pure Sine Wave Output	
		ECO Mode for higher efficiency	
		Automatic Battery Management	
		Intelligent Fan Speed Control	
		LCD Display for monitoring and configuration	
		Cold Start Capability	
		Generator Compatible	
		Automatic restart after mains recovery	
3	Input		
3.1	Input Voltage Range	110V – 300V AC	
3.2	Nominal Input Voltage	220 / 230 / 240V AC	
3.3	Input Frequency	40 – 70 Hz	
3.4	Input Power Factor	≥ 0.99	
3.5	Input Current Harmonic Distortion (THDi)	≤ 5%	
4	Output		
4.1	Output Voltage	220 / 230 / 240V AC	
4.2	Output Frequency	50 / 60 Hz	
4.3	Output Voltage Regulation	± 1%	
4.4	Output Frequency Regulation	± 0.1 Hz	

SNo.	Parameter	Specifications	Compliance (Yes/No)
4.5	Output Waveform	Pure Sine Wave	
4.6	Crest Factor	3:01	
4.7	Transfer Time	Zero Transfer Time in Online Mode	
5	Efficiency		
5.1	Online Mode Efficiency	≥ 93%	
5.2	ECO Mode Efficiency	≥ 97%	
6	Battery		
6.1	Battery Type	VRLA / SMF Batteries	
6.2	Recharge Time	90% recharge within 4–6 hours	
6.3	Battery Protection	Deep discharge and overload protection	
7	Display & Monitoring	LCD Display with Input, Output, Battery and Load Status	
8	Alarms	Audible alarms for Mains Failure, Low Battery, Overload and Fault	
9	Protection	Short Circuit, Overload, Battery Low, Surge Protection	
10	Physical	Tower Type Floor Mounted UPS	
10.1	Cooling	Forced Air Cooling	
10.2	Noise Level	< 50 dBA	
11	Environmental		
11.1	Operating Temperature	0°C to 40°C	
11.2	Humidity	0 – 95% RH Non-Condensing	
12	Certifications	IEC 62040-1, IEC 62040-2, IEC 62040-3, CE Compliance	
16.	DC UPS		
1	Capacity (in kVA)	120kW , 3-Phase Input / 3-Phase Output UPS	
2	Technology and Capability	a) True Online configuration double conversion UPS with 3-Level Inverter Technology	
		b) Modular & Scalable UPS with hot swappable Power Module of rating of 20kW.	
		c) Hot Swappable STS Module & control Module	
		d) Parallel capability up to Six no. of Power Modules for Vertical redundancy & up to eight UPS units for capacity.	
		e)Redundant System with optional redundant controller, Dual Aux Power Supply.	
		f) Dual CAN Bus within frame & redundant CAN Bus between parallel systems to enable UPS to be removed or inserted UPS in parallel configuration without need of transferring it to	
		bypass mode	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		g) Green mode of operation to improve operational efficiency (>96%) on varying & dynamic loading conditions without compromising the redundancy required in the application.	
		h) Top & Bottom cable Entry options.	
		i) DSP (Digital Signal Processor) / Microprocessor based control, using IGBT devices and high switching frequency PWM	
		j) Capability of independent or common battery bank operation of the UPS when operated in Parallel Redundant System.	
		k) Brushless DC Fans with speed control	
		l) Energy Recycle Mode that enables testing of the unit for load testing without external load & helps in Load simulation	
3	Model Name & Number		
4	Input		
	Input facility -Phases / Wires	3-Phase / 4-Wire & Gnd (R, Y, B	
		-Phases & Neutral + Ground)	
	Nominal Input Voltage	380 / 400 / 415V AC	
	Input Voltage Range	305 - 477 V AC	
	Nominal Input Frequency	50 / 60 Hz (Auto selectable)	
	Input Frequency Range	40-70 Hz	
	Input Power Factor	> 0.99 on Full resistive load Load	
	Input Current Harmonic Distortion (THDi)	< 3% on Full Load (with Mains Vthd less than 1%)	
5	Output		
5.1	Nominal Output Voltage	380 / 400 / 415V AC (Selectable)	
5.2	Output Voltage Regulation	+/- 1%	
5.3	Nominal Output Frequency	50 / 60 Hz (Selectable)	
5.4	Output Frequency Regulation	+/- 0.05 Hz (Free Running / Self Clocked Mode)	
		+ / - 5 % (Synchronized to Mains Mode, Selectable)	
5.5	Output Frequency Slew Rate	1 Hz / s	
5.6	Output Wave Form	Pure sine wave	
5.7	Output Voltage Distortion (Vthd)	<= 1% (For 100% Linear / Resistive Load)	
		<= 5% (For 100% Non-Linear / RCD Load)	
5.8	Crest Factor	3 : 1 On Full Load	

SNo.	Parameter	Specifications	Compliance (Yes/No)
5.9	Unbalanced load on phases	100% unbalanced load should be allowed	
5.1	Displacement angle for 100% balanced Load	120 deg +/- 2 deg	
6	Transient Response / Recovery		
6.1	Transient response: Dynamic regulation for 0% to 90 % step load	+/- 5%	
7	Transfer Time		
7.1	Transfer Time (Mode of operation)	Nil from Mains mode to Battery Mode	
		Nil from Battery Mode to Mains mode	
7.2	Transfer Time (Inverter to Bypass / Bypass to Inverter)	< 1 ms (Synchronized Mode)	
		< 10 ms (Asynchronized Mode)	
7.3	Automatic & Bi-directional static by-pass (In-built)	Uninterrupted transfer of load from Inverter to bypass (under overload / fault conditions) & automatic retransfer from bypass to inverter (on removal of overload / fault conditions)	
8	Efficiency (At Nominal Voltage & Resistive Load up to kW rating of UPS)		
8.1	Overall Peak Efficiency (AC to AC) - Online (Double Conversion)	96%	
8.2	Overall Efficiency (AC to AC) - Online (Double	95%	
	Conversion) on 25% Loading		
8.3	Eco mode efficiency	99%	
9	Overload		
9.1	Inverter Overload capacity (Mains Mode & Battery Mode)	125% for 10 minutes	
		150% for 60 seconds, > 150% for 1 sec	
10	Display Panel (In-build Touch Display)		
	Measurements (On Touch Display)	Input: Voltage /Current/ Frequency	
		Bypass: Voltage /Current/ Frequency	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		Output: Voltage / frequency / Current	
		Battery: Voltage / Capacity	
		Load: In kVA / kW / Percentage	
		Temperature: STS/Inverter/PFC	
	Event Logging & Statistical Data (On LCD): UPS should capture and display upto 10000 events	Events Logs (10000 events) like: Over temperature / DC Bus Fail / Fan Fail / Fuse Fail / Overload / Short-circuit / Device Fail / Inverter Fail / Rectifier Fail / Bypass Fail, etc	
		Statistical Data: No. of power failures	
		/ Transfers to Bypass / Total Running time, etc	
	User Programmable Parameters & Settings (On Touch Display)	Bypass: Voltage / Frequency Range	
		Inverter: Voltage / Frequency / Eco Mode / Frequency converter	
		Battery: Type / Banks / Chargers Current / Manual & Automatic Testing	
		Mode selection : online Mode,Green Mode,ECO Mode, Energy Recycle	
		Mode & Frequency conversion mode	
		Auto Equalize charge enable/disable option with selectable interval	
		Alarms: Buzzer Test / Buzzer Mute	
		Date & Time Setting	
		Password: User / Administrator Setting	
		Information: UPS Serial No. / Firmware	
		Log & Statistical Data Reset & Firmware upgrade	
11	Alarms		
	Audible Alarms	Mains Failure / Battery Low Alarm / UPS Overload / Fault / Shortcircuit	
12	Battery Bank	VRLA	
	Backup Required	240 minutes on 20 kVA/kW	
	Make, Type, Model No. & Country of Origin	Vendor to Furnish	
13	Physical		
	Operating Temperature	0 to 40 deg C full load	
	Storage Temperature	-25 to 70 deg C	
	Operating Humidity	0 to 95% RH (Non-condensing)	
	Operating Altitude	1000 m (meters above sea level) without derating, Derating 1% for each additional 100m.	
	Protection Class	IP – 20	
	Type of Cooling	Forced Air	

SNo.	Parameter	Specifications	Compliance (Yes/No)
	Noise Level	< 65 dbA at 1 meter distance	
	Form Factor	Free Standing Floor Mounted UPS	
	Dimension (w x d x h) in mm	Vendor to Furnish	
	Weight - in kg	Vendor to Furnish	
	Reliability	MTBF greater than 350000 hours	
	Connections - Rectifier Input / Output / Bypass Input / Battery	Breakers for input,output,bypass & Maintenance bypass	
14	Certifications		
	Manufacturer	QMS: As per ISO 9001: 2008	
		EMS: As per ISO 14001: 2004	
		OSHAS: As per ISO 18001: 2007	
		TL 9000	
	Product	Safety: As per IEC62040-1	
		EMC: As per IEC62040-2	
		Performance : As per IEC62040-3	
		ESD: As per IEC61000-4-2 Level 4	
		RF: As per IEC61000-4-3 Level 3	
		FT/Burst: As per IEC61000-4-4 Level 4	
		Surge: As per IEC61000-4-5 Level 4	
		CE Declaration of Conformance	
17.	DR UPS		
1	Capacity (in kVA)	120kW , 3-Phase Input / 3-Phase Output UPS	
2	Technology and Capability	a) True Online configuration double conversion UPS with 3-Level Inverter Technology	
		b) Modular & Scalable UPS with hot swappable Power Module of rating of 20kW.	
		c) Hot Swappable STS Module & control Module	
		d) Parallel capability up to Six no. of Power Modules for Vertical redundancy & up to eight UPS units for capacity.	
		e)Redundant System with optional redundant controller, Dual Aux Power Supply.	
		f) Dual CAN Bus within frame & redundant CAN Bus between parallel systems to enable UPS to be removed or inserted UPS in parallel configuration without need of transferring it to	
		bypass mode	
		g) Green mode of operation to improve operational efficiency (>96%) on varying & dynamic loading	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		conditions without compromising the redundancy required in the application.	
		h) Top & Bottom cable Entry options.	
		i) DSP (Digital Signal Processor) / Microprocessor based control, using IGBT devices and high switching frequency PWM	
		j) Capability of independent or common battery bank operation of the UPS when operated in Parallel Redundant System.	
		k) Brushless DC Fans with speed control	
		l) Energy Recycle Mode that enables testing of the unit for load testing without external load & helps in Load simulation	
3	Model Name & Number		
4	Input		
	Input facility -Phases / Wires	3-Phase / 4-Wire & Gnd (R, Y, B	
		-Phases & Neutral + Ground)	
	Nominal Input Voltage	380 / 400 / 415V AC	
	Input Voltage Range	305 - 477 V AC	
	Nominal Input Frequency	50 / 60 Hz (Auto selectable)	
	Input Frequency Range	40-70 Hz	
	Input Power Factor	> 0.99 on Full resistive load Load	
	Input Current Harmonic Distortion (THDi)	< 3% on Full Load (with Mains Vthd less than 1%)	
5	Output		
5.1	Nominal Output Voltage	380 / 400 / 415V AC (Selectable)	
5.2	Output Voltage Regulation	+/- 1%	
5.3	Nominal Output Frequency	50 / 60 Hz (Selectable)	
5.4	Output Frequency Regulation	+/- 0.05 Hz (Free Running / Self Clocked Mode)	
		+ / - 5 % (Synchronized to Mains Mode, Selectable)	
5.5	Output Frequency Slew Rate	1 Hz / s	
5.6	Output Wave Form	Pure sine wave	
5.7	Output Voltage Distortion (Vthd)	<= 1% (For 100% Linear / Resistive Load)	
		<= 5% (For 100% Non-Linear / RCD Load)	
5.8	Crest Factor	3 : 1 On Full Load	
5.9	Unbalanced load on phases	100% unbalanced load should be allowed	

SNo.	Parameter	Specifications	Compliance (Yes/No)
5.1	Displacement angle for 100% balanced Load	120 deg +/- 2 deg	
6	Transient Response / Recovery		
6.1	Transient response: Dynamic regulation for 0% to 90 % step load	+/- 5%	
7	Transfer Time		
7.1	Transfer Time (Mode of operation)	Nil from Mains mode to Battery Mode	
		Nil from Battery Mode to Mains mode	
7.2	Transfer Time (Inverter to Bypass / Bypass to Inverter)	< 1 ms (Synchronized Mode)	
		< 10 ms (Asynchronized Mode)	
7.3	Automatic & Bi-directional static by-pass (In-built)	Uninterrupted transfer of load from Inverter to bypass (under overload / fault conditions) & automatic retransfer from bypass to inverter (on removal of overload / fault conditions)	
8	Efficiency (At Nominal Voltage & Resistive Load up to kW rating of UPS)		
8.1	Overall Peak Efficiency (AC to AC) - Online (Double Conversion)	96%	
8.2	Overall Efficiency (AC to AC) - Online (Double	95%	
	Conversion) on 25% Loading		
8.3	Eco mode efficiency	99%	
9	Overload		
9.1	Inverter Overload capacity (Mains Mode & Battery Mode)	125% for 10 minutes	
		150% for 60 seconds, > 150% for 1 sec	
10	Display Panel (In-build Touch Display)		
	Measurements (On Touch Display)	Input: Voltage /Current/ Frequency	
		Bypass: Voltage /Current/ Frequency	
		Output: Voltage / frequency / Current	
		Battery: Voltage / Capacity	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		Load: In kVA / kW / Percentage	
		Temperature: STS/Inverter/PFC	
	Event Logging & Statistical Data (On LCD): UPS should capture and display upto 10000 events	Events Logs (10000 events) like: Over temperature / DC Bus Fail / Fan Fail / Fuse Fail / Overload / Short-circuit / Device Fail / Inverter Fail / Rectifier Fail / Bypass Fail, etc	
		Statistical Data: No. of power failures	
		/ Transfers to Bypass / Total Running time, etc	
	User Programmable Parameters & Settings (On Touch Display)	Bypass: Voltage / Frequency Range	
		Inverter: Voltage / Frequency / Eco Mode / Frequency converter	
		Battery: Type / Banks / Chargers Current / Manual & Automatic Testing	
		Mode selection : online Mode,Green Mode,ECO Mode, Energy Recycle	
		Mode & Frequency conversion mode	
		Auto Equalize charge enable/disable option with selectable interval	
		Alarms: Buzzer Test / Buzzer Mute	
		Date & Time Setting	
		Password: User / Administrator Setting	
		Information: UPS Serial No. / Firmware	
		Log & Statistical Data Reset & Firmware upgrade	
11	Alarms		
	Audible Alarms	Mains Failure / Battery Low Alarm / UPS Overload / Fault / Shortcircuit	
12	Battery Bank	VRLA	
	Backup Required	240 minutes on 20 kVA/kW	
	Make, Type, Model No. & Country of Origin	Vendor to Furnish	
13	Physical		
	Operating Temperature	0 to 40 deg C full load	
	Storage Temperature	-25 to 70 deg C	
	Operating Humidity	0 to 95% RH (Non-condensing)	
	Operating Altitude	1000 m (meters above sea level) without derating, Derating 1% for each additional 100m.	
	Protection Class	IP – 20	
	Type of Cooling	Forced Air	
	Noise Level	< 65 dbA at 1 meter distance	
	Form Factor	Free Standing Floor Mounted UPS	

SNo.	Parameter	Specifications	Compliance (Yes/No)
	Dimension (w x d x h) in mm	Vendor to Furnish	
	Weight - in kg	Vendor to Furnish	
	Reliability	MTBF greater than 350000 hours	
	Connections - Rectifier Input / Output / Bypass Input / Battery	Breakers for input,output,bypass & Maintenance bypass	
14	Certifications		
	Manufacturer	QMS: As per ISO 9001: 2008	
		EMS: As per ISO 14001: 2004	
		OSHAS: As per ISO 18001: 2007	
		TL 9000	
	Product	Safety: As per IEC62040-1	
		EMC: As per IEC62040-2	
		Performance: As per IEC62040-3	
		ESD: As per IEC61000-4-2 Level 4	
		RF: As per IEC61000-4-3 Level 3	
		FT/Burst: As per IEC61000-4-4 Level 4	
		Surge: As per IEC61000-4-5 Level 4	
		CE Declaration of Conformance	
18.	**DG Set (250 kVA)**		
1	Diesel Engine	Six Cylinders Inline, Liquid Cooled, Turbocharged with After Cooled, Developing 310 hp @ 1500 RPM. Engine is with Electric Start, Compression Ignition, 4 Stroke Cycle, designed to run continuously at 1500 RPM. Confirming to IS 10002, ISO-3046, BS 5514 standards. Radiator with Fan, Fuel Injection equipment with Electronic Governor, Dry type Air Cleaner, Exhaust Silencer, Lube Oil filter (Spin On Type), Fuel Oil filter (Spin On Type), 2X12V Electric starting system, Battery charging alternator, Stop Solenoid, Lube Oil pressure Gauge, Water Temperature Gauge, Lube Oil temperature Gauge, Battery Voltage, K - Cool Super Plus coolant, First Fill Lube Oil.	
2	Alternator	Suitable for continuous duty operations rated at 1500 RPM 415 V, 0.8 PF, 50Hz, 3Ph. in SPDP Enclosure, Self- Excited & Self- regulated, Brush less, 'H' class Insulation, Floor mounted with anti-friction Shielded Ball Bearing on end. The alternator conforms to IS: 4722, BS EN 60034-1 suitable for tropical conditions.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
3	Base Frame	Suitable to couple above Engine & Alternator made from steel sheet metal	
4	Fuel Tank	8 Hrs Capacity for continuous running, with Diesel fuel Inlet & Outlet, Air Vent & Drain plug arrangements	
5	Battery	2 Nos.12 V Battery with Leads	
6	Genset Controller Unit with Control Panel	Genset Controller unit with totally enclosed, Steel Construction Control Panel suitable for indoor floor / wall mounting installation having safeties and display parameters.	
7	Gen-set Display Parameters	Phase Voltage, Line current, Frequency, Average Voltage, Average Current, Phase kW & Total kW, kWH, kVA, kVAR, PF.	
8	Engine Display Parameters	Lube Oil Pressure, Engine Temperature, Fuel Level Status, Engine speed, Battery Voltage, Minimum	
		Battery Voltage, Lube Oil Temperature, Engine Hours, No. of Starts.	
9	Electrical Safeties (along with Display)	Genset Under/Over voltage, Under/Over Battery voltage, Under/Over Frequency, Phase Failure, Phase sequence reverse, Over Current, Over kW.	
10	Mechanical Safeties (along with Display)	Phase Voltage, Low Lube oil pressure, High Lube oil Temperature, High engine coolant temperature, Low coolant level, Low Fuel Level, Start/Stop fail, Battery Charging Alternator fail.	
11	Acoustic Enclosure	Enclosure should be modular in construction, Base Frame should be made of Sheet metal, Durable industrial locking system must be provided on Doors, Door Gaskets are made in high quality EPDM material.	
12	Corrosion Resistance	All sheet metal parts/components are hot dipped in seven tanks process, Pretreated and Passivated, Sheet metal components are with Pretreated and Passivated Base Powder Coated, Base Frame must be Epoxy Coated/Powder Coated, Zinc Passivated Hardware should be used to avoid rusting.	
13	Acoustic Insulation	Sound proofing of the Enclosure must do with Quality Foam confirming to IS: 7888 Standard, Acoustic foam shall be fire retardant and fire resistant, Attenuates shall be provided to control sound at entry and exit of container, specially designed Residential Silencer is provided.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
14	Ventilation & Air Circulation	Exhaust pipe inside Enclosure is thoroughly insulated by Cladding of Rock wool and Sheet.	
15	Electrical	Neutral Body Earthing points at the sides of enclosure are isolated through Moulded compound.	
16	Safeties	Emergency Push button to Stop the DG set from outside, Low Fuel oil level, Low Lube oil pressure, Low Coolant Level, High Engine Temperature.	

Group 3: Surveillance & Field Devices

SNo.	Parameter	Specifications	Compliance (Yes/No)
19.	**Fixed Camera (5 MP)**		
1	Image Sensor:	5 MP outdoor, 1/2.8"CMOS with IP67 rating	
2	Max Resolution:	1920 x 1080	
3	Focal Length:	Motorized Lens 05-55mm	
4	Zoom/Focus Adjust:	Motorized zoom and focus -Auto back focus	
5	Iris:	P-iris	
6	IR Distance:	163 ft/50m	
7	Minimum Illumination:	Colour 0.01 Lux, B/W 0 Lux	
8	Shutter Speed:	Auto 1/3~1/100000 or more, manual	
9	Day/Night Performance:	True day/night (IR cut filter)	
10	Wide Dynamic Range	True WDR; 120 dB	
11	WDR Feature	OFF, Auto, Low, Medium and High	
12	Gain control	Auto/Manual	
13	Backlight compensation	Yes	
14	White balance mode	Auto/Manual	
15	Privacy masking	5 areas or more	
16	Motion Detection	4 areas or more	
17	Video Analysis	Motion/ Tampering/ Intrusion/ Line Cross	
18	Network Loss Detection	Yes	
19	Image Settings:	Brightness, Contrast, Saturation, Sharpness, Mirror, Flip, Corridor, Hue, Rotation, Anti-flicker, BLC, AWB	
20	Video compression	H.265, H.264 compression, M-JPEG,	
21	Video streaming	Quad streaming or better	
22	Video resolution	1080p, 720p, 720x567, 720x480, 640x480, 640x360, 320x240	
23	Streaming:	Unicast and Multicast streams. Quad streaming.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		Stream 1 & 2 Should be 1920x1080 @25/30 fps	
24	Frame rate	1080p @ 30 fps	
25	Bit rate	128K~8000K	
26	Rate Control	CBR / CVBR	
27	GOP	1~100 or more	
28	Dynamic GOP	ON/OFF	
29	Max Dynamic GOP	1~254 or more	
30	Audio Compression	G.711 8KHz/16-bit	
31	Encoding	A-Law and U-Law	
32	Audio In Volume	High, Mid and Low. Should be able to available in camera web page	
33	Audio Out Volume	High, Mid and Low. Should be able to available in camera web page	
34	AE Mode	Auto, 50Hz, 60Hz and Lock	
35	Iris	P-iris or better	
36	ROI	5 zone or more	
37	OSD	Date/Time and Name	
38	Audio Streaming	Two-way	
39	Audio Input	Line-in	
40	Audio Output	Line-out	
41	Connectors	Should have a compulsory Reset button audio -In & Out Port, RJ 45 Port	
42	Interface	10/100 Mbps Ethernet, RJ-45	
43	Network port security	802.1x	
44	Supported protocols	IPv4, IPv6, HTTP, HTTPS, SSL, TCP/IP, UDP, UPnP, RTSP, RTP, SMTP, NTP, DHCP, FTP, Zero Configure, Bonjour	
45	ONVIF	Profile S, G, T & M	
46	Approvals:	CE, FCC, STQC, BIS ER:01 2024, IP67, IK10, NEMA4X, RoHS, NDAA Compliant	
47	Users	Live viewing/Administrator for up to 10 clients	
48	Browsers	Google Chrome, Mozilla Firefox, Microsoft Edge	
49	Event trigger	Motion detection, Tampering detection, Alarm in	
50	Notifications	Send message via e-mail/record to FTP/NAS/SD card, record JPG/mp4	
51	Power supply	PoE IEEE 802.3af, Class 3/DV 12V	
52	Storage	Micro SD (512 GB)	

SNo.	Parameter	Specifications	Compliance (Yes/No)
53	Alarms:	1 alarm input/1 alarm output	
54	Operating Temp	50° to 140° F (-20° to 55° D54 E54C)	
55	Humidity	10% ~ 90%RH (no condensation)	
56		Camera, VMS & NVR should be of same make/OEM	
20.	**PTZ Camera**		
1	Image Sensor:	1/2.8” 5MP Sony CMOS progressive sensor or better	
2	Max Resolution:	2592 x 1944	
3	Focal Length:	Motorized Lens 4.25 - 170 mm (40X optical zoom) or better	
4	Zoom/Focus Adjust:	Motorized zoom and Auto Focus (Auto & manual)	
5	IR Distance:	250 m or better	
6	Minimum Illumination:	Colour: 0.05 lux; B/W: 0.01 lux (IR OFF; 0 lux IR ON)	
7	Iris:	P-iris	
8	Shutter Speed:	Auto 1/3~1/10000 or more, manual	
9	Day & Night Performance:	Automatically removable IR-cut filter	
10	HDR	Required	
11	Defog	Required	
12	Image Settings:	Brightness, Sharpness, Contrast, Saturation, Hue, White Balance, Exposure Control, 3DNR, 2DNR, Colour Noise reduction, Text Overlay, ROI (areas each for stream 1 and 2); Privacy Mask (5 areas); Motion Detection (4 areas);	
13	Video compression	H.265 or better	
14	Video streaming	Quad streaming or better	
15	Video resolution	2592 × 1944, 2560 × 1440, 2048 × 1536, 1920 × 1080, 1280 × 1024, 1280 × 720, 1024 × 768, 800 × 600, 720 × 480, 640 × 480, 352 × 240, 320 × 240	
16	Streaming	Unicast and Multicast streams. Quad streaming. Stream 01: 2592 x 1944 @30fps Stream 02: 1920 x 1080 @30fps Stream 03: 1920 x 1080 @30fps Stream 04: 320 x 240 @30fps At least Three streams should be at @60 fps with 1080p	
17	Frame rate	5MP at 25/30 fps and 2MP @50/60 fps	
18	Rate Control	LBR/CBR/CVBR	
19	Pan Range:	360° continuous pan	
20	Pan Speed:	0.1° - 300°/second	

SNo.	Parameter	Specifications	Compliance (Yes/No)
21	Tilt Range:	-20° - 90°	
22	Tilt Speed:	0.1° - 300°/second	
23	Presets:	256; 8 Sequence, 8 cruise, 4 auto pan	
24	Audio Compression	G.711/ G.726/ AAC/ LPCM	
25	Audio Streaming	2 Way	
26	Sytem	PAL/NTSC	
27	OSD	Date & Time, Text Contents, Image (Transparency 0-255)	
28	Connectors & button	24 VAC Power: terminal block. Network/PoE: RJ-45. Audio In/Out and Alarm In/Out: terminal block. SDHC/SDXC Card Slot. Reset button. Indicator: network status LED.	
29	Interface	1Gbp Ethernet(Auto, Half Duplex, Full Duplex), RJ-45 or better	
30	Security	IP address filtering, HTTP/HTTPS Sever Certificate Validation, SSL, multi-user authority, SMTP Server Certification Validation, SFTP Server Host Key Fingerprint, Password Security, CA Certificate, User Authentication/ HTTPS/ IP Filter/ IEEE 802.1x, TLS 1.3, SHA-256, DES, AES-256, User Access Log, TPM 2.0, FIPS 140 Level 2 or better	
31	Supported protocols	IPv4/v6, QoS, TCP, UDP, DHCP, UPnP, SNMP V3, LLDP, RTMP, RTP, RTSP(All four stream), HTTP, VLAN, HTTPS, RTSPS, FTP, NTP, ONVIF: S, G, T, M	
32	Event Triggers	External Input, Analytics, Network Failure Detection, Periodical Event, Manual Trigger	
33	Event Actions	External output Activation Video and audio recording to edge storage File Upload : FTP, network share and email Notification : HTTP, FTP, email	
34	Browsers	Google Chrome, Mozilla Firefox, Microsoft Edge	
35	Analytics	Motion Detection, Tampering, Audio detection, Line Crossing, Object in zone, Object Counting (line cross, number of objects in Zone), Loitering, Parking Violation, Wrong Way, People gathering, Abandoned Object, Removed Object, Face Recognition, LPR Recognition, Auto Face Enrollment, Vehicle Recognition & Classification, Heat Map, PPE Detection, Auto Tracking, Tagging	
36	LiDER	Required	

SNo.	Parameter	Specifications	Compliance (Yes/No)
37	Power supply	IEEE802.3bt, Type 3, class 6, max 56.00 watt AC24V	
38	Storage	Supports Micro SD (1.5 TB), Support for recording to NAS	
39	Alarms:	Alarm in x 4, Alarm out x 2	
40	Operating Temp	-40°C to 50°C, Need Inbuild Heater	
41	Humidity	10% ~ 90%RH (no condensation) or better	
42	Approvals:	CE, FCC, BIS ER:01 2024, IP66, RoHS, NDAA Compliant	
43	Cyber Security compliance	The cameras offered must be cyber security certified with NDAA & ER 01:2024.	
21.	**ANPR Camera**		
1	Image Sensor:	1/2.8" 5MP Sony CMOS progressive sensor or better	
2	Max Resolution:	2592 x 1944	
3	Lens	5 ~ 50 mm or Better	
4	Lens Type	CS/i-CS Mount, Remote Focus (ABF) or better	
5	Minimum Illumination:	Colour 0.1 Lux, B/W 0.01 Lux	
6	Max. Aperture:	f/1.6	
7	Iris:	DC Auto Iris	
8	Field-of-View:	H: 6.0° (tele) - 60.0° (wide)| V: 4.2° (tele) - 35.0° (wide)	
9	Shutter Speed:	1/3~1/10000 or more, manual	
10	Day & Night Performance:	Automatically removable IR-cut filter	
11	HDR	Required	
12	Image Settings:	Brightness, Sharpness, Contrast, Saturation, Hue, White Balance, Exposure Control, Defog, 3DNR, 2DNR, Colour Noise reduction, HDR, EIS, Text Overlay, ROI (areas each for stream 1 and 2); Privacy Mask (5 areas); Motion Detection (4 areas); Tamper Detection, Audio Detection, Network Failure Detection, Shock Detection	
13	Video compression	H.265 or better	
14	Video streaming	Quad streaming or better	
15	Video resolution	2592 × 1944, 2560 × 1440, 2048 × 1536, 1920 × 1080, 1280 × 1024, 1280 × 720, 1024 × 768, 800 × 600, 720 × 480, 640 × 480, 352 × 240, 320 × 240	
16	Streaming	Unicast and Multicast streams. Quad streaming.	
		Stream 01: 2592 x 1944 @30fps	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		Stream 02: 1920 x 1080 @30fps	
		Stream 03: 1920 x 1080 @30fps	
		Stream 04: 320 x 240 @30fps	
		At least Three streams should be at @60 fps with 1080p	
17	Frame rate	5MP at 25/30 fps and 2MP @50/60 fps	
18	Rate Control	LBR, CBR, CVBR	
19	Audio Compression	G.726 (16/24/32/40 kbps), G.711 (ULaw/ALaw), AAC, PCM (128/256/384/768 kbps)	
20	Audio Streaming	2 Way	
21	Audio Input	Line-in and Built-in Mic	
22	Audio Output	Line-out	
23	Sytem	PAL/NTSC	
24	OSD	Date & Time, Text Contents, Image (Transparency 0-255)	
25	Connectors & button	Should have a compulsory Reset button, Audio In & Mic In (Line In) 3.5mm jack, RJ 45 Port, USB Type- A/C, Alarm I/O, RS485 Terminal	
26	Interface	1Gbp Ethernet, RJ-45	
27	Security	IP address filtering, HTTPS encrypted data transmission, SSL, multi-user authority, Password Security, CA Certificate, User Authentication/ HTTPS/ IP Filter/ IEEE 802.1x, TLS 1.3, SHA-256, DES, AES, User Access Log, TPM 2.0, FIPS 140	
28	Supported protocols	IPv4/v6, QoS, TCP, UDP, DHCP, UPnP, SNMP V3, LLDP, RTMP, RTP, RTSP, HTTP, VLAN, HTTPS, RTSPS, FTP, NTP, ONVIF: S, G, T, M	
29	Browsers	Google Chrome, Mozilla Firefox, Microsoft Edge	
30	Analytics	Motion Detection, Tampering, Audio detection, Line Crossing, Object in zone, Object Counting (line cross, number of objects in Zone), Loitering, Parking Violation, Wrong Way, People gathering, Abandoned Object, Removed Object, Face Recognition, LPR Recognition, Auto Face Enrollment, Vehicle Recognition, Heat Map, PPE Detection	
31	Power supply	PoE IEEE 802.3af, Class 3/DV 12V	
32	Storage	Supports Micro SD (1.5 TB), Support for recording to NAS	
33	Alarms:	Alarm in x 2, Alarm out x 1	

SNo.	Parameter	Specifications	Compliance (Yes/No)
34	Operating Temp	-50°C to 55°C, Need Inbuild Heater	
35	Humidity	up to 90%RH (no condensation) or better	
36	Approvals:	CE, FCC, BIS ER:01 2024, IP66, IK10, RoHS, NDAA Compliant	
Housing			
37	Viewing Window:	Tempered glass	
38	Construction:	Die-cast aluminum alloy	
39	Cabling:	2x M16 waterproof cable glands	
40	Fan:	59° F (15° C) On; 77° F (25° C) Off (10 W)	
41	Power Input:	60W PoE IEEE 802.3at	
42	IR Features:	3 W; 163 ft (50 m) range	
43	Coating:	White eposy powder coating	
44	Ratings:	Weather: IP66; Vandal: IK10	
45	Operating Temperature:	-58° F - 140° F (-50 °C - 60° C)	
46	Cyber Security compliance	Weatherproof: IP66/68; Vandalproof: IK10	
22.	**Panoramic Camera**		
1	Image Sensor:	1/1.6" 12.5 MP Sony CMOS progressive sensor or better	
2	Max Resolution:	3520 x 3520	
3	Focal Length:	1.7mm, (+/-) 0.1 mm	
4	IR Distance:	15 m or better	
5	Minimum Illumination:	Colour 0.1 Lux, B/W 0.01 Lux	
6	Field-of-View:	195° (at full resolution); 360° (surround view)	
7	Shutter Speed:	Auto 1/3~1/10000 or more, manual	
8	Day & Night Performance:	Automatically removable IR-cut filter	
9	WDR & HDR	Required	
10	Defog	Required	
11	Image Settings:	Brightness, Sharpness, Contrast, Saturation, Hue, White Balance, Exposure Control, Defog, 3DNR, 2DNR, Colour Noise reduction, HDR, Text Overlay, ROI (areas each for stream 1 and 2); Privacy Mask (5 areas); Motion Detection (4 areas); Tamper Detection, Audio Detection, Network Failure Detection	
12	Video compression	H.265 or better	
13	Video streaming	Quad streaming or better	

SNo.	Parameter	Specifications	Compliance (Yes/No)
14	Video resolution	3520 x 3520, 2992 x 2992, 1920 x 1080, 1280 x 1024, 1280 x 720, 1024 x 768, 800 x 600, 720 x 480, 640 x 480, 640x360, 640x512, 352x240	
15	Frame rate	30fps or better	
16	Edge Dewarping	Required	
17	Multiple Dewarp Display Mode	Digital PTZ, Panorama View, Single View ePTZ Dewarp, Two Views 180 Dewarp, Quad View ePTZ Dewarp	
18	Rate Control	LBR, CBR, CVBR	
19	Audio Compression	G.711, G.726, AAC, LPCM	
20	Audio Streaming	2 Way	
21	Audio I/0:	1/1 (line in/line out), Microphone built-in, Speaker Line out	
22	Sytem	PAL/NTSC	
23	OSD	Date & Time, Text Contents, Image (Transparency 0-255)	
24	Connectors & button	Should have a compulsory Reset button, PoE, Video, Data: RJ-45; Power: 12 VDC plug; Alarm In/Out: terminal block; Audio In/Out; Reset button	
25	Interface	1Gbp Ethernet, RJ-45	
26	Security	Multi-user authentication with role-based access control, HTTP/RTSP Digest authentication, Account lockout protection, HTTPS (SSL/TLS) encryption, IP filtering (IPv4/IPv6), IEEE 802.1X (EAP-MD5/TLS 1.3/TTLS/PEAP), SNMP v3 (MD5/SHA-512, DES/AES), Certificate management (Self-signed & CA), Secure event transmission (SMTP/FTP/HTTP), System logging & audit trail, VLAN & QoS support, TPM 2.0, FIPS 140 compliant	
27	Supported protocols	RTP/RTSP/RTSP (All four stream) over HTTP, RTP over UDP/TCP, MJPEG over HTTP, HTTP/HTTPS, TCP/IP, UDP, IPv4/IPv6, WebSocket, MQTT, SNMP v1/v2/v3, UPnP, LLDP, DDNS, RTMP, SMTP, FTP, HTTP Notification, IEEE 802.1X, QoS, VLAN, PPPoE, Multicast, ARP, ICMP, IGMP, NTP, ONVIF: S, G, T, M	
28	Event Triggers	External Input, Analytics, Network Failure Detection, Periodical Event, Manual Trigger	
29	Event Actions	External output Activation Video and audio recording to edge storage File Upload: FTP, network share and email Notification: HTTP, FTP, email	

SNo.	Parameter	Specifications	Compliance (Yes/No)
30	Browsers	Google Chrome, Mozilla Firefox, Microsoft Edge	
31	Analytics	Motion Detection, Tampering, Audio detection, Line Crossing, Object in zone, Object Counting (line cross, number of objects in Zone), Loitering, Parking Violation, Wrong Way, Abandoned Object, Removed Object, Face Recognition, LPR Recognition, Human/Vehicle Classification, Object Classification/ Recognition, Heat Map	
32	Power supply	PoE IEEE 802.3at, Class 4/DC 12V	
33	Storage	Support for microSD/microSDHC/microSDXC card (1.5 TB), Support for recording to NAS	
34	Alarms:	Alarm in x 1, Alarm out x 1 or better	
35	Operating Temp	-30°C to 60°C, Need Inbuild Heater	
36	Humidity	up to 95%RH (no condensation) or better	
37	Approvals:	UL, CE, FCC, BIS ER:01 2024, IP66, IK10, RoHS, NDAA Compliant	
38	Cyber Security compliance	The cameras offered must be cyber security certified with NDAA & ER 01:2024.	
23.	**Thermal Camera**		

SNo.	Parameter	Specifications	Compliance (Yes/No)
24.	**Body Worn Camera Solution**		
1	Product Type	Advanced Body Worn Camera	
2	Camera Design	Sleek, minimalist and ruggedized unibody chassis	
3	Dimensions	Approx. 100 mm x 60 mm x 20 mm	
4	Weight	Ultra-lightweight design for all-day active wear	
5	Mounting Options	Magnetic clips, quick-release tactical mounts, lightweight uniform attachments	
6	Weather Protection	Weather-resistant rugged chassis	
7	Camera Position	Top-center flush camera module	
8	Optics	High-fidelity optics with ultra-wide field of view	
9	Low Light Capability	Advanced sensor technology for low-visibility environments	
10	User Interface	Streamlined interface for immediate recording initiation	
11	Battery Backup	High-density battery supporting extended shifts	
12	Live Streaming	Low-latency video and audio transmission to central control unit	
13	Data Security	Encrypted data stream using proprietary transmission protocols	
14	Real-Time Monitoring	Real-time situational awareness for command centers	
15	GPS / Tracking	Live dynamic mapping and workforce tracking	
16	Remote Management	Remote task and operational management through proprietary application	

SNo.	Parameter	Specifications	Compliance (Yes/No)
17	Communication	Seamless communication between field personnel and management	
18	Deployment Monitoring	High-level overview of unit deployment and workforce coverage	
19	Application Areas	Infrastructure, transit, industrial inspections, security & rapid response	
25.	**Dashboard Camera Solution**		
1	Image Sensor	1/3" progressive scan RGB CMOS or better,1920x1080 or better	
2	Day/ Night Operation	Yes, with Built-in IR Cut Filter	
3	Lens	2.8 mm, F1.7	
4	Minimum Illumination	Colour: 0.07 lux at 30 IRE, F1.7	
		B/W: 0.02 lux at 30 IRE, F1.7	
		0 lux with IR illumination on	
5	IR Illumination	Built in Or External Optimized IR with 15-meter range	
6	Field of View	Horizontal field of view: 110° or better	
7	Electronic Shutter	1/20000 s or better	
8	Compression	H.264/H.265 or better	
9	Frame Rate and Bit Rate	Upto 25 FPS/30 FPS at all resolutions with Controllable Bit Rate/ Bandwidth and Frame Rate	
10	GOP/ GOV	Ability to change the GOP/GOV Length to optimize the bandwidth and storage	
11	Multi View Streams	Up to 5 individually cropped out view areas	
12	Video Streams	Minimum 4 Streams @ H.265, 2MP, 25 fps/30 fps	
13	Motion Detection	Yes, built in with multiple configurable areas in the video stream	
14	Image settings	WDR-120 db, Text over relay with Date & time, and a customer-specific text, camera name, graphical image etc	
15	Event Triggers	A. The camera shall be able to send and received trigger directly from any other camera without interface of VMS. B. Intelligent Video, Edge Storage Events, Software Alarms, Camera Tampering.	
16	Edge Storage	Built in SD card slot with support of 512 GB SD card.	
17	Storage	The Camers shall have the feature to directly record the videos/ images onto Nas without any Software	

SNo.	Parameter	Specifications	Compliance (Yes/No)
18	Network Protocals	IPv4/IPv6, RTP, TCP/IP, UDP/IP, HTTP, HTTPS, IGMP, ICMP, DHCP, DNS, SMTP, FTP, NTP, DDNS, QoS, SNMP, 802.1x	
19	Security	Password protection, IP address filtering, HTTPS encryption, IEEE 802.1x (EAP-TLS) network access control, Digest authentication, User access log, Centralized Certificate Management, brute force delay protection, signed firmware, Camera should check authenticity of firmware every time it reboots.	
20	Firmware Upgrade	The firmware upgrade shall be done though web interface, The firmware shall be available free of cost	
21	Logs	The camera shall provide minimum 150 logs of latest connections, access attempts, users connected, changes in the cameras etc	
22	Memory	1 GB RAM, 512 MB Flash	
23	Interface	RJ45: male, 10BASE-T/100BASE-TX or M12: female, rugged, D-coded with rotatable coupling nut.	
		3.5 mm audio in connector,	
		1 input, 1 output ,12 V DC/15 mA	
24	Enclosure	IP66/67, IK10 or better, aluminium casing,	
25	Power requirements	Power over Ethernet (PoE) IEEE	
		802.3af/802.3at Type 1 Class 2or 3 Max.: 12 W	
26	Operating Temp & Humidity	–5°C to 55°C & 10–100% RH (noncondensing)	
27	Analytics	Motion Detection, Tampering, Shock detection, Line crossing, Loitering, Audio Detection The camera shall provide a platform allowing the upload of third-party applications into the camera	
28	MAC compliant	The MAC Addresses of all the camera supplied should be from OEM.	
29	Audio	External microphone input or line input, built-in microphone	
26.	**Drones**		
1	Platform Type	Drone / UAV Quadcopter	
2	Endurance (Tethered)	Minimum 12 Hours Mission Time	
3	Endurance (Untethered)	Minimum 35 Minutes Flight Time	
4	All Up Weight	Maximum 20 Kilograms	
5	Maximum Operating Altitude	Up to 3000 meters AMSL	

SNo.	Parameter	Specifications	Compliance (Yes/No)
6	Maximum Operating Height (AGL)	Up to 125 meters Above Ground Level	
7	Payload Type	EO/IR Integrated Camera or other compatible sensors	
8	Anti-Jam GNSS Capability	Anti-jam GNSS supported (Optional)	
9	Wind Resistance	35 kmph steady winds and 50 kmph gust resistance	
10	Environmental Protection	Water and Dust Resistant	
11	Operating Temperature	-10°C to +55°C	
12	Autonomous Operation	Fully Autonomous Operation Supported	
13	Hover Capability	Hovering capability up to 125 meters	
14	RF / GPS Protection	Immune to RF and GPS jamming	
15	Communication Link	Fiber Optic Data Link	
16	Acoustic Signature	Minimal Decibel Count	
17	Visual Signature	Incredibly Low Visual Signature	
18	Payload Flexibility	Custom Payload Integration Supported	
19	Imaging Capability	Best-in-class Day/Night Combined Payloads	
20	Safety Mechanisms	Multiple onboard safety features	
21	Application	Border Control Operations	
22	Application	Military Force Protection	
23	Application	Perimeter Protection	
24	Application	Infrastructure Security & Monitoring	
25	Application	Tactical & Frontline Support	
26	Application	Ad-hoc Telecom Tower Deployment	
27	Application	Surveillance of Forward Posts	
28	Application	Base Security for Military Compounds	
29	Application	Effective Patrolling & Overwatch	
30	Application	Special Operations Support	
31	Application	Search & Rescue Operations	
32	Winch Control System	Fully Automatic Motorized Winch Control System	
33	Power Output	3000W Standard Power Output	
34	Power Input	220V AC Input Supply	
35	Release Mechanism	Tension-based Release Mechanism	
36	Display Interface	LCD Display for Important Parameters	
37	Emergency Protection	Emergency External Stop Switch	
38	Network Integration	Fiber-optic integration with existing user network	
39	Secure Communication	Encrypted Secure Fiber-optic Communication	

SNo.	Parameter	Specifications	Compliance (Yes/No)
40	Operational Requirement	Minimal manpower required for operation	
41	Tether Cable Length	Minimum 125 meters	
42	Ground Control Station	Personalized GCS Software	
43	Mission Planning	Mission Planning Capability Supported	
44	GCS Hardware	Rugged MIL-grade Laptop	
45	Operation Mode	One Touch Operation Supported	
46	Fail-safe Feature	Automatic Return to Home on communication/power failure	
47	GPS Redundancy	Multiple GPS modules onboard	
48	Power Backup	Seamless switching to onboard battery during power failure	
27.	**Local Processing Unit (LPU)**		
1		Local Processing Unit Shall be Aluminium Alloy Casing	
2		Local Processing Unit Shall be of min. 9th Generation with Core i7 CPU	
3		It shall have 2 nos. LAN 16-bit DIO SATA, 4, COM, 6-48 V DC Wide Voltage Input	
4		It shall support GPU Intel HD Graphics 630 min.	
5		Memory DDR4 2133 MHz, up to 32 GB	
6		Display Port 1 nos., VGA 1 nos. HDMI	
7		It shall support min. Secondary storage 2 X 2.5" SATA HDD/SSD Bay/ 1XM.2 2280 SATA Interface	
8		It shall support min. USB 3.) (4) nos.	
9		It shall have LAN- 2 Nos. Intel I210T PCIe Gig. Ethernet, 1 nos. PCIe Gig Ethernet support iV Pro	
10		AC Input External Adaptor (Option)	
11		Voltage input- 100 VAC ~240 VAC @ 50~60Hz	
12		Temperature 0 ~ 70 Degree C	
13		Storage Temperature 0 ~ 60 Degree C	
14		Certifications CE, FCC	

Group 4: Public Safety, Communication & Emergency Systems

SNo.	Parameter	Specifications	Compliance (Yes/No)
28.	**Emergency Call Box (ECB)**		
1	Field Side Equipment	Construction: Cast Iron/Steel Foundation, Sturdy Body for equipment	

SNo.	Parameter	Specifications	Compliance (Yes/No)
2		Call Button: Watertight Large Push Button, Visual Feedback for button press	
3		Connectivity: Ethernet	
4		Sensors: For tempering/ vandalism	
5		IP66, IK09 Protection	
6		Operating Temperature 0 to 70 C	
7		Speaking Distance minimum 5 ft	
8		Inbuilt Class D Amplifier	
9		Minimum 3 Inputs ad 2 Output relay contacts	
10		ECB should be able to make calls to the PA system	
1	CCR Side Equipment	Central Software based server application capable of working on virtual environment/cloud with 100% redundancy for DC & DR. System should be capable for Secure connection of device as per international standard ISO 27001:2013.	
2		Access control mechanism would be also required to establish so that the usage is regulated.	
3		Integration with VaMS and Command and control centre or any other component if required	
4		PA Master Controller to have facility for multiple mic inputs, direct dialling buttons, LCD screen	
5		Software Client for making Calls to PA and ECB	
6		Automatic Volume Control, Call recording of all ECB calls with date and time	
7		Operating temperature for control desk 0 to +60C	
29.	**PAS Amplifier**		
1	125-Watt IP amplifier	125-Watt IP amplifier with 70/100 Volt loudspeaker output	
30.	**PAS Horn Speaker**		
1	30W Horn Speaker	30W Horn Speaker	
31.	**Digital Handheld Wireless Sets**		
1	Device Type	Nationwide 4G LTE Push-to-Talk Handheld Device	
2	Communication Type	Private and Group Push-to-Talk Communication	
3	Connectivity	4G LTE, 3G and Wi-Fi Connectivity	
4	GPS Capability	GPS Location Tracking Supported	
5	Audio Quality	Loud and Clear Audio with Noise Suppression	
6	Bluetooth	Bluetooth Enabled	
7	Emergency Button	Dedicated Emergency Alert Button	
8	Lone Worker Protection	Lone Worker Monitoring Supported	

SNo.	Parameter	Specifications	Compliance (Yes/No)
9	Man Down Alert	Automatic Man Down Detection Supported	
10	Fall Alert	Fall Detection Supported	
11	Channel Capacity	Multiple Channel Support	
12	Contact Capacity	Large Contact List Support	
13	Battery Capacity	High-Capacity Li-Ion Battery	
14	Battery Backup	Long Duration Battery Backup	
15	GNSS Support	GPS / GLONASS / Galileo / BeiDou Supported	
16	Wi-Fi Standard	IEEE 802.11 Wi-Fi Support	
17	SIM Capability	SIM Based LTE Communication	
18	Protection Rating	IP Rated Rugged Device	
19	Encryption	AES-256 Encryption Supported	
20	Operating Temperature	Industrial Operating Temperature Support	
21	Environmental Compliance	MIL-STD Rugged Compliance	
22	Device Management	Over-the-Air Device Management Supported	
23	Push-to-Talk	Instant Push-to-Talk Communication	
24	Real-Time Presence	Real-Time User Presence Supported	
25	GPS Tracking	Real-Time User Tracking Supported	
26	Group Calling	Group and Broadcast Calling Supported	
27	Secure Communication	Secure Nationwide Communication	
28	Cloud Integration	Motorola WAVE PTX Cloud Supported	
29	Mobile Integration	Mobile Application Integration Supported	
30	Dispatch Integration	Compatible with WAVE Dispatch Console	
32.	**ECB & PA Control Desk Call Station**		
1		Indoor IP based ECB and PA Control Desk Call Station with 8-inch Touch Display for centralized emergency communication and public announcement management	
2		High resolution capacitive touch screen display for call handling, monitoring and system operation	
3		Gooseneck Microphone Kit for live voice announcements and emergency communication	
4		Integrated Desk Mount Kit suitable for control room / ICCC desk installation	
5		Supports PA and ECB call initiation, monitoring and call management functions	
6		Native IP / Ethernet based communication architecture	
7		Supports SIP / VoIP based communication and integration with centralized server	

SNo.	Parameter	Specifications	Compliance (Yes/No)
8		Built-in speaker and microphone for handsfree communication	
9		User friendly graphical interface for quick access and operation	
10		Multiple programmable function keys for emergency and broadcast operations	
11		Supports live announcements, recorded messages and zone selection	
12		Full duplex audio communication with echo cancellation and noise reduction	
13		Compatible with centralized PA and ECB management software platform	
14		Real-time status indication and event monitoring facility	
15		Suitable for 24x7 continuous operation in ICCC / Control Room environment	
33.	**IP Phones**		
1		Enterprise Grade IP Phone with SIP based communication support	
2		HD Voice Quality with wideband audio support	
3		Backlit LCD / Color Display for call status and user interface	
4		Supports multiple SIP accounts and line appearances	
5		Full Duplex Speakerphone with Acoustic Echo Cancellation	
6		Dual 10/100/1000 Mbps Ethernet Ports with integrated switch	
7		Power over Ethernet (PoE) support as per IEEE 802.3af	
8		Supports handset, handsfree and headset operation modes	
9		Programmable DSS / Soft Keys for quick dialing and functions	
10		Supports Call Hold, Transfer, Forward, Conference and Redial functions	
11		Supports Caller ID, Call Waiting and Call History	
12		XML / Web based configuration and centralized provisioning support	
13		Supports VLAN, QoS and Network Security features	
14		Compatible with SIP based IP PBX and Unified Communication platforms	

SNo.	Parameter	Specifications	Compliance (Yes/No)
15		Supports IPv4 / IPv6 network protocols	
16		Wall Mount and Desktop installation support	
17		RJ45 Ethernet Interface for LAN connectivity	
18		Low power consumption with energy efficient operation	
19		Operating Temperature suitable for indoor office environment	
20		CE / FCC / RoHS compliant product	
34.	**Public Address System (PAS)**		
1	Field Side Equipment	Should have the capability to control individual PAS i.e. to make an announcement at select location (1:1) or multiple locations (1: many). The PAS should also support both, Live and Recorded inputs	
2		IP amplifier with minimum 250 Watts, Class D.	
3		Native IP connectivity, no convertors to be used	
4		0 to 55 C Temperature rating for Amplifier	
5		Automatic Volume Control	
6		Frequency Response: 50Hzto 15000 Hz for Amplifier	
7		2Inputs and 1 Output relay contacts in Amplifier	
8		Speaker: Minimum 4 Speakers 30 W capacity	
9		Frequency Response of Speaker 350 -10,000Hz	
10		Line Monitoring Facility for speakers	
11		IP 55 Housing for amplifier	
1	Control room Side Equipment	Central Software based server application capable of working on virtual environment/cloud with 100% redundancy for DC & DR. System should be capable for Secure connection of device as per international standard ISO 27001:2013.	
2		Access control mechanism would be also required to establish so that the usage is regulated.	
3		Integration with VaMS and Command and control centre or any other component if required	
4		PA Master Controller to have facility for multiple mic inputs, direct dialling buttons, LCD screen	
5		Software Client for making Calls to PA and ECB	
6		Automatic Volume Control, Call recording of all PA announcements with date and time	
7		Operating temperature for control desk 0 to +60C	
35.	**Dispatcher Subscription**		

SNo.	Parameter	Specifications	Compliance (Yes/No)
1	Application Type	Browser-Based Dispatch Application	
2	Deployment	Cloud Based Centralized Communication Platform	
3	Accessibility	Accessible from Any Internet Connection	
4	Communication Type	Push-to-Talk Voice Dispatching	
5	Talkgroup Monitoring	Monitor up to 20 Talkgroups	
6	Communication Modes	One-to-One, Group and Broadcast PTT	
7	Presence Monitoring	Available, DND and Offline Status Monitoring	
8	Talkgroup Scanning	Priority Talkgroup Scanning Supported	
9	Voice Messaging	Voice Message Fallback Supported	
10	Call Logging	Call Logging Supported	
11	Call Recording	Call Recording Supported	
12	Supervisory Override	Supervisory Override Supported	
13	Alerts	Alert Notification Supported	
14	Messaging Support	Integrated Multimedia Messaging	
15	Text Messaging	Text Message Support up to 2000 Characters	
16	Image Sharing	GIF, JPEG, PNG Image Sharing Supported	
17	Video Sharing	MPEG-4 Video Sharing Supported	
18	Audio Sharing	AAC and MP3 Audio Sharing Supported	
19	Document Sharing	PDF Attachment Sharing Supported	
20	Location Sharing	Real-Time Location Sharing Supported	
21	Mapping Capability	User Mapping and Tracking Supported	
22	Geofencing	Geofencing Supported	
23	Location History	Location Replay and History Supported	
24	Address Search	Point of Interest and Address Search Supported	
25	In-Map Communication	Communication through Map Interface Supported	
26	Processor Requirement	Intel Core i5 or Above Recommended	
27	RAM Requirement	Minimum 8 GB RAM	
28	Operating System	Windows 8.1/10 Pro or Enterprise	
29	Browser Support	Internet Explorer 11 and Chrome 45+	
30	Internet Requirement	Minimum 2 Mbps Internet Connectivity	
31	Audio Device Support	Headsets, Microphones and Speakers Supported	
32	Platform Compatibility	Compatible with WAVE PTX Ecosystem	
33	Dispatch Control	Centralized Team Coordination Supported	
34	Real-Time Coordination	Real-Time Communication and Resource Management	
35	Secure Access	Secure Login and Access Control Supported	

Group 5: Network and Communication Infrastructure

SNo.	Parameter	Specifications	Compliance (Yes/No)
36.	**Core Router**		

SNo.	Parameter	Specifications	Compliance (Yes/No)
1		1U/2U or chassis based 19 Inch Rack mountable Ethernet switch.	
2		All Functionalities of Switch shall be IPv6 compliant, and it should work on IPv6 Platform without any additional hardware/ software.	
3		The switch shall be supplied with the latest Modular OS version	
4		Switch should support minimum 48x10/25G SFP28+ Ports and 8x40/100G QSFP28 from day 1.	
5		Must offer system performance of at least 4000 Gbps switch bandwidth and 1000 Mpps forwarding rate.	
6		Switch should support dedicated/Virtual stacking with minimum 400Gbps of Cluster Capacity. Minimum 3meter Stacking cables and accessories should be supplied along with switches. Switch should support stacking upto 8 units	
7		Switch must support dual redundant FAN modules and Hot Swappable power supplies	
8		Switch should support minimum 16GB RAM and 64GB flash/SSD	
9		Should support minimum 250K MAC or more	
10		Should support minimum 200K IPV4 Routes	
12		Should support minimum 100K IPV6 Routes	
13		Should support IEEE standards: IEEE 802.3ab, EEE 802.3z, IEEE 802.3ae, IEEE 802.3ad, IEEE 802.1ab, IEEE 802.1v	
14		Vlan Ids:4000 or more and 4K active VLANs	
15		Switch should support IEEE 802.1d Spanning tree protocol	
16		Switch should support 802.1s MSTP (Multiple instances of STP)	
17		Switch should support 802.1w RSTP (Rapid spanning tree), Should support IP FRR/IRF /ITU G.8032 or equivalent for ring resiliency for fast/better convergence from day 1	
18		Networking Solution should support Loop Free topology with STAR, RING and Mesh architecture.	
19		Switch should support 802.3ad Link Aggregation	
20		Switch should support atleast 8 nos of 802.1p Priority Queues per port.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
21		Switch should support IGMP Snooping, MLD v1/v2 from day 1, Multicast Groups-4K or more, switch should support BGP, OSPFv3 and EVPN/VxlAN or equivalent for future scalability.	
22		Switch should support Port mirroring/RSPAN	
23		Switch should support shall be supported with Ipv4/Ipv6: Static routing, PBR, RIPv2, RiPng and OSPFv2/v3	
24		Switch should be scalable to support BGP and IS-IS in same hardware.	
25		Switch should support MAC and 802.1 X authentication	
26		Switch should support Radius and TACACS	
27		Switch should support out-of-band management Port, Console Port and USB port.	
28		Switch should support RMON (4 Groups)	
29		Switch should support network management via SNMPv1/v2/v3	
30		Switch Shall support Netflow/IPFIX/sflow for flow exports.	
31		Switch should support for Config/image upload and download from TFTP/FTP servers.	
32		Switch should support 80MB or more packet buffer	
33		The switch shall conform to IEC-60950/CSA-60950/EN-60950/UL-60950, EN 300 386, CISPR 32, Class A, IEC 61000-4-5 standard for safety requirements of information technology equipment.	
34		The offered equipment must be able to operate in the following environmental conditions	
35		Operating temperature: 0°C to 45°C	
36		Relative Humidity: 10% to 95% Non-condensing	
37		Switch MAC ID should reflect the OEM/Manufacturing Entity Name and it Should be available public domain to verify the same.	
38		OEM Should be present in Latest IDC/Gartner Reports.	
39		Switching OEM Should have 15 years+ presence in India.	
37.	**Core Switches**		

SNo.	Parameter	Specifications	Compliance (Yes/No)
1		1U/2U or chassis based 19 Inch Rack mountable Ethernet switch.	
2		All Functionalities of Switch shall be IPv6 compliant and it should work on IPv6 Platform without any additional hardware/ software.	
3		The switch shall be supplied with the latest Modular OS version	
4		Switch should support minimum 48x10/25G SFP28+ Ports and 8x40/100G QSFP28 from day 1.	
5		Must offer system performance of at least 4000 Gbps switch bandwidth and 1000 Mpps forwarding rate.	
6		Switch should support dedicated/Virtual stacking with minimum 400Gbps of Cluster Capacity. Minimum 3meter Stacking cables and accessories should be supplied along with switches.Switch sould support stacking upto 8 units	
7		Switch must support dual redundent FAN modules and Hot Swappable power supplies	
8		Switch should support minimum 16GB RAM and 64GB flash/SSD	
9		Should support minmum 250K MAC or more	
10		Should support minmum 200K IPV4 Routes	
12		Should support minmum 100K IPV6 Routes	
13		Should support IEEE standards:-IEEE 802.3ab,EEE 802.3z,IEEE 802.3ae,IEEE 802.3ad,IEEE 802.1ab,IEEE 802.1v	
14		Vlan Ids:4000 or more and 4K active VLANs	
15		Switch shold support IEEE 802.1d Spanning tree protocol	
16		Switch shold support 802.1s MSTP (Multiple instances of STP)	
17		Switch shold support 802.1w RSTP (Rapid spanning tree), Should support IP FRR/IRF /ITU G.8032 or equivalent for ring resiliency for fast/better convergence from day 1	
18		Networking Solution should support Loop Free topology with STAR ,RING and Mesh architecture.	
19		Switch should support 802.3ad Link Aggregation	
20		Switch should support atleast 8 nos of 802.1p Priority Queues per port.	
21		Switch should support IGMP Snooping, MLD v1/v2 from day 1 , Multicast Groups-4K or more , switch should support BGP ,OSPFv3 and EVPN/VxlAN or equivalent for future scalability.	
22		Switch should support Port mirroring/RSPAN	
23		Switch should support shall be supported with Ipv4/Ipv6: Static routing, PBR, RIPv2,RiPng and OSPFv2/v3	

SNo.	Parameter	Specifications	Compliance (Yes/No)
24		Switch should scalable to support BGP and IS-IS in same hardware.	
25		Switch should support MAC and 802.1 X authentication	
26		Switch shuld support Radius and TACACS	
27		Switch should support out-of-band management Port,Console Port and USB port.	
28		Switch should support RMON (4 Groups)	
29		Switch should support network management via SNMPv1/v2/v3	
30		Switch Shall support Netflow/IPFIX/sflow for flow exports.	
31		Switch should support for Config/image upload and download from TFTP/FTP servers.	
32		Switch should support 80MB or more packet buffer	
33		The switch shall conform to IEC-60950/CSA-60950/EN-60950/UL-60950,EN 300 386,CISPR 32, Class A,IEC 61000-4-5 standard for safety requirements of information technology equipment.	
34		The offered equipment must be able to operate in the following environmental conditions	
35		Operating temperature: 0°C to 45°C	
36		Relative Humidity: 10% to 95% Non-condensing	
37		Switch MAC ID should reflect the OEM/Manufacturing Entity Name and it Should be available public domain to verify the same.	
38		OEM Should be prensent in Latest IDC/Gartner Reports.	
38.	**L3 Managed Distribution Switch**		
1		1U/2U or chassis based 19 Inch Rack mountable Ethernet switch.	
2		All Functionalities of Switch shall be IPv6 compliant, and it should work on IPv6 Platform without any additional hardware/ software.	
3		The switch shall be supplied with the latest Modular OS version	
4		Switch should support minimum 48x10/25G SFP28+ Ports and 8x40/100G QSFP28 from day 1.	
5		Must offer system performance of at least 4000 Gbps switch bandwidth and 1000 Mpps forwarding rate.	
6		Switch should support dedicated/Virtual stacking port with minimum 400Gbps of Stacking/Cluster	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		Capacity. Minimum 3meter Stacking cables and accessories should be supplied along with switches. Switch should support stacking upto 8 units	
7		Switch must support dual redundant FAN modules and Hot Swappable power supplies	
8		Switch should support minimum 16GB RAM and 64GB flash/SSD	
9		Should support minimum 250K MAC or more	
10		Should support minimum 200K IPV4 Routes	
11		Should support minimum 100K IPV6 Routes	
12		Should support minimum 100K multicast entries/routes	
13		Should support IEEE standards: IEEE 802.3ab, EEE 802.3z, IEEE 802.3ae, IEEE 802.3ad, IEEE 802.1ab, IEEE 802.1v	
14		Vlan Ids:4000 or more and 4K active VLANs	
15		Switch should support IEEE 802.1d Spanning tree protocol	
16		Switch should support 802.1s MSTP (Multiple instances of STP)	
17		Switch should support 802.1w RSTP (Rapid spanning tree), Should support IP FRR/IRF /ITU G.8032 or equivalent for ring resiliency for fast/better convergence from day 1	
18		Networking Solution should support Loop Free topology with STAR, RING and Mesh architecture.	
19		Switch should support 802.3ad Link Aggregation	
20		Switch should support at least 8 nos of 802.1p Priority Queues per port.	
21		Switch should support IGMP Snooping, MLD v1/v2 from day 1, Multicast Groups-4K or more, switch should support BGP, OSPFv3 and EVPN/VxlAN for future scalability.	
22		Switch should support Port mirroring/RSPAN	
23		Switch should support shall be supported with Ipv4/Ipv6: Static routing, PBR, RIPv2, RiPng and OSPFv2/v3	
24		Switch should be scalable to support BGP and IS-IS in same hardware.	
25		Switch should support MAC and 802.1 X authentication	
26		Switch should support Radius and TACACS	

SNo.	Parameter	Specifications	Compliance (Yes/No)
27		Switch should support out-of-band management Port, Console Port and USB port.	
28		Switch should support RMON (4 Groups)	
29		Switch should support network management via SNMPv1/v2/v3	
30		Switch Shall support Netflow/IPFIX/sflow for flow exports.	
31		Switch should support for Config/image upload and download from TFTP/FTP servers.	
32		Switch should support 32MB or more packet buffer	
33		The switch shall conform to IEC-60950/CSA-60950/EN-60950/UL-60950, EN 300 386, CISPR 32, Class A, IEC 61000-4-5 standard for safety requirements of information technology equipment.	
34		The offered equipment must be able to operate in the following environmental conditions	
35		Operating temperature: 0°C to 45°C	
36		Relative Humidity: 10% to 95% non-condensing	
37		Switch MAC ID should reflect the OEM/Manufacturing Entity Name, and it Should be available public domain to verify the same.	
38		OEM Should be present in Latest IDC/Gartner Reports.	
39		Switching OEM Should have 15 years+ presence in India.	

Group 6: Cyber Security Infrastructure

SNo.	Parameter	Specifications	Compliance (Yes/No)
39.	**Firewall**		
A1	A. Hardware Architecture	The appliance-based security platform should provide firewall, Application Control, Antimalware/Antivirus,Web Filtering and IPS functionality in a single appliance from day one	
A2		The appliance should support atleast 8x 10GE SFP+/SFP, 8 x GE RJ45, dual Hot Swappable Power Supply from dayone. And also have provison for 4x GE Slots SFP along with dedicated management and HA port.	
A3		The appliance hardware should be a multicore CPU architecture with a hardened 64-bit operating system.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
A4		Proposed Firewall can be ASIC based in nature / open architecture based on multi-core cpu to protect & scale against dynamic latest security threats.	
B1	B. Performance & Scalability	Firewall shall support Transparent and NAT/Route modes concurrently using Virtual Contexts. Minimum 10 Virtual Firewall licenses required	
B2		Firewall shall support a minimum of 30 Gbps application control throughput/ firewall throughput in real-world environment including AVC (Application Visibility Control) and logging	
B3		Firewall shall deliver minimum 25 Gbps NGFW Threat Prevention throughput with all features enabled (Application, NGIPS, AV, AM, logging).	
B4		Architecture shall separate Control Plane (management) and Data Plane (security and network processing). This separation can be physical or logical.	
B5		Firewall must be a single appliance with redundant fans and hot-swappable power supplies	
B6		Firewall shall support at least 12 million concurrent sessions.	
B7		Firewall shall support at least 700,000 connections per second.	
B8		Firewall shall support 50 Gbps IPSec VPN throughput or higher.	
B9		Appliance must include TPM chip to protect cryptographic keys and passwords from tampering or phishing.	
C1	C. Firewall Features	Firewall shall support access-rules based on IPv4/IPv6, user/groups, application, geolocation, URL, zones, VLAN, etc.	
C2		Support for manual and auto NAT, Static NAT, Dynamic NAT, Dynamic PAT.	
C3		Support for NAT64, NAT66, and DHCPv6 from day one.	
C4		Support Static, OSPF, OSPFv3, and BGP routing protocols.	
C5		Support multicast protocols including IGMP and PIM	
C6		Detect, log, and take action against network traffic using over 3,500 application signatures.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
C7		Application signatures must be manually and automatically updatable.	
C8		Administrator shall define application control policies by application group or list	
C9		System must provide automatic inspection for traffic using non-standard ports.	
C10		IPS module must support 18,000+ signatures and import Snort/Suricata format	
C11		Provide IP reputation feeds with regularly updated global databases.	
C12		Support integration of third-party and custom IP reputation feeds, including global blacklist	
C13		Support DNS-based threat intelligence feeds.	
C14		OEM must operate its own global Threat Intelligence and Analysis Center.	
C15		Detection engine should identify reconnaissance, buffer overflow, VoIP, and P2P attacks	
C16		Support geo-location-based threat detection and blocking. Ability to sanitize Microsoft Office documents and PDF files by stripping harmful active content (hyperlinks, embedded media, JavaScript, macros) while preserving textual content integrity	
C17		Engine must detect variants of known and unknown threats (zero-day).	
C18		Provide SD-WAN features with path measurement (jitter, latency, packet loss).	
C19		Support URL-based threat intelligence feeds.	
C20		Support WAN load balancing algorithms – volume, session, IP-based, spillover.	
C21		Provide AV and file blocking per-policy or user group for HTTP, SMTP, POP3, IMAP, FTP, etc	
C22		Integrated web content filtering solution without external devices/modules.	
C23		Query real-time URL database with 110M+ websites categorized in 70+ categories	
C24		Allow web filtering per policy or per user for HTTP and HTTPS traffic.	
C25		Include blocking of web plug-ins (ActiveX, Java, Cookies), URL blocking, and exempt lists	

SNo.	Parameter	Specifications	Compliance (Yes/No)
C26		Firewall must support post-quantum cryptography algorithms such as ML-KEM, BIKE, HQC, Frodo	
C27		Integrated traffic shaping and bandwidth management functionality	
D1	D. High Availability	Support Active/Active and Active/Standby failover modes.	
D2		Support EtherChannel or equivalent for redundancy and failover control	
D3		Support redundant interfaces to ensure link-level redundancy.	
D4		Support IEEE 802.3ad link aggregation for bandwidth increase and redundancy.	
D5		Include integrated redundant hot-swappable power supplies.	
D6		Support automatic traffic redirection from failed links to healthy ones.	
E1	E. Management & OEM Criteria	Firewall on-device manager and proposed external manager should have GUI access over standard browser. In case of firewall manager fails, device should be access through on device manager using standard browser for networks and security policy	
E2		OEM must not be blacklisted in the last three years by any government body.	
E3		OEM must have a local representative or authorized support presence in the India.	
E4		Include 5-year licenses for all major services – Firewall, VPN, IPS, URL Filtering, Anti-Bot, APT, Antivirus, Anti-Spam, DNS and 24x7 Support.	
E5		All throughput must be achieved from a single appliance. Clustering/stacking (N+1) not accepted.	
E6		Firewall family or operating system must have valid EAL4 certification or higher.	
E7		Proposed solution must preferably have same Single OS at all layers to manage and provide complete centralized control over office networking. Solution must have facility to have security grid with automation capability to create key stiches using inetgrations out of the box for firewalls, Switches, routers and AP's which should be monitored basis regular triggers to provide automated action capability. All the events/logs	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		from Firewall, Switches, APs, Router should be stored in a single soluton proposed.	
E8		OEM should be present in latest Gartners Leader quadrant	
E9		Complete solution should be from single OEM to support secured, homogeneous to support seamless intergartion solution.	
40.	**WAF & Server Load Balancer**		
1		The appliance should be high performance purpose built next generation multi-tenant hardware with Network function virtualization . The Appliance should support multiple network functions virtualization with dedicated hardware resources for each virtual instance. The Device should have 2 Virtual Instance from day 1 and scalable upto 12 Instances on license upgarde. It should also run 3rd party and open source network functions on same appliance like Linux- CenOS/Ubuntu based applications.	
2		The Appliance should have 8*10GbE SFP+ ports and minimum 4 TB HDD and dual power supply.	
3		The WAF OEM should be different from Firewall OEM and WAF OS and SLB OS should be different.	
4		The appliance should support L7 RPS should be 10 Million and support 50 K SSL TPS for RSA 2K key, 35 K SSL TPS for ECDSA P25.	
5		WAF should supports in-line modes- Bridge, routed, transparent mode, reverse proxy mode and out of path (TAP/SPAN).	
6		The WAF should support negative and positive security model The positive Security recognizes the characteristics of normal application traffic by automatic traffic learning in order to form the positive security model (whitelist model), which allows only traffic matching these whitelists to pass.	
9		The WAF should detect and block SQL injection attacks, support injection detection based on get, post, cookie, etc., and support the detection of code bypassing SQL injection; The WAF should prevent XSS cross-site attacks, including the detection of storage and reflection cross-site	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		methods, and the detection of code bypassing XSS cross-site attacks.	
10		The solution should provide full ipv6 support and OEM should be IPv6 gold-certified. OEM should be listed vendor for ipv6 phase-2 certification.	
11		The WAF should protect against command injection attacks, such as Linux and Windows system command execution; The WAF should protect against common types of injection attacks, including SSI, LDAP, XPATH, mail header, file injection, etc.	
13		The WAF should protect application layer and Network DOS attacks, support application layer resource consumption type denial of service attack detection and denial of service attack detection caused by malformed data and malformed protocol.	
14		The WAF should prevent attacks against session tampering and hijacking, including attacks against cookie, session and user parameters, and can prevent attacks such as directory traversal attacks and CSRF attacks.	
15		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.	
16		The solution should support Multi-level virtual service policy routing,-Static, default and backup policies for intelligent traffic distribution to backend servers	
17		The WAF should support Web Anti-Defacement (WAD) function to detect and prevent the defaced web pages from being returned to the client. It should returns the cached original web page to make the anti-defacement effects unnoticeable or returns a 503-error page to the client to end the service.	
18		The solution should provide application & server health checks for well-known protocols such as ARP, ICMP, TCP, DNS, RADIUS, HTTP/HTTPS, RTSP etc.	
19		The solution must support Single Sign-On (SSO) for web-based applications and web-based file server	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		access. It should also support SAML secure application access	
20		The solution should provide comprehensive and reliable support for high availability and N+1 clustering based on Standard VRRP Per VIP based Active-active & active standby unit redundancy mode.	
21		The access control of black- and whitelists should be supported, and global and local settings should be supported.	
22		The WAF support access control based on client source IP, server URL and port.	
23		The WAF should support IP reputation subscription to protect against Botnet, Cybercrime, Phishing, SPAM, TOR, scanners etc.	
24		The WAF should support Access control based on GeoIP regions: The administrator can generate IP blacklist based on the IP region table to achieve the region-based access control. The WebUI can generate and display region-based statistics graphs/security events.	
25		The WAF should have auto-learning feature, enhancing network security through real-time traffic analysis. It automatically generates IP subnets for protection by continuously learning network patterns. One for querying the status and details of the network model learning, and another for resetting the learned model to refine security strategies.	
26		The Web Application Firewall (WAF) must support HTTP/2 and HTTP/1.1 for both communications.	
32		WAF should support Browser fingerprint for identification and tracking technology that relies on various characteristics such as browser type, version, installed plugins, screen resolution, and other system parameters of the user's network environment rather than IP addresses.	
33		The solution should support certificate parser, and solution should integrate with client certificates to maintain end to end security and non-repudiation. It should support Certificate format as	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		"OpenSSL/Apache, *.PEM", "MS IIS, *.PFX", and "Netscape, *.DB".	
34		It should support advance functions Authoritative name sever, DNS proxy/DNS NAT, full DNS server with DNSEC, DNS DDOS, application load balancing from day one. It should be capable of handling complete Full DNS bind records including A,MX, AAAA, CNAME, PTR, SOA etc.	
35		The solution should have license upgrade feature on same appliance to support machine authentication based on combination of HDD ID, CPU info and OS related parameters i.e. mac address to provide secure access/authentication to corporate resources.	
36		The WAF should have reports which can be generated according to time, and the report graphics can be set to column, bar, and pie charts. Reports can be exported to multiple formats, such as PDF, HTML and Excel; The WAF should have reports which can be automatically generated on a regular basis, such as daily, weekly, and monthly; the reports can be sent to the designated recipient via FTP or email.	
41.	**DDOS Protection**		
1		The proposed solution should have dedicated DDoS protection device not as add on license Feature on ADC and NGFW. The solution should have external bypass functionality.	
2		The proposed solution should detect and mitigate both network- layer DDoS attacks and advanced application layer attacks.	
3		The proposed solution should have the capability to be configured in detect as well as protect mode.	
4		The proposed solution should be deployed in inline mode (L2 & L3) and SPAN/TAP mode (out of path).	
5		The proposed solution should prevent suspicious traffic for threats and blocking malicious traffic.	
6		The Solution must have 50 K SSL TPS for RSA 2K key and 35 K SSL TPS for ECDSA P25 and L7 RPS should be 6 million and L4 CPS should be 4 million.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
7		The Appliance should have dedicated 8x10GbE SFP+ ports (SX Fiber incl.) and Minimum 4TB SSD and dual power supply.	
8		Should protect ICMP attacks: ICMP floods, ping floods, smurf, IP Spoofing, LAND attack, Teardrop, IP Option Timestamp, IP Option Route Record, IP Option Source Route, Ping of Death, Tracert, ICMP Redirect, ICMP Unreachable, ICMP Large Packet.	
9		The solution should support protection policy for L3 protocol (IP), L4 protocol (TCP, UDP, ICMP) and layer 7 protocol SSL hanshake attack	
10		Should protect TCP based attacks: TCP SYN Flood, TCP SYN-ACK Flood, TCP ACK Flood, TCP FIN/RST Flood, TCP Connection Flood, TCP Slow Connection, TCP Abnormal Connection, TCP Fragments Flood, Defence WinNuke, TCP Error Flag	
11		Should protect UDP based attacks: UDP Flood, UDP Fragment Flood, UDP Fingerprint, Fraggle, UDP Large Packet	
12		Should protect HTTP & HTTPS based attacks: HTTP GET Flood, HTTP POST Flood, HTTP Slowloris, HTTP Slow POST, HTTP URL monitor, SSL Handshake, SSL Renegotiation	
13		Should protect DNS based attacks: DNS Cache Poisoning Defense, DNS Length Check Defense , DNS NxDomain Defense, DNS Query Flood Defense , DNS Reply Flood Defense, DNS TTL Check , DNS Source Authentication	
14		The solution should support Brute Force attack mitigation	
15		The solution should support the behaviour based DDOS mitigation.	
16		The solution should provide the traffic AUTO learning function for the DDOS traffic monitoring	
17		The traffic Auto learning threshold can be applied automatically after auto learning completed.	
18		The solution should provide the multi-level DDOS mitigation policy and different mitigation action based on DDOS traffic type.	
19		The solution should Access control list for IP, TCP, UDP, DNS, HTTP, URL, blacklist and whitelist,	

SNo.	Parameter	Specifications	Compliance (Yes/No)
20		The solution should support Access control list based on inbulit GeoIP with configurable duration.	
21		The solution should be able to import third party IP database through File or URL.	
22		The system should support IPv4 and IPv6 dual stack without deteriorating performance	
23		The solution shall have built-in high availability (HA) features in the following mode: Active-Passive, Active-Active using VRRP	
24		The solution shall be able to immediately support both IPv4 and IPv6 and implements dual stack architecture.	
25		The solution must be able to integrate with existing management system via SNMP version 3 and SNMP version 2	
26		The solution must provide the latest Management Information Base (MIB) file for SNMP operation.	
27		The solution log shall contain the following information: Attack logging like Source IP, Destination IP, Destination Port, Group Name, Service Name, Protocol Attack Type, Action, Anomaly Count, DDoS Attack and logging to Syslog	
28		The solution shall provide the flexibility of performing configuration via GUI and command base remotely.	
29		The solution should support IPv6 as well as IPv4 and have the ability to turn IPv4/IPv6 traffic to IPv6/IPv4 traffic on the backend and the solution should be IPv6 ready logo certified from the day 1 and OEM should be listed vendor for ipv6 phase-2 certification	
30		The solution shall be able to export syslog to existing syslog server and SIEM system.	
31		The solution shall support the provisioning of the reports - Attack reports -top sources, targets, attack type, Attack Severity Distribution, Attack Source Region	
32		The solution must be able to generate summary attack report of daily/weekly/monthly	
33		The solution must provide packet capture for debugging.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
42.	**Network Intrusion Detection System (IDS)**		
1		Scope: Supply, install, configure, test, commission Network Intrusion Detection System (NIDS) sensors and central manager with licenses for entire contract period; integrate with existing SOC/SIEM.	
2		Compliance: Adherence to CERT-In Directions dated 28-Apr-2022 incl. 6-hour incident reporting, 180-day log retention in India, and NTP sync with NIC/NPL traceable servers.	
3		Architecture: Out-of-band NIDS sensors (SPAN/TAP); option to run inline in fail-open for PoC only; centralized manager (appliance/VM) with MFA and RBAC.	
4		IPv4/IPv6 Dual Stack: Full detection on IPv4 and IPv6 traffic; interoperability per TEC IPv6 conformance guidance.	
5		Detection Methods: Signature, protocol anomaly, and behavior/ML-based detection for L2–L7 including HTTP/2/3, TLS/QUIC, DNS, SMTP, SMB, SQL, SSH.	
6		Encrypted Traffic Analytics: JA3/JA3S, SNI/cert telemetry and flow analytics without mandatory TLS decryption.	
7		Threat Intel & Updates: Automatic signature/intel updates; STIX/TAXII support; air-gapped update option; update caching on-prem.	
8		ICS/OT/IoT Awareness: Protocol decoders for Modbus, DNP3, BACnet, MQTT, CoAP where applicable.	
9		Analytics & Triage: Risk scoring, ATT&CK mapping, campaign grouping, deduplication/suppression, custom correlation, incident timelines.	
10		Forensics: PCAP extraction with configurable retention; chain-of-custody metadata; case evidence packaging for CERT-In reporting.	
11		Logging & Retention: Store security logs >=180 days locally; export to SIEM via syslog/CEF/LEEF/JSON with hashing.	
12		Time Synchronization: All components sync with NIC/NPL or traceable NTP servers; drift alerts.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
13		Performance (per sensor): Sustained IDS throughput >=5 Gbps; >=100k new flows/sec; >=2M concurrent flows; >=3 Mpps; PCAP buffer >=2 TB.	
14		High Availability: Manager and sensors support HA/cluster; rolling upgrades; health monitoring (SNMP/REST).	
15		Security of Platform: Hardened OS, secure boot, signed updates, FIPS-validated crypto or equivalent; no default/hidden accounts; mutual TLS for mgmt.	
16		Access Control: Granular RBAC (viewer/analyst/incident-manager/admin), MFA, JIT access, dual-control for destructive actions.	
17		Integrations: SIEM/SOAR/ticketing via REST/syslog/TAXII; CERT-In/NIC-CERT incident export templates; NTP evidence in reports.	
18		Reporting: CERT-In 6-hour incident templates; monthly SOC posture reports; log-retention attestations.	
19		Manageability: Backup/restore of policies/signatures/cases; DR runbooks; multi-tenant segregation for multi-dept operations.	
20		QoS/Resilience Context: DNS abuse/BGP anomaly monitoring hooks and dashboards (read-only analytics) for resilience posture.	
23		Warranty & Support: 5-year comprehensive OEM warranty with signature/content updates; TAC L3 support in India.	
27		Data Governance: All logs/PCAP/telemetry stored/processed within India; cloud components (if any) must support audit & data residency.	
43.	**Security Information & Event Management (SIEM)**		
1		The Next generation SIEM should encompass logs, packet, user and end point data in single platform with added context and threat Intelligence Should provide complete network forensics and visibility through deep packet inspection high speed packet capture and analysis. SIEM for Logs and deep packet inspection should be from Single OEM.	
2		The solution should be able to collect raw logs in real-time to a Central log database from any IP	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		Device (existing/proposed) including but not limited to: • Networking devices (Router/switches etc.) • Security devices (IDS/IPS, Anti- Virus/HIPS, Patch Management, Firewall/DB Security solutions etc.) • Operating systems (Linux/Windows/SOLARIS OS etc.) • Enterprise Platforms (Servers, Storage, Database etc.) • Logs from All City Networks devices and sensors to identify malicious traffic using standard Protocols.	
3		The solution should be able to collect the logs in an agent/ agent less manner and store the same to a Central log database from any IP Device. The raw logs should be time stamped, compressed to optimize storage utilization. The solution should be able to perform Real time monitoring of log data and perform Network traffic analysis to identify threats. Should be able to monitor traffic from L2 to L7 layer metrics conversations in the network and share the network data (Packet + Meta data) to generate alerts as they happen in real time by using single correlation and detection rules within SIEM.	
4		The solution should collect the entire log sent by the devices by guaranteeing chain of custody for regulatory compliance should provide pre-defined report templates. The reports should also provide reports out of the box such as PCI- DSS, HIPAA, SOX, NERC, FISMA, ISO, GLBA, GPG13.	
5		The SIEM & Log Monitoring solution should be from a different OEM than the Prevention Security solutions like F/W, IPS, HIPS, AV, DLP, EMS, FIM, APN, NPM and Encryption.	
6		The solution must have three-tiered architecture with physical segregation of duties between them. Collectors to collect and forward, Logger to retain raw and normalized logs for forensics, audit and compliance and forward to correlation which should do real time correlation and must be able to handle twice the peak EPS and 3 times the Burst	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		EPS without queuing or dropping logs. All three tiers/components (Collection, Correlation and Management) should be sized and licensed for same amount of EPS count. Platform must be on VM's or physical servers. Solution must be Sized for 10,000 Sustained EPS considering event size of 500 bytes or 400 GB per day and all the infrastructure including Total storage (Min 150 TB from day 1) should be considered on the above parameters without any assumptions. Solution should support online log management with up to 6 months of log retention.	
7		SIEM solution should have provision for parser creation for unsupported / home grown applications. The solution should also support API integration with other proposed devices.	
8		SIEM solution should be able to receive and consume global threat feeds automatically and manually.	
9		The Solution should detect common events like D-DOS / DOS, Scanning, Worms, Unexpected application services. (e.g., tunnelled protocols, backdoors, use of forbidden application Protocols), Policy violations, etc. The solution should profile traffic by TCP and UDP Port.	
10		The proposed system should encrypt the logs or the channel of logs transmission before sending to the correlation engine. The System should also compress the logs before transmission to the log correlation engine.	
11		Should be able to provide complete packet-by-packet details pertaining to one or more session of interest including Session replay, page reconstruction, image views, artefact & raw packet and object extractions.	
12		The SIEM solution should provide correlation against data collected from multiple devices across the network. There should be no limitation or license sholuld not be based on number of devices to be supported. Any addition in no. of devices should have no cost impact on department.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
13		The SIEM solution should be capable to obtain security logs from different sources and integrate the logs for correlation and analysis.	
14		Should have a minimum predefined set of rules to monitor the complete file system must be able to whitelist files that may have suspicious behaviours but are in fact legitimate	
15		The solution sould have ability to detect high privilege access anomaly detection for misuse, sharing, or takeover. Uses behavioural analysis to identify any anomalous activity that falls outside of the user normal pattern of life. Unusual Credential use - models the times and devices normally used by each username, and alerts when there is an unusual combination	
16		The product must provide the ability to schedule reports to run hourly, daily, weekly or monthly. There must be numerous output formats and delivery options for scheduled reports.	
17		Solution must collect log from all log-generating devices including application and it must not have limitation in number of devices it will collect logs from.	
18		Solution must secure logs at source itself by identification of logs using a stateless (no key management) architecture of format preserving encryption. The solution should display the type of data being transported via HTTP into and out of the network (i.e. text, image, video etc.), The solution should support session reconstruction and object extractions from sessions. It should have ability to recover files which are in the payload of network traffic such as PDF, exe, etc.	
19		The solution must provide value in assisting in adhering to audit requirements, alerting of non-compliance and providing necessary reports that can be used during an audit.	
20		The solution must be capable of detecting attacks in real-time through advance correlation unsing single rule for logs and packets to pivot on the exact payload for reconstruction and generate digital evidence .The central correlation engine database	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		should be updated with real time security intelligence updates provided by the SIEM OEM	
21		The solution must be able to detect malicious payload in network traffic. Detect and reconstruct files back to its original type. Detect hidden or embedded files. Detect and flag out renamed files	
22		The proposed solution must be able to provide the complete platform to perform Network forensics solution.Solution should create indexes for payload objects and not just rely on header information should have out of the Box Packet Parsers for identification and analysis of protocols and other header metrics. The solution should provide network traffic insight by a. Classifying protocols and applications b. Reconstructed file such as a Word document, image, Web page, VOIP and system files c. Deep-packet inspection d. Cross correlation for Analysis & Aggregation e. Reconstruct sessions and analyze artifacts f. Preview artifacts and attachments	
23		Network traffic inspection to detect suspicious activities such as different malware family used by Threat Actor groups, TTPs used for malicious activities and lateral movements or The solution should detect and respond to threats based on MITRE ATT&CK tactics and techniques and report the appropriate MITRE ATT&CK tactic and /or technique in the platform user interface, provide support for STIX/TAXII integrations.	
24		The logger layer must have storage to store online logs and must be capable of providing dashboards like failed logins, bandwidth talkers, late or early login etc. Should provide RBAC to generate dashboard for different stakeholders	
25		Support disaster recovery setup with warm / hot back up for Console, Correlation and Collection with ready to function state at any given time and system should display number of use cases deployed mapped which would provide a view on security posture.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
26		Provides the following but not limited to real time alerting based on observed security threats: DDoS, Worm outbreak, Botnets, Exploitation and attack attempts, Attack sources vis-à-vis specific attacks and top exploits, compromised systems, Unexpected application services (e.g., tunnelled protocols, backdoors, use of forbidden application Protocols),attack vectors such as the following are detected, Web Login brute force attempts, Should provide complete network visibility through deep packet inspection through high speed packet capture and analysis.	
27		The solution should be software based SIEM with hardened OS, database platform. Collection, Co-relation and Console layer should be physically and logical separate.	
28		Raw and normalized Logs should be handled and stored in tamper proof way across SIEM solution. Alter/modify tamper rights w.r.t Raw logs. SIEM should support syslog over TLS to ensure that logs can be transported in a confidential manner.	
29		The solution must provide a complete audit trail and accountability during the incident handling for forensic investigations. The system should have ability to perform event forensics to determine what really happened before, during, and after the event.	
30		SIEM should have the ability to natively collect logs from logstash.	
31		Search Performance – Structured Data: The proposed solution search performance must be capable of searching through millions of structured (indexed) events	
32		The proposed solution must provide a common Content Editor to create or modify resources within the system. All aspects of this editor must apply to the development of rules, reports, dashboards and any other resource that will be created in the system.	
33		Solution shoud use self-learning behavioural analysis to dynamically model each user,	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		probabilistically identifying any anomalous activity that falls outside of the user normal pattern of life.	
34		Solution should be focused on unsupervised machine learning so that it does not require any human/analyst to create data science models. Solution should support Machine Learning (ML) driven risk scores and risk profiles for user	
35		To avoid generating too many false positives, solution must support deploying correlation rules in test mode to test the rules thoroughly before deploying in production mode. The solution should allow a wizard-based interface for rule creation. The solution should support logical operations and nested rules for creation of complex rules.	
36		The solution should have the capability to send notification messages and alerts through email, Syslog and Scripts, etc.	
37		Solution should support Machine Learning (ML) driven risk scores and risk profiles for user	
38		SIEM UEBA solution should not be app based or plugin based and should be dedicated machine learning engine running on appliance	
39		UEBA in built in SIEM should be a pure unsupervised machine learning engine with no need to configure any settings not limited to baselines, thresholds, decays, risks scores. Also, there should not be any need to configure thresholds through settings during learning or production phase	
40		Quoted SIEM Solution must have its presence in India for more than 10 years OEM of the SIEM must have at least 3 deployments of more than 20000 Sustained EPS in Government of India organization. Relevant documents for the same to be provided along with technical bid.	

Group 7: ICCC and Control Center Infrastructure

SNo.	Parameter	Specifications	Compliance (Yes/No)
44.	**Integrated Command & Control Center (ICCC) Platform**		

SNo.	Parameter	Specifications	Compliance (Yes/No)
1	Solution & Platform	The Command & Control solution should be implemented and complied to the industry open standards based Commercial-of- the-shelf (COTS) products.	
2		The Command & Control solution should be Microservice based & support containerization of services.	
3		The Command & Control solution should be Cloud ready and has to be Cloud Agnostic.	
4		System shall have capability to host on On-premise and Cloud Data Centre.	
5		System must have load balancing and high availability to meet SLA.	
6		System must provide a comprehensive and industry accredited Unified Open Standard API (Application Program Interface) or SDK (Software Development's Kit) to allow interfacing and integration with existing systems, and future application and sensors which will be deployed on the field.	
7		System shall have capability to support future integration with department's future initiatives	
8		System should support Interoperability and Portability (replicable). System shall be able to integrate with any type of sensor platform or vertical solutions being used for the smart services irrespective of the technology used.	
9		Solution should not be dependent on proprietary hardware.	
10		System shall be able to normalize the data coming from different devices of same type or different data sources and should support Common Standard Open Data Models for data normalization (i.e. Different VMS from different OEMs, etc.) and display unified view of alerts	
11	Command & Control Center Components	Web / Client server to manage client requests. Client should provide web-based access to dashboards, one-stop portals / GUI to event information, overall status, and details.	
12		ICCC, through its integration with various smart devices and smart applications, will act as a Decision Support System for city administration to	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		respond to the real time events by consuming data feeds from different data sources and by processing information out of these data sets	
13		The system should provide language support for both Hindi and English language on the user interface. The user should have the option to select either of the 2 languages	
14		Mobility: should enable app-based access to monitor alerts, and SOPs to mobile users.	
15		Security & Roles – should manage roles definition for internal as well as external access	
16		Centralized data storage for operational data : Should provide facility for centralized storage of operational data	
17	Incident Management	Should have an ability to display alarm condition through visual display and audible tone	
18		Should have an ability to simultaneously handle multiple alarms from multiple workstations	
19		Should have an ability to sort alerts/Incident according to different configurable columns	
20		Should have an ability to automatically prioritize and display multiple alarms and status conditions according to pre- defined parameters such as alarm type, location, sensor, severity, etc.	
21		Should display the highest priority alarm and associated data / video in the queue as default, regardless of the arrival sequence	
22		Should support comprehensive reporting on event status in real time manually or automatically by a sensor, CCTV video feeds, any other sensor.	
23		Should support for sudden critical events and linkage to standard operating procedures automatically without human intervention. Operator should be able to associate pre-defined forms and attachments while handling an Incident in runtime.	
24		Should have an ability to export alarm report in various formats including pdf, jpeg, html, txt formats	
25		Should support for multiple incidents with both segregated and/or overlapping management and response teams.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
26		Should support Geospatial rendering of event and incident information.	
27		Should support plotting of area of impact using polynomial lines to divide the area into multiple zones on the GIS maps.	
28		Should support incorporation of resource database for operation and mobilizing the field resources for response. Resources may be assigned and mobilized as per the defined Standard Operating Procedure in the system	
29	GIS Display	Shall view the environment through geospatial map and shall support OGC WMS standard.	
30		Shall allow user to view sensor and related name from the displayed map.	
31		Shall allow all resources, objects, sensors and elements on the map to be georeferenced such that they have a real-world coordinate.	
32		Shall visually display a camera sensor and icons for different category of cameras.	
33		Shall visually display an alarming sensor on map.	
34		Shall visually differentiate sensor alarm on map through color and icon identifiers	
35		Shall allow user to choose camera and take live video image snapshot and save to file from any camera	
36		Shall allow user to choose camera from map to move PTZ cameras	
37		Shall allow user to choose camera to play, pause, stop, fast-forward, rewind, and play recorded video from preset time	
38	Video Display	Shall view live or recorded video from CCTV Camera / VMS	
39		Shall display video in 1x1, 2x2, 3x3 and 4x4 window formats	
40		Shall enable operator to specify video windows to be displayed in matrix	
41		Shall view either live or recorded video can be displayed in the video matrix window.	
42		Shall enable matrix settings to be saved per user	
43		Shall play, fast-forward, rewind, pause, and specify time to play recorded video	

SNo.	Parameter	Specifications	Compliance (Yes/No)
44		Shall take a video still image (snapshot) from live or recorded video	
45		Shall have the capability to move PTZ cameras	
46		Shall enable video snapshot to be taken and saved from any windowpane in the matrix view	
47		Shall rotate through multiple video views based on predefined video camera sequence and duration.	
48		Shall enable user to only view and control video for which they have been assigned permissions by the administrator	
49	Standard Operations Procedures (SOP)	Command & Control Center should provide for defining un-limited number of configurable and customizable standard operating procedures through graphical, easy to use interface.	
50		Standard Operating Procedures should be established, approved sets of actions considered to be the best practices for responding to a situation or carrying out an operation.	
51		The users should be able to edit the SOP, including adding, editing, or deleting the activities.	
52		In run time, users shall be able to modify tasks statuses on the list. They should be able to complete tasks, cancel them and mark them as 'in progress'. Completing a task shall be as easy as checking a box.	
53		The users should be able to also add comments to or stop the SOP (prior to completion).	
54		There should be provision for automatically logging the actions, changes, and commentary for the SOP and its activities, so that an electronic record is available for after- action review.	
55		The system will support post incident analysis through different reports generated that will enable the authorities to find gap/deficiency in the incident handling and help improve and/or rewrite SOPs	
56		The SOP Tool should have capability to define the following activity types:	
57		Manual Activity - An activity that is done manually by the owner and provide details in the description field.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
58		Automation Activity - An activity that initiates and tracks a particular work order and select a predefined work order from the list.	
59		If-Then-Else Activity - A conditional activity that allows branching based on specific criteria. Either enter or select values for Then and Else.	
60		Notification Activity - An activity that displays a notification window that contains an email template for the activity owner to complete and then sends an email notification.	
61	Field Mobile User	The ICCC shall support mobile apps support for Android smartphones and tablets. The mobile apps shall communicate with the Mobile Server of the DC over any WiFi or mobile GPRS/3G/4G connection.	
62		Mobile apps shall communicate with the ICCC via a Mobile. Communication between the mobile device and the Mobile Server shall support encryptions.	
63		Mobile User shall receive the alert from Operator to address the incident on field	
64		Mobile user shall provide function to update the status of alert, share input via message and close alert activities are completed	
		Mobile user shall be allowed to create emergency situation alert via SOS button	
65		Mobile app allows user to Upload Attachment directly through camera & user should be able to View/Remove attachment before uploading	
66	Health Monitoring	Should provide icon-based user interface on the GIS map to report non-functional device.	
67		Should also provide a single tabular view to list all devices along with their availability status in real time.	
68		The ICCC shall monitor the health of the system, log health related events, and calculate statistics like uptime, downtime.	
69	Dashboard & Key Performance Indicator	Real time dashboard on the situational view should provide information about security information so that officials have better understanding of what is happening on the ground.	
70		Should provide dashboard filtering capabilities that enable end-users to dynamically filter the data in	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		their dashboard based upon criteria, such as region, dates, product, brands, etc. and capability to drill down to the details	
71		Command & Control Center should be able to facilitate measurement or criteria based on performance policies against defined SLAs	
72		Green indicates that the status is acceptable, based on the parameters for that KPI, no action is required.	
73		Yellow indicates that caution or monitoring is required, action may be required.	
74		Red indicates that the status is critical and action is recommended.	
75	Reporting Requirement	The system should provide Informative and aesthetic dashboards providing simple clicks and friendly visualization	
76		The solution should generate reports of alerts/incidents based on the area, sensor type or periodic or any other customer reports as per choice of the administrators	
77		The reports generated can be scheduled to specific stakeholders on daily, weekly or any custom basis without manual intervention	
78	Collaboration Tools	The CCC platform should have the capability to bring in multiple stake holders automatically into a common collaboration platform for ex: persistent chat rooms in response to a SOP defined to handle a particular event.	
79	Authentication	Use authentication information to authenticate individuals and/or assign roles.	
80		Support LDAP authentication mechanism.	
81	Authorization & Access Control	Comprehensive policy-based security administration to provide all users specific access based on user's responsibilities for relevant web components. Maintenance of authorization policy in a central repository for administration purposes.	
82		Should support to enable assignment of permissions to groups, and administration of access control across multiple applications and resources. Secure administration tools to manage users, groups, permissions and policies.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
83	Multi-Level Access Control & Management	User will be defined with Geography boundary to load the relevant sensors and alerts	
84		Escalation of alerts to next level if not addressed in defined time limit	
85		Central monitoring will have complete visibility of alerts and provide guidance to field operation team	
86	Administration Activities	The Configuration UI application shall allow the administrator or users with appropriate privileges to change the system configuration.	
87		The Configuration UI shall have a home page with single-click access to various tasks.	
88		The Integrated UI shall provide links to facilitate the following functions: • Configure Site hierarchy (multi-level support expected) • Configure the Sensor systems (like VMS, FRS, PAS, ...) • Configure Users, Roles and Permissions • Configure Alert & related categories • Configure business rules and escalation rule	
89	Event correlation	Command & Control Centre should be able to correlate two or more events coming from different subsystems (incoming sensors) based on time, place, custom attribute and provide correlation notifications to the operators based on predefined business and operational rules in the configurable and customizable rule engine.	
90	Flexible single sign-on (SSO)	Support LDAP authentication mechanism	
45.	**Enterprise Management System (EMS)**		
1		NMS shall be able to monitor and configure asked switches, router and wireless access points (should be proposed against the proposed devices) and should have scalability to manage up to 5000 devices in future. NMS shall be able to manage both wired and wirelessnetworks in single pane of glass management. APM can be provided by same EMS OEM or it can be an integrated solution from other OEM. Rest all the modules should be from single OEM.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
2		NMS should be scalable to provide deep application visibility using AVC, NetFlow/Sflow,NBAR or packet inspection to recognize a wide variety of applications and SNMP.NMS should be able to provide Network topology.	
3		The proposed EMS OEM must have at least 2 deployment (in state/central Government/ PSU/BFSI) in India with 10,000 core network devices such as router, switch, firewall being monitored and their configuration is also managed in this deployment in last five years. Reference PO copy and completion/ signoff document need to be submitted.	
		The solution should be capable of running in Linux platform with time series database (not RDBMS) as backend and should be 64-bit application to fully utilize the server resources on which it is installed.	
		The organization should have ISO 45001, ISO 55000, ISO 270001, ISO 27034, SOC3 and CMMI Level 3 certification for their internal processes and certificate must be provided.	
		Proposed solution should be CIS certified and certificate must be provided.	
		Proposed solution should have IPR/copyright registered in India. Copyright certificate to be submitted.	
		Proposed solution should be ITIL v4 complied for 9 processes from Peoplecert.	
4		Should provide a customizable at-a-glance summary of all discovered devices and existing network switches to proactively identify problem areas and help prevent network downtime. The network has to be manageable at Network Operations Center(NOC) and through secured browser.	
5		Should be able to discover, configure, monitor, manage, and deploy configurations todynamically update groups of devices.	
6		Should allow flexible definitions of administrator roles and responsibilities with RBAC(Role based Access Control) for different teams.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
7		Should enable performance management by providing customizable dashboards andhistorical data visibility.	
8		Should be able to generate reports designed to summarize utilization of and traffic patternson network interfaces.	
9		Tool should provide option for the users to choose personalized GUI Color theme (Multi-Color, Dark/Light Theme), It should have Multi-Language Support so every state user can use system with in their own language. Multiple Logo supports based on the user state, system should load their state default logo. System should support Key board sort custs to navigate through different modules and perform faster actions	
10		Should have direct OEM 24x7x365 TAC support and hardware replacement warranty for 5Years.	
	Enterprise management System (EMS) - General		
11		Enterprise Management System should provide for end to end performance, availability, fault and event and impact management for all enterprise resources that encompasses the heterogeneous networks, systems, applications, databases and client infrastructure presentin the enterprise	
12		The EMS shall be able to support the proposedhardware and software Components (IT and Non-IT) deployed. The software shall be capable of providing early warning signals on the performance issues, and future infrastructure capacity augmentation. The EMS shall also support single pane / dashboard with visibility across multiple areas of applications for monitoring	
13		Following functionalities are essential and required from such EMS tools: • Availability Monitoring, Management and Reporting • Performance Monitoring, Management and Reporting • Helpdesk Monitoring, Management and Reporting • Asset Management	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		• Incident Management and RCA reporting Change and Configuration management	
14		The Service Management solution to be used for incident and problem management, Inventory& Asset management, Service Request Management, Self Service, Service level management should be built to leverage the same common Configuration Management Database (CMDB) with a unified architecture	
15		The tool should have Integrated Web based feature to build Network Diagram, No separate client window to configure network Diagram. The builder should be similar to MS Visio with all pre-loaded shapes and icons.	
16		Solution should provide for future scalability of the whole system without major architectural changes	
17		Solution should be distributed, and scalable and opento third party integration	
18		The solution should be able to monitor all the IT assets for the organization across all the location spread across including servers, network, routers, switches etc.	
19		The agent and agentless monitor should be able to collect & manage event/ fault, performance and capacity data and should not require separate collectors	
20		The solution should reduce manual customization efforts and should speed-up problem identification and resolution of the IT performance anomalies with intelligent events	
21		Solution should carry out probable cause analysis thereby helping operators to identify the root cause without having to write complex rules for correlation	
22		Should be configurable to suppress events for key systems/ devices that are down for routine maintenance or planned outage	
23		The solution should provide the mechanism for creation of knowledgebase and provision the same to the end users with the ability to search for known errors from the knowledge base	

SNo.	Parameter	Specifications	Compliance (Yes/No)
24		The solution should provide network, server, application and database performance information and alarms and should be able to show it in a single console and provide a reporting interface for all network and system components	
25		The solution should be extensible enough to support capacity planning and optimization with data collected through the deployed performance management agent or from agentless data collectors	
26		Database Monitoring: The solution should be able to monitor all the market leading database solution providers	
27		The Database monitoring should seamlessly integrate with the same EMS dashboard/ Portal and provide integration with the central event console	
28		The tool should provide the organization the ability to easily collect and analyse specific information of applications & databases	
29		The solution should manage service levels for delivery and support of business services	
30		Ability to create custom KPI metrics and scorecard/compliance reports that are updated automatically	
31		Single dashboard provides the as-is scenario by consolidating the data across the organization	
32		Should support top down dashboards with drill down capabilities into detailed information	
33		Should support comprehensive and configuration-level roll-back for changes	
34		Should support Configuration-level Control of Tasks, Objects, and Policies	
36		The configuration changes to be done on target network devices must follow an approval-based system wherein changes can be performed only after required approvals are passed. Tool must have in-built approval mechanism along with option to integrate with Change Management module of other ITSM tools for the approval process.	
37		Tool must provide an option for taking remote access via Telnet / SSH to target CLI- based Network Devices with an option to record all sessions to	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		capture all commands being executed on the remote devices. The tool must allow session relay wherein a higher-privileged user can view the ongoing CLI session of a lower-privileged user in real-time from the tool GUI. The sessions should be saved for historical analysis with flexible filter options like searching for sessions in which a particular command has been executed.	
38		It should automatically trends and provides dynamic performance baselines for applications and services	
39		It should proactively identify errors affecting end-users, instead of waiting for a call from an employee or an incident being raised	
40		It should provide comprehensive view of application performance from the end- user perspective; it should distinguish between broad and targeted slow-downs, allowing drill- down into	
41		Solution should provide DDoS reports in real time within 1 minute after detection of attack with details of IP, Ports, ASN numbers, Router Interfaces, Customers facing the attacks	
42		It should use real end user performance as one of the feed for more accurate root cause analysis and automated repair of business service performance issues	
	Technical		
43		Application monitoring parameters: • Database Monitoring Attributes • User Connections (#) • Transaction Count • Log Space Available • Deadlocks/ sec • Database Free Space (%) • Database Used Space (MB) • Disk Reads (per sec) • Disk Writes (per sec) • Cache hit ratio • Lock Memory • Average Wait Time (per table) • Buffer Cache Hit Ratio (%) • Commits (per sec)	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		• Memory Used (MB) • Percent Memory Used (%) • Availability (%) • Commits (per sec) • Percent Memory Used (%) • Buffer Cache Hit Ratio (%) • Active Instances (#)	
44		The proposed system shall support multiple types of discovery like IP range discovery including built-in support for IPv6, Seed router based discovery and discovery whenever new devices are added with capability to exclude specific devices	
45		Web Server Monitors but not limited to: • Post Requests (per sec) • Get Requests (per sec) • Errors (per sec) • Client-Side Errors (per sec)	
		Server-Side Errors (per sec) Percent Busy Connections (%)	
46		Solution should support comprehensive SLA management platform that cuts across Infrastructure Management and Service Management. For e.g. monitors and reports across different parameters like CPU utilization, disk space, response times, resolution times (e.g. incident closed on 2 hours) performance and custom parameters of an enterprise etc.	
47		The solution should have a consolidated, automated graphical report for SLA compliance with ability to drill down to reason for non-compliance	
	Discovery, Configuration and Faults: Monitoring and Management		
48		The proposed system shall support multiple types of discovery like IP range discovery including built-in support for IPv6, Seed router based discovery and discovery whenever new devices are added with capability to exclude specific devices	
49		The system shall provide discovery & inventory of physical network devices like Layer-2 & Layer-3 switches, Routers and other IP devices and shall provide mapping of LAN & WAN connectivity.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
50		The discovery shall be able to identify and model of the ICT asset.	
51		The proposed system shall provide a detailed asset report, organized by system shall provide sufficient reports that identify unused ports in the managed network infrastructure that can be reclaimed and reallocated. The proposed system shall also intelligently determine which ports are operationally dormant.	
52		The proposed system shall determine device availability and shall exclude outages from the availability calculation with an option to indicate the reason.	
53		The proposed system shall include the ability to monitor and visualize a virtualized system infrastructure by discovering and monitoring virtual machines and providing ability to depict the logical relationships between virtual servers and virtual machines.	
54		Should monitor Type of Service (ToS), Differentiated Services Codepoint (DSCP), and Per-Hop Behaviour (PHB),BGP AS and NEXT HOP	
55		The proposed solution shall have the ability to collect data from the virtual systems without solely relying on SNMP.	
56		The proposed solution shall support an architecture that can be extended to support multiple virtualization platforms and technologies.	
57		The proposed system shall support SNMPv3-based network discovery and management out- of-box without the need for any external third-party modules.	
58		The proposed system shall be able to administer configuration changes to network elements by providing toolkits to automate the following administrative tasks of effecting configuration changes to network elements like Capture running & start- up configuration, Upload configuration etc.	
	Reporting		
59		The proposed system shall provide sufficient reports pertaining to asset and change management, alarms and availability of critical	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		network resources as well as network response times for critical links.	
60		The proposed system shall able to perform real-time or scheduled capture of device configurations. It shall also provide features to capture, view & upload network device configuration.	
61		The proposed system shall able to store historical device configurations captured in the database and thereby enable comparison of current device configuration against a previously captured configuration as well as compare the current configuration against any user-defined standard baseline configuration policy.	
62		The proposed system shall be able to monitor compliance & enforce change control policies within the diverse infrastructure by providing data & tools to run compliance reports, track& remediate violations, and view history of changes.	
63		The proposed tool shall display configuration changes differences in GUI within central Console. Also this shall be able to identify which user has made changes or modifications to device configurations using the Interface.	
	Service Level Management: Monitoring and Management		
64		The proposed service management system shall provide a detailed service dashboard view indicating the health of each of the component and services provisioned as well as the SLAs.	
65		The system shall provide an outage summary that gives a high-level health indication foreach service as well as the details and root cause of any outage.	
66		The system shall be capable of managing IT and Non- IT resources in terms of the business services they support, specify and monitor service obligations, and associate users/Departments/ Organizations with the services they rely on and related Service/Operational Level Agreements. Presently, services shall include E-mail, Internet Access, Intranet and other services hosted.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
67		The Service Level Agreements (SLAs) definition facility shall support defining a set of one or more service that specify the Service obligations stipulated in an SLA contract for a particular time period (weekly, monthly, and so on).	
68		SLA violation alarms shall be generated to notify whenever an agreement is violated or is in danger of being violated.	
69		The system shall provide the capability to designate planned maintenance periods for services and take into consideration maintenance periods defined at the IT resources level. In addition, the capability to exempt any service outage from impacting an SLA shall be available.	
70		Should be able to receive flows from non-SNMP-enabled devices, like VMware vSwitch	
71		The system shall provide a historical reporting facility that shall allow for the generation ofon-demand and scheduled reports of Service related metrics with capabilities for customization of the report presentation.	
72		The system shall provide for defining service policies like Service Condition High\Low Sensitivity, Port Status High\Low Sensitivity shall be provided out of the box.	
73		The System shall have all the capabilities of a Network Management System which shall provide Real-time network monitoring and Measurement off end-to- end Network performance & availability to define service levels and further improve upon them.	
	Network Performance Monitoring, Management and Reporting: Monitoring and Management		
74		The tool shall provide a live exceptions list displaying the various health and threshold exceptions that are occurring in the managed infrastructure.	
75		The tool shall have the capability to configure different polling speeds for different devices in the	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		managed infrastructure with capability to poll critical devices	
76		This central console shall also provide all required network performance reports (including latency, threshold violations, packet errors, availability, bandwidth utilization etc.) for the network infrastructure. The proposed system shall identify over-and under-utilized links and assist in maximizing the utilization of current resources.	
77		The proposed system shall provide an integrated performance view for all the managed systems and networks along with the various threshold violations alarms in them.	
78		The proposed monitoring solution should be able to monitor network traffic by capturing flow data from network devices, including Cisco Netflow v5 or v9, Juniper J- Flow, IPFIX, sFlow, NetStream data and also sampled Netflow data. Solution must be able to store ALL flows without any rollups or loss for retention period - for security and audit purposes.	
79		The proposed system shall be able to auto-calculate resource utilization baselines for the entire managed systems and networks and allow user to set corresponding upper and lower threshold limits.	
	Application Performance Monitoring, Management and Reporting: Monitoring and Management		
80		The proposed solution shall proactively monitor all user transactions for any web- application hosted; detect failed transactions; gather evidence necessary for triage and diagnosis of problems that affect user experiences and prevent completion of critical business processes	
81		The proposed solution shall see response times based on different call parameters. For example, the proposed solution shall be able to provide CPU utilization metrics.	
82		The proposed solution shall give visibility into user experience without the need to install agents on user desktops.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
83		The proposed solution shall be able to provide the ability to detect and alert which exact end users experience HTTP error codes such as 404 errors or errors coming from the web application.	
84		The proposed system shall be able to detect user impacting defects and anomalies and reports them in real-time for Slow Response Time, Fast Response time, Low Throughput, Partial Response, Missing component within transaction	
85		The proposed system shall be able to instantly identify whether performance problems like slow response times are within or outside the Data center without having to rely on network monitoring tools.	
86		The proposed system shall be able to provide trend analysis reports and compare the user experience over time by identifying transactions whose performance or count has deteriorated over time.	
	Systems and Database Performance Monitoring, Management and Reporting: Monitoring and Management		
87		The proposed system shall address management challenges by providing centralized management across physical and virtual systems. The proposed system shall be able to monitor various operating system parameters such as processors, memory, files, processes, file systems, etc. where applicable, using agents on the servers to be monitored.	
88		It shall be possible to configure the operating system monitoring agents to monitor based on user-defined thresholds for warning/critical states and escalate events to event console of enterprise management system.	
89		It shall also be able to monitor various operating system parameters depending on the operating system being monitored yet offer a similar interface for viewing the agents and setting thresholds.	
90		The proposed solution shall support monitoring Processors, File Systems, Log Files, System Processes, and Memory etc.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
91		The proposed tool shall provide Process and NT Service Monitoring wherein if critical application processes or services fail, administrators are immediately alerted and processes and services are automatically re-started.	
92		The proposed tool shall be able to provide Log File Monitoring which enables administrator to watch system logs and text log files by specifying messages to watch for. When matching messages gets logged, the proposed tool shall notify administrators and enable to act like sending an email.	
93		The proposed database performance management system shall integrate network, server & database performance management systems and provide the unified view of the performance state in a single console.	
94		It shall be able to automate monitoring, data collection and analysis of performance from single point.	
95		It shall also provide the ability to set thresholds and send notifications when an event occurs, enabling database administrators (DBAs) to quickly trace and resolve performance- related bottlenecks.	
96		The proposed system shall provide Performance Management and Reporting Provides real- time and historical performance of physical and virtual environments enabling customers gain valuable insights of a given virtual container of the relative performance of a given Virtual Machine compared to other Virtual Machines, and of the relative performance of groups of Virtual Machines.	
97		Role based Access Enables role-based management by defining access privileges according to the role of the user.	
98		The proposed Virtual Performance Management system shall integrate latest virtualization technologies	
	Helpdesk - Monitoring, Management and Reporting		

SNo.	Parameter	Specifications	Compliance (Yes/No)
99		The proposed helpdesk system shall provide flexibility of logging, viewing, updating and closing incident manually via web interface.	
100		The proposed helpdesk system shall support ITIL processes like request management, problem management, configuration management and change order management with out-of-the-box templates for various ITIL service support processes.	
101		Each incident shall be able to associate multiple activity logs entries via manual update or automatic update from other enterprise management tools.	
102		The proposed helpdesk system shall be able to provide flexibility of incident assignment based on the workload, category, location etc.	
103		Each escalation policy shall allow easy definition on multiple escalation levels and notification to different personnel via window GUI/console with no or minimum programming.	
104		The proposed helpdesk system shall provide grouping access on different security knowledge articles for different group of users. The proposed helpdesk system shall have an updateable knowledge base for tech al analysis and further help end-users to search solutions for previously solved issues. The proposed helpdesk system shall support tracking of SLA (service level agreements) for call requests within the help desk through service types.	
105		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, web etc.	
106		The proposed helpdesk system shall integrate tightly with the Knowledge tools and CMDB and shall be accessible from the same login window.	
107		It shall support remote management for end-user &allow analysts to do the desktop sharing for any system located anywhere, just connected to internet.	
108		The proposed tool must provide an option to design dynamic workflows, lifecycle, Tasks, Notification action for each service which can be requested	

SNo.	Parameter	Specifications	Compliance (Yes/No)
	Incident Management and Root Cause Analysis Reporting		
109		Tool should have option to promote knowledge to analysts (ServiceDesk) and end users (Service Portal)	
110		Incidents shall be categorized and prioritized. While prioritizing incidents the impact and urgency of the incident shall be taken into consideration.	
111		It shall be ensured that the incident database is integrated with Known Error Database (KeDB), Configuration Management Database (CMDB). These details shall be accessible to relevant personnel as and when needed.	
112		Information security incidents and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken.	
113		Conduct regular reviews on performance of incident management activities against documented Key Performance Indicators (KPI's).	
114		Controls related to incident management need to be implemented and each implemented control shall have a documentary evidence to substantiate and demonstrate effective implementation.	
	Change and Configuration Management		
115		Change and configuration management shall be governed by the change management and configuration management policy.	
116		Change management provides information on changes, and enables better control of changes to reduce errors and disruption in services.	
117		All changes shall be initiated using change management process; and a Request for Change (RFC) shall be created. All requests for change shall be evaluated to determine the impact on business processes and IT services, and to assess whether change shall adversely affect the operational environment and introduce unacceptable risk.	
118		Controls related to change management need to be implemented and each implemented control shall	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		have a documentary evidence to substantiate and demonstrate effective implementation.	
119		The roles and responsibilities of the management shall include review and approval of the implementation of change management policies, processes and procedures.	
120		A configuration management database shall be established which stores unique information about each type Configuration Item CI or group of CI.	
121		The Configuration Management Database (CMDB)shall be managed such that it ensures its reliability and accuracy including control of update access.	
122		The degree of control shall maintain the integrity of services and service components taking into consideration the service requirements and the risks associated with the CI.	
123		Corrective actions shall be taken for any deficiencies identified in the audit and shall be reported to the management and process owners.	
124		Information from the CMDB shall be provided to the change management process and the changes to the CI shall be traceable and auditable.	
125		A configuration baseline of the attached CI shall be taken before deployment of a release into the live environment. It shall be stored in the safe environment with appropriate access control.	
126		Master copies of CI shall be recorded in the CMDB and shall be stored in secure physical or electronic libraries which shall be referenced in the configuration records. This shall be applicable to documentations, license information, and software and hardware configuration images.	
127		Master copies of CI shall be recorded in the CMDB and shall be stored in secure physical or electronic libraries which shall be referenced in the configuration records. This shall be applicable to documentations, license information, and software and hard	
	IPAM		

SNo.	Parameter	Specifications	Compliance (Yes/No)
128		IPAM solution should have complete IP discovery , IP management with historical tracking	
129		IPAM should have IP Grouping, Sub grouping and role and privileged based access.	
130		Support both IPv4 and V6 along with IP Classes	
	Asset Management		
131		IMACD Lifecycle Management with ITSM Integration: The system must provide full support for the IMACD lifecycle - including Installation, Movement, Addition, Change, and Disposal of IT assets. These IMACD processes should be seamlessly integrated with core ITSM modules such as Incident, Change, and Problem Management. For instance, if a Change Request is initiated for asset relocation, the related IMACD request must be cross-referenced and linked for traceability. All IMACD workflows should support role-based access control (RBAC) at both request and process levels, ensuring secure, permission- driven operations. Additionally, audit trails must be maintained for compliance and transparency.	
132		Asset Installation Management: The platform should allow users to initiate Asset Installation Requests covering deployment of hardware, software, and network components. These requests must include task assignments, approval workflows, and validation checkpoints to ensure that deployed asset are configured correctly and integrated seamlessly into t h e existing infrastructure. Support for dependency mapping and post-install verification is essential.	
133		Asset Movement with Intelligent Gatepass Control: The system must support Asset Movement Requests, including the generation of digital Gatepasses with customizable fields. Each Gatepass should contain QR codes for individual assets, ownership details, source and destination addresses, and movement status, signature field etc. The Gatepass should be exportable in PDF format and support scanning during transit and at the receiving location. Upon successful receipt and	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		scanning, the system should automatically update the asset's location and clear or transfer ownership accordingly.	
134		Asset Addition and Capacity Expansion Support: Users must be able to raise Asset Addition Requests for onboarding new users, devices, applications, or IT components. The process should include validation checks, approvals, asset tagging, and integration with capacity/resource planning modules. The system should track and document each addition to ensure alignment with IT policies and future scalability.	
135		Asset Disposal and Compliance Management: The system must facilitate secure and compliant Asset Disposal processes for obsolete, damaged, or redundant IT assets. This includes integration with disposal vendors, capture of disposal certificates, data sanitization logs, and final approval workflows. The platform should ensure adherence to organizational, environmental, and legal standards, and maintain disposal audit records for future reference.	
46.	**Videowall**		
	Video wall cube		
	Display Wall Screen size	70" (diagonally) with Laser Light Source complete configuration with covered base	
	Indicative Configuration	10 columns x 4 rows	
	Projection Technology	LASER DLP based Rear Projection	
	Total resolution of Video wall	Minimum wall resolution of video wall should be 320 Megapixel	
	Screen to Screen Gap	≤ 0.2 mm	
		Individual cube should be equipped with One laser bank, and the laser bank should have an array of diodes. Single or multiple diode failure should not impact image display on the screen. Multiple Laser banks not acceptable due to possibility of convergence issues	
	Brightness of engine	Min 2200 Lumens	
	Laser Safety	Minimum 1000 Laser cubes should be working in India to prove Laser safety	

SNo.	Parameter	Specifications	Compliance (Yes/No)
	Brightness Uniformity	Minimum 95 %	
	Dust Prevention	Should be IP6X certified. Test certificate should be submit as proof along with technical bid submission	
	Light Source Lifetime	Lifetime of Light Source in normal Mode : 1,25,000Hrs	
	Remote	IR remote control should also be provided for quick access	
	Inputs	1 no. of Display Port, DVI and HDMI each	
	Screen Support	Screen should be minimum 3 layers with a Hard Backing to prevent bulging	
	Heat Dissipation	Less Than 1400 BTU/h – Normal mode	
	Power	Dual Redundant and Hot Swappable Power Supply. This should be built inside the cube for fail safe operation with cooling features	
		Power supplies extended or kept outside the cube are not acceptable	
	Eco mode	Less than 350 Watt	
	Cooling Inside Cube	Any advanced cooling mechanism and Cooling mechanism should not have any hazardous liquid.	
	Remote management	Remote management through IP for parameter adjustment. Should be able to control & monitor individual cube, multiple cubes.	
	through IP		
	Access	Rear only	
	Pixel clock	Min 162 MHz or higher to ensure flicker less display	
	Source Redundancy	System should able to switch to secondary input if primary input is not available.	
		System should also automatically switch back to primary input from secondary input as soon as the primary input is available again.	
	Cube Depth	Cube Depth - 550 ±5 % mm	
	Operating conditions		
	Temperature	10°C-40°C | 50°F-105°F	
	Humidity	Up to 80% non-condensing	
	Video wall controller		
	The network-based solution should consist of a set of encoders and decoders, which can encode Digital or Analog		

SNo.	Parameter	Specifications	Compliance (Yes/No)
	signals and transmit them over the network. The decoders should be able to decode these signals and display up to 64 sources per channel. The decoders should have high accuracy frame-sync to enable multiple decoders to form a prefect video wall. It should be possible to show any of the input sources or all of the input sources in any position on the wall, in any size and any configuration. The system should support automatic format detection for plug and play simplicity. Adding a source or display unit to the system should only entail adding an encoder or a decoder. The quantity of encoders should be equal to the inputs to the system; the quantity of the decoders should be equal to the no of displays in the system. The encoder and decoders should meet the minimum specification as follows.		
	ENCODER		
	Parameter	Desired Specification	
	Input	HDMI 2.0/ DP1.2 support up to 3840x 2160@ 60 Hz	
	Input Color Depth	Color Depth 8 /10bits per pixel	
	Input Channels	Channels 1	
	Ethernet	Ethernet Gigabit 1000 BASE-T	
	Interface	2x RJ-45, Redundant LAN port	
	Protocols	Protocols DHCP, UDP,TCP/IP	

SNo.	Parameter	Specifications	Compliance (Yes/No)
	IP Address	IP Address Static IP address, Automatic IP address	
	Power on Ethernet	Support POE	
	KVM	Support IP KVM function	
	MTBF	> 100,000 Hours	
	Supported Resolutions	Minimum Up to 3840x 2160 @ 60 Hz	
	Power Requirement	100-240 VAC	
	Operation Temperature	Minimum range 0-40 deg. C	
	Display processor		
	Parameter	Desired Specification	
	Output	HDMI 2.0 support up to 3840x 2160@ 60 Hz	
	Color Depth	8/10 bits	
	Channel	Channels 1	
	Ethernet	Gigabit 1000 BASE-T	
	Interface	2x RJ-45, Redundant LAN port	
	Power on Ethernet	Support POE	
	Protocols	DHCP, UDP, TCP/IP	
	IP Address	Static IP address, Automatic IP address	
	KVM	Support IP KVM function	
	Image Processing	Max. 64 free window in one display	
		High tap filter for image scaling	
		Support H2.64/H.265/ MPEG4 Decoding	
		Accurate synchronization for display wall	
		Bezel Compensation	
		Window title with vector texts	
	MTBF	> 100,000 Hours	
	Power Requirement	100-240 VAC	
	Operation Temperature	Minimum range 0-40 deg. C	
	SERVER SPECIFICATIONS		
	CPU	CPU: Processor: Intel Xeon E3-1230 v5 Processor (Quad Core, 3.40 GHz, 8M Cache, 80W) or above;	
	Memory	8GB UDIMM, 2400MT/s, Single Rank, x8 Data Width or above;	
	Network	1000-M LAN port*2;	
	OS	Windows Server 2008/2012/2016（64 bits	
	HDD	240GB SSD SATA Mix Use 6Gbps 512n 2.5in Hot-plug Drive or above;	

SNo.	Parameter	Specifications	Compliance (Yes/No)
	WALL MANAGEMENT SOFTWARE		
	Architecture	Browser & Server based Architecture	
	Web browser login	User should be able to login the server with Internet Explorer. There should be no need to install any additional software on the control computer.	
	Layouts	Should support static layout and automatic layout creation, editing, loading, and deleting. Any layout should be loaded in under 1 sec (irrespective of size of display & number of windows)	
	Multiple Display Support	Software should able to manage multiple displays simultaneously including status monitoring, video window control and properties setup.	
	Preview of signals	Software should able to preview video signals before opening window on display wall	
	Drag & Drop	Operator should be able to preview the content of video/RGB signal by dragging the signal source into the signal preview window should be possible	
	Preview of signals	The system software should support at least 5 RGB / Video signals preview at the same time.	
	Multiple concurrent users	Software should support multiple users managing a display wall or more display walls at the same time.	
	Layout Scheduler	All the Layouts can be scheduled as per user convenience	
	Auto Launch of Layouts	Software should support auto launch of Layouts according to specified time event by user	
	Log file	Software should support user log file management	
	Offline Layouts	It should be possible to create offline layouts	
	No of input source per channel	It should support at least 48 signal sources displaying in one display unit simultaneously with freely scalable windows.	
	Playback	The software GUI should be able to show the live view of all the sources on the browser	
	Grid management	System software should able to manage Videowall region into multiple regions as per user requirements.	
	Pre window option	User should be able to see multiple signal source in one window with specified time interval and with user defined sequence.	
	Wi-Fi Control	User should be able to control complete system through IPAD and Android system over Wi-Fi	

SNo.	Parameter	Specifications	Compliance (Yes/No)
47.	**Workstations**		
1	Processor	Intel Core Ultra 7 265K (20 Core 3.9GHz) or better	
2	RAM	32 GB DDR5 5600 MT/s to be supplied.	
		Support upto 128GB DDR5 5600 MT/s	
3	Storage	512 GB M.2 NVMe SSD to be supplied	
		Support upto 3x M.2 NVMe SSD	
		Support upto 3x 3.5” HDD, front accessible	
4	Chipset	Intel W880 workstation class chipset	
5	Graphic Card	1x Nvidia RTX2000 ADA 16GB GPU to be supplied.	
		Support upto Nvidia RTX Pro 6000 Blackwell workstation edition.	
6	Network	1x 1GbE and 1x 5GbE	
7	Expansion Slots	4 – PCIe add-in slots (1- Gen5 x16 + 3- x4 of mixed Gen3/Gen4)	
8	I/O Ports	USB Type A – 2 in front and 2 in rear	
		USB Type C – 2 in front and 2 in rear	
		1 – RJ45 1GbE	
		1 – Global headset jack (audio in/out combo)	
9	Power	Support for 360W, 500W and 1500W PSU.	
		Suitable PSU to be provided as per system requirement.	
10	OS	Windows 11 Pro	
11	Monitor	Dual 24” monitors should be supplied from the same OEM	
12	Keyboard & Mouse	Wired Keyboard & Mouse from same OEM	
13	Optical Drive	8x DVD+/-RW	
14	Form Factor	32L mid-tower for better PSU/GPU headroom	
15	Security Features	SafeID with ControlVault 3+: Dedicated hardware credential vault, FIPS 140-3 Level 3 certified.	
		SafeBIOS & Indicators of Attack: Off-host BIOS / firmware verification and telemetry to detect tampering at device level; integrated with industry-leading security tools.	
		TPM 2.0, Digital Device Identity and Secured Component Verification (DDI), Certificate Based Authentication (CBA) and Authenticated BIOS Interface (ABI)	
16	Product Certification	BIS, Energy Star and EPEAT	

SNo.	Parameter	Specifications	Compliance (Yes/No)
17	OEM Certification	ISO9001, ISO27001 and ISO45001	
18	Warranty	5 years On-site comprehensive Next Business Day warranty with 24x7x365 remote hardware support. The warranty details along with the offered BOM should be available online on the support website of the OEM.	
48.	**Keyboard Joystick for PTZ**		
1	Joystick Type	3-axis proportional joystick with Pan / Tilt / Twist Zoom control	
2	PTZ Control	Real-time proportional PTZ movement with variable speed control	
3	Preset Control	Support for PTZ preset call and preset programming	
4	Buttons	Minimum 8	
5	Housing	Metal and plastic	
6	Power	DC12V-2A	
7	Interface	1 Ethernet port, IEEE 802.11b/g/n	
8	Connectors	Minimum USB2.0	
9	Operating temperature	14°F-131°F (-10°C~55°C)	
10	Operating Humidity	20%~80% Frostless	
11	Storage Temperature	14°F-140°F (-10°C-60°C)	
12	Storage Humidity	0-90% Frostless	
13	Product Certification	CE/FCC/BIS	
49.	**LED TV 55”**		
1	Screen Size (Diagonal) (cm)	53.5 - 55.5	
2	Panel Type	Twisted Nematic (TN)	
3	Resolution (Pixels)	1920 x 1080 (Full HD)	
4	Aspect Ratio	16:09	
5	Brightness (Nits)	250	
6	Native Contrast Ratio (Minimum)	1000:01:00	
7	Viewing Angle (Horizontal: Vertical) (Degree)	170:160	
8	Response Time (millisecond)	5 milliseconds	
9	Antiglare Coating	No	
10	Split Screen Feature	Available	
11	Inbuilt Speakers	Available	

SNo.	Parameter	Specifications	Compliance (Yes/No)
12	VGA Port	Available	
13	HDMI Port	Not Available	
14	DVI-D Port	Available	
15	Display Port	Not Available	
16	Power Consumption in Operating Mode (Maximum) (Watt)	19.5	
17	Power Consumption in Sleep Mode (Maximum) (Watt)	0.45	
18	Mounting Arrangement	Table Mount	
19	TCO Certification	TCO-07	
20	BIS Registration under CRS of Meity	Yes	
21	Operating Temperature Range (Degree Celsius)	0-40 Degree C	
22	Operating Humidity (%RH)	20% - 80%	
23	Power Supply	230V AC, 50 Hz	
24	Type Of Power Supply	External	
25	On Site OEM Warranty (Year)	5	

Group-8: Data Center, Servers & Storage Infrastructure

SNo.	Parameter	Specifications	Compliance (Yes/No)
50.	**Application & Failover Application Server**		
1	Application Server	1U 10x2.5" Chassis	
2		General Computing - Power Efficiency	
3		Data Center Environment 30 Degree Celsius / 86 Degree Fahrenheit	
4		32 Core, 2.3GHz Processor	
5		1U Performance Heatsink	
6		32GB DDR5 6400MHz (2Rx8) RDIMM	
7		Select Storage devices - no configured RAID required	
8		RAID 8i 4GB Flash PCIe Gen4 12Gb Adapter	
9		1U 4x2.5" SAS/SATA Backplane	

SNo.	Parameter	Specifications	Compliance (Yes/No)
10		M.2 RAID SATA/NVMe Enablement Kit	
11		M.2 480GB Read Intensive NVMe SSD	
12		10GBASE-T 2-port Ethernet Adapter	
13		x16/x16 PCIe Gen5 Cable Riser	
14		Full Height + Low Profile Riser Cage	
15		1300W 230V/115V Titanium Hot-Swap Power Supply	
16		2.8m, 10A/100-250V, C13 to C14 Jumper Cord (India)	
17		1U Performance Fan Module	
18		1U Standard Media Bay	
19		Toolless Slide Rail Kit	
20		TPM 2.0 with Secure Boot	
21		Enable IPMI-over-LAN	
22		Intrusion Cable	
23		3yr Base Warranty	
24		1U Security Bezel	
25		Operating System & Licensing	
26		Windows Server 2025 Addl Lic	
27		Windows Server 2025 Standard Additional License (16 core) (No Media/Key) (POS Only)	
28		Windows Server 2025	
29		Windows Server 2025 Standard (16 core) - MultiLang (not preinstalled)	
30		Registration only	
31		Win Svr Standard 2025 to 2022 Downgrade Kit-Multilanguage	
32		Drop-in-the-Box	
33		Additional Licensing	
34		Windows Server 2025 Standard Additional License (16 core) (No Media/Key) (POS Only)	
35		Win Svr Standard 2025 to 2022 Downgrade Kit-Multilanguage	
36		Windows Server 2025 Standard (16 core) - MultiLang (not preinstalled)	
37		Management Software	
38		Advanced Server Management Software, Per Endpoint w/5 Yr SW S&S	

SNo.	Parameter	Specifications	Compliance (Yes/No)
39		Registration only	
40		Per Managed Endpoint w/5 Yr SW S&S	
41		Support & Services	
42		Server Support 24X7 4HR Response	
43		Support Duration - 60 Months	
44		24x7 4hr Response	
45		Installation	
46		Server Installation	
47		Hardware Installation (Business Hours)	
48		Add-On Service	
49		Keep Your Drive (KYD) Add-On	
50		Duration - 60 Months	
	Failover Application Server		
1		1U 10x2.5" Chassis	
2		General Computing - Power Efficiency	
3		Data Center Environment 30 Degree Celsius / 86 Degree Fahrenheit	
4		32C 225W 2.3GHz Processor	
5		1U Performance Heatsink	
6		32GB DDR5 6400MHz (2Rx8) RDIMM	
7		Select Storage devices - no configured RAID required	
8		RAID 8i 4GB Flash PCIe Gen4 12Gb Adapter	
9		1U 4x2.5" SAS/SATA Backplane	
10		M.2 RAID SATA/NVMe Enablement Kit	
11		M.2 480GB Read Intensive NVMe SSD	
12		10GBASE-T 2-port Ethernet Adapter	
13		x16/x16 PCIe Gen5 Cable Riser	
14		Full Height + Low Profile Riser Cage	
15		1300W 230V/115V Titanium Hot-Swap Power Supply	
16		2.8m, 10A/100-250V, C13 to C14 Jumper Cord (India)	
17		1U Performance Fan Module	
18		1U Standard Media Bay	
19		Toolless Slide Rail Kit	

SNo.	Parameter	Specifications	Compliance (Yes/No)
20		TPM 2.0 with Secure Boot	
21		Enable IPMI-over-LAN	
22		Intrusion Cable	
23		1U Security Bezel	
24		3yr Base Warranty	
25		OS & Licensing	
26		Windows Server 2025 Addl Lic	
27		Windows Server 2025 Standard Additional License (16 core) (No Media/Key) (POS Only)	
28		Windows Server 2025	
29		Windows Server 2025 Standard (16 core) - MultiLang (not preinstalled)	
30		Registration only	
31		Win Svr Standard 2025 to 2022 Downgrade Kit-Multilanguage	
32		Drop-in-the-Box	
33		Additional Licensing	
34		Windows Server 2025 Standard Additional License (16 core) (No Media/Key) (POS Only)	
35		Win Svr Standard 2025 to 2022 Downgrade Kit-Multilanguage	
36		Windows Server 2025 Standard (16 core) - MultiLang (not preinstalled)	
37		Management Software	
38		Server Management Software, Per Endpoint w/5 Yr SW S&S	
39		Registration only	
40		Per Managed Endpoint w/5 Yr SW S&S	
41		Support	
42		Server Support 24X7 4HR RESP	
43		Premier Support	
44		Months	
45		24x7 4hr Resp	
46		Installation	
47		Server Installation	
48		Hardware Installation (Business Hours)	
49		Add-On	

SNo.	Parameter	Specifications	Compliance (Yes/No)
50		Server Keep Your Drive Add-On	
51		KYD	
52		Duration 60 Months	
51.	**Recording Server**		
1	Recording Server	Recording Server 2U : 2U Rack Server – 3yr Base Warranty	
2		2U 12x3.5" Chassis	
3		General Computing - Power Efficiency	
4		Data Center Environment 30 Degree Celsius / 86 Degree Fahrenheit	
5		16C 150W 2.3GHz Processor	
6		2U Performance Heatsink	
7		16GB DDR5 6400MHz (1Rx8) RDIMM	
8		Select Storage devices - no configured RAID required	
9		RAID 16i 4GB Flash PCIe Gen4 12Gb Adapter	
10		3.5" 20TB 7.2K SATA 6Gb Hot Swap 512e HDD	
11		2U 12x3.5" SAS/SATA Backplane	
12		M.2 RAID SATA/NVMe Enablement Kit	
13		M.2 480GB Read Intensive NVMe SSD	
14		10GBASE-T 2-port Ethernet Adapter	
15		x16 Rear Direct PCIe Riser Slot	
16		1300W 230V/115V Titanium Hot-Swap Power Supply	
17		2.8m, 10A/100-250V, C13 to C14 Jumper Cord (India)	
18		2U High Performance Fan Module	
19		Toolless Slide Rail Kit	
20		2U EIA Latch Standard	
21		TPM 2.0 with Secure Boot	
22		Enable IPMI-over-LAN	
23		2U Security Bezel	
24		Intrusion Switch Cable Kit	
25		3 Years Base warranty	
26		Controller / Management	
27		Advanced Server Management Controller License	
28		Controller Premium Feature Enablement (FOD)	

SNo.	Parameter	Specifications	Compliance (Yes/No)
29		Operating System	
30		Windows Server 2025	
31		Windows Server 2025 Standard (16 core) - MultiLang (not preinstalled)	
32		Registration only	
33		Win Svr Standard 2025 to 2022 Downgrade Kit-Multilanguage	
34		Drop-in-the-Box	
35		Additional Licensing	
36		Win Svr Standard 2025 to 2022 Downgrade Kit-Multilanguage	
37		Windows Server 2025 Standard (16 core) - MultiLang (not preinstalled)	
38		Management Software	
39		Server Management Software, Per Endpoint w/5 Yr SW S&S	
40		Registration only	
41		Per Managed Endpoint w/5 Yr SW S&S	
42		Support	
43		Server Support 24X7 4HR RESP	
44		Premier Support	
45		Months	
46		24x7 4hr Resp	
47		Installation	
48		Server Installation	
49		Hardware Installation (Business Hours)	
50		Add-On	
51		Server Keep Your Drive Add-On	
52		KYD	
53		duration 60 Months	
	Failover Recording Server		
1		2U 12x3.5" Chassis	
2		General Computing - Power Efficiency	
3		Data Center Environment 30 Degree Celsius / 86 Degree Fahrenheit	
4		16C 150W 2.3GHz Processor	
5		2U Performance Heatsink	

SNo.	Parameter	Specifications	Compliance (Yes/No)
6		16GB DDR5 6400MHz (1Rx8) RDIMM	
7		Select Storage devices - no configured RAID required	
8		RAID 16i 4GB Flash PCIe Gen4 12Gb Adapter	
9		3.5" 20TB 7.2K SATA 6Gb Hot Swap 512e HDD	
10		2U 12x3.5" SAS/SATA Backplane	
11		M.2 RAID SATA/NVMe Enablement Kit	
12		M.2 480GB Read Intensive NVMe SSD	
13		10GBASE-T 2-port Ethernet Adapter	
14		x16 Rear Direct PCIe Riser Slot	
15		1300W 230V/115V Titanium Hot-Swap Power Supply	
16		2.8m, 10A/100-250V, C13 to C14 Jumper Cord (India)	
17		2U High Performance Fan Module	
18		Toolless Slide Rail Kit	
19		2U EIA Latch Standard	
20		TPM 2.0 with Secure Boot	
21		Enable IPMI-over-LAN	
22		2U Security Bezel	
23		Intrusion Switch Cable Kit	
24		3yr Base Warranty	
25		Controller / Management	
26		Server Management Controller Premium License	
27		Controller Premium Feature Enablement (FOD)	
28		Operating System	
29		Windows Server 2025	
30		Windows Server 2025 Standard (16 core) - MultiLang (not preinstalled)	
31		Registration only	
32		Win Svr Standard 2025 to 2022 Downgrade Kit-Multilanguage	
33		Drop-in-the-Box	
34		Additional Licensing	
35		Win Svr Standard 2025 to 2022 Downgrade Kit-Multilanguage	

SNo.	Parameter	Specifications	Compliance (Yes/No)
36		Windows Server 2025 Standard (16 core) - MultiLang (not preinstalled)	
37		Management Software	
38		Server Management Software, Per Endpoint w/5 Yr SW S&S	
39		Registration only	
40		Per Managed Endpoint w/5 Yr SW S&S	
41		Support	
42		Server Support 24X7 4HR RESP	
43		Premier Support	
44		Months	
45		24x7 4hr Resp	
46		Installation	
47		Server Installation	
48		Hardware Installation (Business Hours)	
49		Add-On	
50		Server Keep Your Drive Add-On	
51		KYD	
52		Duration 60 Months	
52.	**Analytics Server**		
1		2U 2.5"/EDSFF 3.S Chassis	
2		General Computing - Power Efficiency	
3		Data Center Environment 25 Degree Celsius / 77 Degree Fahrenheit	
4		64C 350W 2.4GHz Processor	
5		2U Performance Heatsink	
6		64GB DDR5 6400MHz (2Rx4) RDIMM	
7		Select Storage devices - no configured RAID required	
8		RAID 16i 4GB Flash PCIe Gen4 12Gb Adapter	
9		2.5" 3.84TB Read Intensive SATA 6Gb HS SSD SED	
10		2.5" 1.92TB Read Intensive SATA 6Gb HS SSD SED	
11		2U 8x2.5" SAS/SATA Backplane	
12		10GBASE-T 2-port OCP Ethernet Adapter	
13		High-speed PCIe Gen5 VPI Adapter (NDR 400Gb class, OSFP, single port)	

SNo.	Parameter	Specifications	Compliance (Yes/No)
14		High-performance PCIe Gen5 GPU Accelerator, ~140GB memory class, passive cooling	
15		NDR 400Gb compatible optical transceiver module	
16		x16 Cable Riser Slot (high power GPU support up to 600W)	
17		x16 Rear Riser Slot	
18		x16 Rear Direct Riser Slots	
19		2700W 230V Titanium Hot-Swap Power Supply	
20		2.0m, 16A/100-250V, C19 to C20 Jumper Cord (India)	
21		2U Ultra High Performance Fan Modules for high power PCIe devices	
22		Long Travel Toolless Slide Rail Kit with Cable Management Arm	
23		Standard Rack Latch Mechanism	
24		TPM 2.0 with Secure Boot	
25		Enable IPMI-over-LAN	
26		Intrusion Switch Cable Kit	
27		3 yr base warranty	
28		**Controller / Management**	
29		Server Management Controller Premium License	
30		Controller Premium Feature Enablement (FOD)	
31		**Management Software**	
32		Advanced Server Management Software, Per Endpoint w/5 Yr SW S&S	
33		Registration only	
34		Per Managed Endpoint w/5 Yr SW S&S	
35		**Installation**	
36		Server Installation	
37		Hardware Installation (Business Hours)	
38		**Add-On**	
39		Server Keep Your Drive Add-On	
40		KYD	
41		Duration 60 Months	
42		**Support**	
43		Server Support 24X7 4HR RESP	
44		Premier Support	

SNo.	Parameter	Specifications	Compliance (Yes/No)
45		Duration 60 Months	
46		24x7 4hr Resp	
53.	Data Lake Server		
1		2U 2.5"/EDSFF 3.S Chassis	
2		General Computing - Power Efficiency	
3		Data Center Environment 25 Degree Celsius / 77 Degree Fahrenheit	
4		64C 350W 2.4GHz Processor	
5		2U Performance Heatsink	
6		64GB DDR5 6400MHz (2Rx4) RDIMM	
7		Select Storage devices - no configured RAID required	
8		RAID 16i 4GB Flash PCIe Gen4 12Gb Adapter	
9		2.5" 3.84TB Read Intensive SATA 6Gb HS SSD SED	
10		2.5" 1.92TB Read Intensive SATA 6Gb HS SSD SED	
11		2U 8x2.5" SAS/SATA Backplane	
12		10GBASE-T 2-port OCP Ethernet Adapter	
13		High-speed PCIe Gen5 VPI Adapter (NDR 400Gb class, OSFP, single port)	
14		High-performance PCIe Gen5 GPU Accelerator, ~140GB memory class, passive cooling	
15		NDR 400Gb compatible optical transceiver module	
16		x16 Cable Riser Slot (high power GPU support up to 600W)	
17		x16 Rear Riser Slot	
18		x16 Rear Direct Riser Slots	
19		2700W 230V Titanium Hot-Swap Power Supply	
20		2.0m, 16A/100-250V, C19 to C20 Jumper Cord (India)	
21		2U Ultra High Performance Fan Modules for high power PCIe devices	
22		Long Travel Toolless Slide Rail Kit with Cable Management Arm	
23		Standard Rack Latch Mechanism	
24		TPM 2.0 with Secure Boot	
25		Enable IPMI-over-LAN	
26		Intrusion Switch Cable Kit	
27		3 yr base warranty	

SNo.	Parameter	Specifications	Compliance (Yes/No)
28		Controller / Management	
29		Server Management Controller Premium License	
30		Controller Premium Feature Enablement (FOD)	
31		Management Software	
32		Advanced Server Management Software, Per Endpoint w/5 Yr SW S&S	
33		Registration only	
34		Per Managed Endpoint w/5 Yr SW S&S	
35		Installation	
36		Server Installation	
37		Hardware Installation (Business Hours)	
38		Add-On	
39		Server Keep Your Drive Add-On	
40		KYD	
41		Duration 60 Months	
42		Support	
43		Server Support 24X7 4HR RESP	
44		Premier Support	
45		Duration 60 Months	
46		24x7 4hr Resp	
54.	Digital Twin & GIS Server		
1		2U 2.5"/EDSFF 3.S Chassis	
2		General Computing - Power Efficiency	
3		Data Center Environment 25 Degree Celsius / 77 Degree Fahrenheit	
4		64C 350W 2.4GHz Processor	
5		2U Performance Heatsink	
6		64GB DDR5 6400MHz (2Rx4) RDIMM	
7		Select Storage devices - no configured RAID required	
8		RAID 16i 4GB Flash PCIe Gen4 12Gb Adapter	
9		2.5" 3.84TB Read Intensive SATA 6Gb HS SSD SED	
10		2.5" 1.92TB Read Intensive SATA 6Gb HS SSD SED	
11		2U 8x2.5" SAS/SATA Backplane	
12		10GBASE-T 2-port OCP Ethernet Adapter	

SNo.	Parameter	Specifications	Compliance (Yes/No)
13		High-speed PCIe Gen5 VPI Adapter (NDR 400Gb class, OSFP, single port)	
14		High-performance PCIe Gen5 GPU Accelerator, ~140GB memory class, passive cooling	
15		NDR 400Gb compatible optical transceiver module	
16		x16 Cable Riser Slot (high power GPU support up to 600W)	
17		x16 Rear Riser Slot	
18		x16 Rear Direct Riser Slots	
19		2700W 230V Titanium Hot-Swap Power Supply	
20		2.0m, 16A/100-250V, C19 to C20 Jumper Cord (India)	
21		2U Ultra High Performance Fan Modules for high power PCIe devices	
22		Long Travel Toolless Slide Rail Kit with Cable Management Arm	
23		Standard Rack Latch Mechanism	
24		TPM 2.0 with Secure Boot	
25		Enable IPMI-over-LAN	
26		Intrusion Switch Cable Kit	
27		3 yr base warranty	
28		Controller / Management	
29		Server Management Controller Premium License	
30		Controller Premium Feature Enablement (FOD)	
31		Management Software	
32		Advanced Server Management Software, Per Endpoint w/5 Yr SW S&S	
33		Registration only	
34		Per Managed Endpoint w/5 Yr SW S&S	
35		Installation	
36		Server Installation	
37		Hardware Installation (Business Hours)	
38		Add-On	
39		Server Keep Your Drive Add-On	
40		KYD	
41		Duration 60 Months	
42		Support	

SNo.	Parameter	Specifications	Compliance (Yes/No)
43		Server Support 24X7 4HR RESP	
44		Premier Support	
45		Duration 60 Months	
46		24x7 4hr Resp	
55.	**PA System ECB Server**		
1		2U 2.5"/EDSFF 3.S Chassis	
2		General Computing - Power Efficiency	
3		Data Center Environment 25 Degree Celsius / 77 Degree Fahrenheit	
4		64C 350W 2.4GHz Processor	
5		2U Performance Heatsink	
6		64GB DDR5 6400MHz (2Rx4) RDIMM	
7		Select Storage devices - no configured RAID required	
8		RAID 16i 4GB Flash PCIe Gen4 12Gb Adapter	
9		2.5" 3.84TB Read Intensive SATA 6Gb HS SSD SED	
10		2.5" 1.92TB Read Intensive SATA 6Gb HS SSD SED	
11		2U 8x2.5" SAS/SATA Backplane	
12		10GBASE-T 2-port OCP Ethernet Adapter	
13		High-speed PCIe Gen5 VPI Adapter (NDR 400Gb class, OSFP, single port)	
14		High-performance PCIe Gen5 GPU Accelerator, ~140GB memory class, passive cooling	
15		NDR 400Gb compatible optical transceiver module	
16		x16 Cable Riser Slot (high power GPU support up to 600W)	
17		x16 Rear Riser Slot	
18		x16 Rear Direct Riser Slots	
19		2700W 230V Titanium Hot-Swap Power Supply	
20		2.0m, 16A/100-250V, C19 to C20 Jumper Cord (India)	
21		2U Ultra High Performance Fan Modules for high power PCIe devices	
22		Long Travel Toolless Slide Rail Kit with Cable Management Arm	
23		Standard Rack Latch Mechanism	
24		TPM 2.0 with Secure Boot	
25		Enable IPMI-over-LAN	

SNo.	Parameter	Specifications	Compliance (Yes/No)
26		Intrusion Switch Cable Kit	
27		3 yr base warranty	
28		Controller / Management	
29		Server Management Controller Premium License	
30		Controller Premium Feature Enablement (FOD)	
31		Management Software	
32		Advanced Server Management Software, Per Endpoint w/5 Yr SW S&S	
33		Registration only	
34		Per Managed Endpoint w/5 Yr SW S&S	
35		Installation	
36		Server Installation	
37		Hardware Installation (Business Hours)	
38		Add-On	
39		Server Keep Your Drive Add-On	
40		KYD	
41		Duration 60 Months	
42		Support	
43		Server Support 24X7 4HR RESP	
44		Premier Support	
45		Duration 60 Months	
46		24x7 4hr Resp	
56.	**ITMS Server**		
1		2U Hybrid Storage Array Chassis	
2		Enterprise Hybrid Storage Architecture	
3		Dual Controller Redundant Architecture	
4		High Availability Active-Active Controllers	
5		Intel Enterprise Storage Processors	
6		System Memory with ECC Protection	
7		RAID-DP / RAID-TEC Data Protection	
8		SSD + NL-SAS/SATA Hybrid Storage Support	
9		2.5"/3.5" Drive Support	
10		SSD Tiering Support	
11		Hybrid Flash Optimized Storage	
12		10GbE Network Connectivity	

SNo.	Parameter	Specifications	Compliance (Yes/No)
13		25GbE / 40GbE / 100GbE Expansion Support	
14		FC/iSCSI/NFS/SMB Protocol Support	
15		Snapshot Technology	
57.	Database Server		
1		2U 12x3.5" Chassis	
2		General Computing - Power Efficiency	
3		Data Center Environment 30 Degree Celsius / 86 Degree Fahrenheit	
4		32C 225W 2.3GHz Processor	
5		2U Performance Heatsink	
6		32GB DDR5 6400MHz (2Rx8) RDIMM	
7		Select Storage devices - no configured RAID required	
8		RAID 16i 4GB Flash PCIe Gen4 12Gb Adapter	
9		3.5" 20TB 7.2K SATA 6Gb Hot Swap 512e HDD	
10		2U 12x3.5" SAS/SATA Backplane	
11		M.2 RAID SATA/NVMe Enablement Kit	
12		M.2 480GB Read Intensive NVMe SSD	
13		10GBASE-T 2-port Ethernet Adapter	
14		x16 Rear Direct PCIe Riser Slot	
15		1300W 230V/115V Titanium Hot-Swap Power Supply	
16		2.8m, 10A/100-250V, C13 to C14 Jumper Cord (India)	
17		2U High Performance Fan Module	
18		Toolless Slide Rail Kit	
19		2U EIA Latch Standard	
20		TPM 2.0 with Secure Boot	
21		Enable IPMI-over-LAN	
22		2U Security Bezel	
23		Intrusion Switch Cable Kit	
24		3yr Base Warranty	
25		Controller / Management	
26		Server Management Controller Premium License	
27		Controller Premium Feature Enablement (FOD)	
28		Operating System & Licensing	

SNo.	Parameter	Specifications	Compliance (Yes/No)
29		Windows Server 2025 Addl Lic	
30		Windows Server 2025 Standard Additional License (16 core) (No Media/Key) (POS Only)	
31		Windows Server 2025	
32		Windows Server 2025 Standard (16 core) - MultiLang (not preinstalled)	
33		Registration only	
34		Win Svr Standard 2025 to 2022 Downgrade Kit-Multilanguage	
35		Drop-in-the-Box	
36		Additional Licensing	
37		Windows Server 2025 Standard Additional License (16 core) (No Media/Key) (POS Only)	
38		Win Svr Standard 2025 to 2022 Downgrade Kit-Multilanguage	
39		Windows Server 2025 Standard (16 core) - MultiLang (not preinstalled)	
40		Management Software	
41		Server Management Software, Per Endpoint w/5 Yr SW S&S	
42		Registration only	
43		Per Managed Endpoint w/5 Yr SW S&S	
44		Support	
45		Server Support 24X7 4HR RESP	
46		Premier Support	
47		Duration 60 Months	
48		24x7 4hr Resp	
49		Installation	
50		Server Installation	
51		Hardware Installation (Business Hours)	
52		Add-On	
53		Server Keep Your Drive Add-On	
54		KYD	
55		Duration 60 Months	
58.	**SAN Storage**		
1		2U 2.5"/EDSFF 3.S Chassis	
2		General Computing - Power Efficiency	

SNo.	Parameter	Specifications	Compliance (Yes/No)
3		Data Center Environment 25 Degree Celsius / 77 Degree Fahrenheit	
4		64C 350W 2.4GHz Processor	
5		2U Performance Heatsink	
6		64GB DDR5 6400MHz (2Rx4) RDIMM	
7		Select Storage devices - no configured RAID required	
8		RAID 16i 4GB Flash PCIe Gen4 12Gb Adapter	
9		2.5" 3.84TB Read Intensive SATA 6Gb HS SSD SED	
10		2.5" 1.92TB Read Intensive SATA 6Gb HS SSD SED	
11		2U 8x2.5" SAS/SATA Backplane	
12		10GBASE-T 2-port OCP Ethernet Adapter	
13		High-speed PCIe Gen5 VPI Adapter (NDR 400Gb class, OSFP, single port)	
14		High-performance PCIe Gen5 GPU Accelerator, ~140GB memory class, passive cooling	
15		NDR 400Gb compatible optical transceiver module	
16		x16 Cable Riser Slot (high power GPU support up to 600W)	
17		x16 Rear Riser Slot	
18		x16 Rear Direct Riser Slots	
19		2700W 230V Titanium Hot-Swap Power Supply	
20		2.0m, 16A/100-250V, C19 to C20 Jumper Cord (India)	
21		2U Ultra High Performance Fan Modules for high power PCIe devices	
22		Long Travel Toolless Slide Rail Kit with Cable Management Arm	
23		Standard Rack Latch Mechanism	
24		TPM 2.0 with Secure Boot	
25		Enable IPMI-over-LAN	
26		Intrusion Switch Cable Kit	
27		3 yr base warranty	
28		Controller / Management	
29		Server Management Controller Premium License	
59.	NAS Storage		
1		2U Hybrid Storage Array Chassis	
2		Enterprise Hybrid Storage Architecture	

SNo.	Parameter	Specifications	Compliance (Yes/No)
3		Dual Controller Redundant Architecture	
4		High Availability Active-Active Controllers	
5		Intel Enterprise Storage Processors	
6		System Memory with ECC Protection	
7		RAID-DP / RAID-TEC Data Protection	
8		SSD + NL-SAS/SATA Hybrid Storage Support	
9		2.5"/3.5" Drive Support	
10		SSD Tiering Support	
11		Hybrid Flash Optimized Storage	
12		10GbE Network Connectivity	
13		25GbE / 40GbE / 100GbE Expansion Support	
14		FC/iSCSI/NFS/SMB Protocol Support	
15		Snapshot Technology	
16		Thin Provisioning	
17		Deduplication and Compression	
18		Encryption at Rest	
19		Hot-Swap Redundant Power Supply	
20		Rack Mount Rail Kit	
21		Redundant Cooling Fans	
22		Cable Management Support	
23		Enterprise Rack Deployment	
24		TPM / Secure Management Features	
25		Remote Management Support	
26		Intrusion / Security Protection	
27		3 Year Base Warranty	
28		Storage Controller Management	
29		Advanced Storage Management License	
30		Premium Feature Enablement	
31		Centralized Storage Management Software	
32		Advanced Monitoring & Reporting	
33		Registration and Licensing	
34		Subscription & Software Support	
35		Installation Services	
36		Storage Installation	
37		Hardware Installation (Business Hours)	

SNo.	Parameter	Specifications	Compliance (Yes/No)
38		Add-On Services	
39		Keep Your Drive Service	
40		KYD Support	
41		Duration 60 Months	
42		Support Services	
43		24x7 4HR Response Support	
44		Premier Support	
45		Support Duration 60 Months	
46		24x7 4 Hour Response	
60.	**Tape Library**		

SNo.	Parameter	Specifications	Compliance (Yes/No)
61.	Backup Solution		
1		The proposed backup solution should be available in a single management console on various OS platforms such as Windows, Linux and MAC	
2		The proposed backup solution shall have same GUI across heterogeneous platforms to ensure easy administration.	
3		The proposed backup solution has in-built frequency and calendar based scheduling system.	
4		The proposed backup solution should be certified “hot-online” backup solution for different type of Enterprise databases and applications. It should have a supported integration minimum with latest versions of MSSQL Database, Oracle Database. Application aware backup license should not be separate from base agent license.	
5		The proposed backup solution shall also support granular recovery for Vmware, Exchange server, Share point. For Virtual environment Hyper-V / VM license should be unlimited including application aware backup.	
6		The proposed backup solution shall also support SAN backup	

SNo.	Parameter	Specifications	Compliance (Yes/No)
7		The proposed backup solution shall also support NAS backup	
8		The proposed backup software should give the option to allow de duplication to be done either on the Application Server or on the Backup Server or at the Target Device.	
9		The backup software should support backup to cloud. Vendor Cloud or any 3rd party cloud like AWS, Azure, Google etc..	
10		The proposed backup solution shall support synthetic full backup / Virtual full backups.	
11		The proposed backup solution shall be able to copy data across firewall.	
12		The proposed backup solution shall support for write protect or restore protect on file level or folder level. etc	
13		The proposed backup solution shall support File and Folder level backup & restore feature	
14		The proposed backup solution shall support file name or folder name or host name wise sort	
15		The proposed backup solution must support at least AES 256-bit encryption capabilities. Encryption should be at both level like intransit and Storage	
16		The proposed backup solution should have blockchain technology for files authentication. If files gets changed by anyone that should be trackable.	
17		The backup software should support missed job execution	
18		The Backup software should be able to recover only critical volumes and later restore other volumes that were backed up in separate sessions.	
19		The backup software should support the Cold replication functionality	
20		The proposed backup solution must support monitoring & reporting methods while backing up and restoring	
21		The proposed solution must work in backup from Physical image to Virtual image or vice versa	
22		The proposed solution must work with both AD and workgroup systems for client backups	

SNo.	Parameter	Specifications	Compliance (Yes/No)
23		Compressed mechanism for security like 128bit or mentioned if any other	
24		The proposed solution must work with Backup policies pertaining to retention period definition as per organization policies	
25		The proposed solution should have inbuilt Anti Ransomware protection for live system as well as backed up data and map drive for endpoints. Also, it should be capable to revert back any ransomware infected file to original stage	
26		The proposed solution should have inbuilt Crypto mining protection for live system.	
27		Proposed solution should have Secure backup data replication with variable-length encryption at the source, along with compression and encryption to ensure that backups are optimized for WAN transmission. This should be ensured without need of any other 3rd party WAN Accelerator requirements.	
28		The proposed solution should not replicate entire storage or backed up data. It should have provision to select specific date for off host backup processing.	

Group-9: Video Management, Analytics & AI Applications

SNo.	Parameter	Specifications	Compliance (Yes/No)
62.	**Video Management System (VMS)**		
1	**Minimum Technical Specifications**	Web client with single point of management for entire system. The VMS software should be supplied with perpetual licenses with lifetime free. Once sold it will be lifetime property of Customer Command Hospital. There should not be any surprise fees, no forced upgrades, no software renewal charges.	
2		The open Platform Video Management Software (VMS) Application, should be a reputed brand in global market, should be from the same camera OEM & should support various third Party ONVIF IP Cameras, this is compulsorily required so that the same VMS Applications can be scaled up in future	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		by just adding third Party IP Cameras & additional Software Licenses.	
3		The VMS system shall be a scalable client – server architecture built using well known operating systems like Windows Server 2019/2022 Standard Edition. Microsoft Windows 2016, 2019 and 2022 64-bit Server.	
4		The Intellectual Property Rights & Source Code of Offered Video Management Software must not reside in a country that is sharing Land Border with India. It should be in the same camera OEM name and OEM should be available with its own service support centre in India.	
5		The offered VMS platform should be as per Make In India Policy with local content of 50% more to compulsory qualify as Class-1 local supplier. The VMS software with 100% LC (designed, developed and manufactured and maintained with global support service centre availability in India) will be given preference.	
6		The IP CCTV System & Components OEM must confirm that Firmware shall be secured through Signed Digital certificates on all active devices including their updates. Firmware must be retained by OEM (Original Equipment Manufacturer) and, it's IPR. The IPR must reside either In India or shouldn't reside or belong to any of Its entity in restricted country as designated by GOI(I.e. China, Pakistan, Bangladesh, Bhutan etc). Must comply with 3rd party run PKI or certificates or encryption policy or SSL Certifications. The required necessary supporting documents are always required to keep with end user against of the above. The CCTV camera OEM must own Its own PGP PKI & Firmware Version & Details must be taken.	
7		Critical/Core components OEM should not have any requirements to have proprietary platforms and should conform to open standards. OEM must be free from Hi-Silicon Chipset; SOC/processor; coded firmware and PCBs should not be from restricted countries; countries sharing land border with India and including those companies or their subsidiaries	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		or group companies or parent company from restricted list of countries /companies. Necessary supporting documents with an undertaking must be submitted along with bid. Customer (…..) has all the rights to evaluate thoroughly, if found any violations in this regards the strict disciplinary actions will be taken against both system integrator and OEM of camera & VMS.	
8		The active Component's OEMs I.e. of IP CCTV and Embedded NVR's/Servers should confirm of not using or procuring any such equipment's or processors or software patches or firmware or in SKD/CKD/ CSU/parts/spares from those or any blacklisted companies (or any subsidiary or affiliate or its 3rd party agencies or such backlisted or barred entities) or by any recognized global forum or Institutions in-view or reporting of suspicious activities of hacking/cyber-attacks/malwares/etc. to safeguard the public safety & security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including the scope of video surveillance system & components. A declaration cum undertaking must be submitted by OEM signed by competent authority (Director Level at OEM company) in this regard. Any false declaration can lead to Bid technical rejection.	
9		Command hospital has all the rights to ask any bidder(s) to demonstrate the complete system at Customer Command hospital, Kondhwa premises as per tender requirement with NO cost No commitment basis. The bidders' technical qualifications fully depends on demonstration qualifications.	
10		A Desktop Client solution shall be available for those users who prefer not to work in a browser environment.	
11		Configuration Sections of Application: Add, discover, configure and operate recording servers, application servers, web servers, as well as IP cameras and encoders (edge devices).	

SNo.	Parameter	Specifications	Compliance (Yes/No)
12		Full live digital video and audio surveillance over a standard 1 Gbps network.	
13		The VMS shall support recording, playback and archiving of video in standard industry compression formats, including H.265, H.264, JPEG and M-JPEG.	
14		True Open Standards (ONVIF) as Basis: Thin client architecture. Centrally licensed. COTS compatible software or available preloaded on a manufacturer certified application/web server or recording server.	
15		Two License Tiers: Associated with number of edge devices and a specific feature set. Licensing shall be based on a per edge device basis	
16	Software Features	Easy to Use Tabs: Access configuration screen and dashboard monitoring systems health. Monitoring Screen: Video display area with available resources list. Multiple Display Views: Configurable with variety layouts. Multiple Monitors: Supported.	
17	Live Video		
		1) Stream through Recording Server with auto fail over to cameras.	
		2) PTZ available from live video.	
		3) Presets and tours are configurable.	
		4) Digital zoom provided on video displays.	
18	Web Based Interface		
		1) Access the VMS from any standard web browser enabled device.	
		2) Browser compatibility: Microsoft Edge. Chrome shall be able to be used with the VMS Chrome extension from the Chrome store.	
		3) Provide live viewing, playback and PTZ controls.	
		4) Mobile App: Apple and Android smart phones and tablets. View live or recorded video. View concurrent multiple video streams; 4 on phones, 9 on tablets. Full control of PTZ, including presets. Quick and simple playback. Pinch to zoom on live and recorded video.	
19		Export Icon: Easy access on display to save a video clip. Archived in MP4 format and authenticated in the player per the ONVIF spec.	
		System should Support to export video of multiple cameras on multiple timelines	

SNo.	Parameter	Specifications	Compliance (Yes/No)
20		Playback: Supported from main screen without leaving live video viewing area. Clicking Playback from time icon will allow selecting the playback to start from a specific date and time using standard calendar tools.	
21		Software Delivery: Provided on manufacturer's website.	
22	Events:	Setup in configuration area. Pre-Event Recording: Supported and with event notification.	
23		Access Control System Support: Accessed using a simple tab click. Interface opens in popup window that can be used in conjunction with the VMS.	
24		Enhanced Edge-based Analytics: Show bounding boxes around detected objects in live and playback video.	
25		Authorization roles shall be configurable; these roles shall then be listed in the Resources list on the monitoring display screen. This Resources list can be viewed in a hierarchy view with these groups or as a flat list.	
26		Video Masking: Available centrally through the VMS. Allow users with the correct authority to unmask video as needed using icon on the display screen. Unmask feature available on live and playback video.	
27		Quick Configuration Wizard: Streamlined process for typical and basic system setup with minimal input required.	
28		Search Functions: Six search functions available including museum search (supports AI classification for those cameras with that functionality), thumbnail search, events framework search, event/alarm search, audit log and Analytics Search. Additionally, the player shall support coloured bounding boxes with for the AI analytics, person (green box), vehicle (cyan/blue box) and animal (yellow box).	
29		Capability for 360-degree lens de-warp available for use with cameras with fisheye lenses.	
30		Integration with Active Directory (AD): Allow user management via the AD.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
31		Override mode: Allows operating in case AD communication is lost.	
32		Import user list: A user list can be prepared in advance in standard Excel sheet saved in .csv format and imported into VMS.	
33		Auto Archive: Archiving can be set up to occur on a schedule, for either all data or only events-based recording, to local or network/cloud storage.	
34		Multi-language Support: All text in the user interface translated to selected language.	
35		Backup and restore for system settings shall be available. Backup can be to a network drive or cloud storage.	
36		Keypads and PLC controls supported. Numeric IDs for devices configurable for use with controls. These devices shall be able to control remote monitors.	
37		Central Software Upgrade Interface: Provides the ability to upgrade the entire system by pushing the upgrade from the Application Server to all devices on the system.	
38		System supports IPv4/IPv6 and HTTPS. There shall be HTTPS support for External Events.	
39		The system shall have built in Log Collection from all system PCs, making it easier to troubleshoot problems. An advanced tool shall be provided.	
40		The system shall accept external text strings from third party systems.	
41		Alarm notification shall be both visual and audible. The display of the alarm tab view can be auto dismissed after a set time and return to the previous view; the alarm tab view can still be accessed as needed. Live view from up to four cameras shall be able to display in the alarm tab. Multiple alarms (external events only) shall be able to be imported in a single action using an Excel sheet template. A Test Email button shall be provided within the interface.	
42		A Report button shall generate an Excel or HTML report of the devices sorted by their hosting recording servers or a flat list.	
43		Devices shall be able to be replaced or moved, for load balancing purposes.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
44		Storage of video and exports can be mapped to another server, a NAS on the network or to the cloud (AWS/Wasabi).	
45		A Server Failover unit shall be able to be configured to take over in the event of an server failure.	
46		A Mapping function shall be provided that allows the placement of resource devices on any imported map. The map shall be either a static or live map. The device icons on the map shall be adjustable in size.	
47		An Events Database shall exist to store any event that occurs in the system. From the Event Search screen, a query shall be able to be created to search for any event that occurs on the system from any resource in the system.	
48		A video clip, either in live or playback, shall be able to be bookmarked for easy referral.	
49		The ability to use mobile devices as mobile cameras shall be available. The mobile device shall be able to receive event alerts.	
50		The VMS shall be able to accept partner systems through an integration framework. These partner resources will show on the Resources list and can display in a tile.	
51		A Snapshot function shall be provided to capture video from live or playback; this snapshot shall be able to be saved. It shall be possible to capture snapshots from all resources and update them all at the same time.	
52		An Audit Log shall be available to track every user's actions.	
53		Keypads/PLC shall have the ability to call up other remote monitors.	
54		Shall be operational in a virtual environment.	
55		An integration framework shall be provided to allow partnerships with third party systems such as LPR and Access Control.	
56		An Alarms Management module shall be provided that shall allow events to be defined as alarms and provide tools to review open alarms and close them. Alarms shall have a defined life cycle and	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		procedures shall be able to be created to handle these alarms, if needed.	
57		A Client Performance Indicator shall be provided to indicate system performance as more cameras are added and displayed.	
58		Monitors can be managed from the Application Server in a central way and a monitor can be defined as an alarm monitor for use by the alarms/rules in the system. Monitor IDs can be synced.	
59		Virtual Matrix Display Controller (VMDC) feature shall be available for user to take control of any client workstation on the same network. User shall be able to view and display video on those remote monitors.	
60		The system shall have an enhanced dashboard that shall present the system's health status and provide health monitoring information and statistics on all connected devices, including Application Server, recording servers and cameras. It shall provide notifications that notifications that provide cyber security and an easy-to-use activity mapping chart.	
61		Multi-User Authorization Login Application. Offers levels of authorization based on functions.	
62	Setup Utility	Allows Administrator to configure additional users as well as user groups.	
		1) User authorization: Configurable for specific system operations. Authorization Permission Setup: Performed using the User screen.	
		2) Authorization Roles: Available to configure from the Authorization Roles screen. Permissions: Provide authority to perform all system functions.	
		3) Users and groups on AD servers may be imported and become a group in the VMS.	
		4) The software shall offer a full multi-user authorization process as follows: Authorization Roles: Created once globally. Authorized and given specific permissions. Users: Created once globally and may be given rights to groups. No virtual limit on number of groups and users authorized in the software. Authorization Roles to be authorized or denied access to: Monitoring screen for video	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		display. Configuration. Dashboard. Video and audio (media) export. Override masking. Override View.	
63		A user, given appropriate access, may remotely configure components connected to the network. An access list shall be able to be created to add those PCs that are allowed to connect to VMS, adding another layer of security.	
65		Software permits viewing of live video from any edge device connected to any recording server on the network.	
66		Export Icon: Simplifies process of exporting video and creating archives and saving video to media, such as: USBs, CD, DVDs or solid-state drives. An embedded player shall be optional with each exported/archived video clip for playback on any machine if configured to do so.	
67		Event Rules: Create rules triggered by an event occurrence. Define actions executed for a given event. Events are selectable. Rules are configurable after an event is selected.	
68		Event Association: Multiple devices may be associated with an event. Actions Triggered by Event: Configurable as On and Off. Display live video. Display a view. Go to a preset. Operate a relay. Run a PTZ tour. Run a view tour. Start a URL. Delay function.	
69		Scheduled Recordings: Applies to cameras, encoders and microphones. Scheduling is based on rules configurable for actions the system takes upon an event. Schedules accessible on recording tab in device configuration. Create and Schedule Recordings: By authorized users. How often schedules repeat; weekly, monthly, yearly or never. Determines how the systems prioritizes schedules if schedule times overlap. Schedules available when configuring recording and rules, saving the need to create multiple and duplicate schedules. Sequencing cameras, including multi-screen displays. Record cameras at different qualities and frame rates from any recorder on the network. Schedule shall allow running preconfigured combinations of camera, sensor and PTZ programmed routines.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
70		System Components: Application/Web Server: Act as main system server; Windows based. Global configuration of the system is stored on this server. Recording Servers: Windows based providing communication, live streaming, recording, video playback and audio from cameras and encoders.	
71		Device Configuration: Valid devices to be configurable for system recognition and operation. Cameras fixed or with integrated PTZ. Microphones. Encoders. Sensors. Relays.	
72		Authentication: Video from cameras is enabled to verify the authentication of the video and present an authentication symbol on the displayed video for recorded playback through the player when enabled only on export.	
73		User Friendly Tabs: Allow monitoring of live and playback video, and configuration of the system.	
74		Login Window: Consists of Username and Password fields. Default Username and Password: Available for initial login. Configurable for increased security; there shall be an option to enforce a complex password.	
75		Serve operators, supervisors and system administrators.	
76	Setup Utility	Monitoring Display Screen:	
		1) Selection of number of tiles to display.	
		2) Resource list of devices in system. Viewable as flat list or hierarchical list based on user configured groups. Resources include names of devices and icons depicting devices. Video Channels (cameras) connected, differentiating between PTZ and fixed cameras. Audio Channels (microphones). Views. Tours. Web Pages. Relay Outputs.	
		3) Display Area: Offers display configurations up to 36 tiles. Full screen View: Available. More views added by clicking the plus sign to create new view tabs while not losing the default view. Controls: Change the layout. Stop all displays. Export. Synchronize playback. Control current selected tab.	
		4) Camera Controls: Display at top of a tile when mouse hovers and may be locked in place. Playback.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		PTZ control. Digital zoom. Unmask. Export. Configuration settings	
		5) Playback controls: Visible when cameras go to playback. Looping a video section. Slow mode. Play from time. Rewind, fast rewind, pause, forward, and fast forward. Back to live video and current time.	
		6) Access to all available programming menus.	
		7) Viewing live devices is performed by dragging a device to any tile. Audio devices display in a smaller area below the video tiles.	
77		Dashboard, Search, Alarms and Configuration Menu Access: Clicking a tab at the top of the screen.	
78		Access Control Systems: Available for integration.	
		1) Meet requirements of business and government access control systems.	
		2) Monitor and control facility access as well as video detection, temperature and communications loss monitoring.	
		3) Provide control and access to users on Local Area Networks (LAN), Wide Area Networks (WAN), wireless networks and the Internet.	
		4) Video viewing playback and PTZ control from the VMS.	
79		A method to add partner systems shall be provided through an integration framework. It shall support access control software Access Control, LPR, software LPR and Thermal Radar sensor.	
		1) When integrating with the access control software Access Control System, digital inputs, relay outputs and action plans created in access control software shall be automatically added in VMS to be configured as any other Resource. Doors shall be able to be edited and user information on the cardholder picture shall be updated once updated in access control software.	
		2) Rules can be configured based on these partner resources and then alarm events shall be able to be created and then searched for.	
		3) The partner icons can also be added to maps.	
		Access Control Systems: Available for integration.	
80		VMS should support ONVIF Profiles S, G & T	

SNo.	Parameter	Specifications	Compliance (Yes/No)
81		VMS system should support high availability and failover with automatic synchronization to ensure maximum uptime.	
82		VMS should support centralized search with multiple categories and filters for bookmarks, recordings, motion alarms, events, vehicles, people, and data from third-party systems.	
83		VMS should provide an SDK or API for seamless integration with third-party systems and should include libraries and documentation for easy integration.	
84		VMS should provide a health monitoring system with real-time alerts and a system dashboard to monitor the health of cameras and servers.	
85		VMS should support installation on virtual servers for flexibility and scalability in large deployments.	
86		VMS system shall be a scalable client-server architecture and capable of supporting installation on both physical and virtual servers.	
87		VMS system should include automatic camera discovery capabilities.	
88		VMS should support multilayered map functionality that allows interactive control of the entire surveillance system, showing system integrity, and integrating seamlessly with a video wall module.	
89		VMS should include comprehensive audit logs showing full system awareness and user activity.	
90		VMS should support integration of external Video Content Analysis (VCA) systems and other third-party video analytics tools.	
91		The VMS platform should be STQC tested as per guidelines by MeitY. The valid certificate from respective VMS OEM must be submitted at the time of bid of this tender.	
92		Considering past experience and multiple issues faced in past and ongoing at Customer Command Hospital, all IP CCTV cameras & VMS proposed by bidder should be from same OEM/Make for seamless integration, better performance & features interoperability & after service sales management.	
93		Bidder will have to confirm in writing that Bidder/OEM of major equipment's like: server,	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		Video wall, Network Switches, VMS, Cameras have functional after sales service centres in India region from last 5 years (pl. submit proof of major documents of company, GST certificate, Shop registration certificate etc.) and are accessible during warranty period and after warranty period as and when required to ensure healthy condition of system for 24 hrs. X 7 basis.	
63.	**Video Summarization**		
1	Indigenous Product & IPR Ownership	The offered Video Summarization module shall be an indigenous module developed, owned, and maintained by the OEM. All source code, model pipelines, intellectual property, design documentation, and build processes shall remain under the OEM's exclusive ownership and control.	
2	Compliance with Indian Cybersecurity Standards	The offered Video Summarization module shall comply with STQC IoTSCS requirements, BIS ER-01:2024 standards (where applicable to software stack components), and relevant CERT-In cybersecurity advisories.	
3	Data Protection & Residency (DPDP Act 2023)	The Video Summarization module shall comply with the Digital Personal Data Protection (DPDP) Act 2023. All video data, derived metadata, attribute indexes, and audit logs generated by the module shall be stored and processed within India.	
4	Quality & Information Security Certifications	The OEM offering the Video Summarization module shall hold valid ISO 9001 (Quality Management) and ISO 27001 (Information Security Management) certifications issued in the OEM's legal name.	
5	Large-Scale Analytics Deployment Experience	The OEM shall have at least one (1) deployment involving video analytics or investigation workflows operating under a centralized command platform and shall produce a valid purchase order.	
6	Federated / Multi-Site Deployment Maturity	The OEM shall demonstrate prior experience deploying analytics modules across multi-site architectures with centralized monitoring and distributed recording environments.	
7	Integrated VMS Stack Operation	The Video Summarization module shall operate as an integrated add-on within the offered VMS stack without requiring a separate user interface or standalone system for core functionality.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
8	Recorded Video Analysis Capability	The module shall analyze recorded video streams and generate summarized outputs to significantly reduce manual viewing time during post-event investigation.	
9	Online & Offline Video Support	The module shall support analysis of both live video feeds and offline pre-recorded video files in standard formats.	
10	Object Extraction Engine	The module shall automatically extract moving objects including People, Vehicles, and Animals from video streams for indexing and summarization.	
11	Object Classification Categories	The Video Summarization module shall classify extracted objects into predefined categories including Person, Two-Wheeler, Car, Bus, Truck, and Animal.	
12	People Classification	The module shall support People categorization including Man and Woman for refined investigation workflows.	
13	Vehicle Classification	The module shall support classification of Two-Wheeled Vehicles (e.g., Bicycle, Motorcycle) and Other Vehicles (e.g., Car, Truck, Bus).	
14	Animal Classification	The module shall support classification of Animals including Dog, Cat, and equivalent detected classes.	
15	Attribute-Based Filtering	The module shall allow filtering of summarized results based on object attributes including clothing color, upper/lower garment type, bag presence, vehicle color, and vehicle type.	
16	Time-Range Filtering	The module shall allow limiting search and summarization to user-defined date and time ranges across authorized cameras.	
17	Camera-Based Filtering	The module shall support restricting analysis to selected cameras or defined camera groups within the system.	
18	Area-Based Inclusion / Exclusion	The module shall allow inclusion or exclusion of user-defined zones for object-based summarization and investigation.	
19	Dwell-Time Filtering	The module shall allow identification and selection of objects dwelling beyond configurable time thresholds within defined areas.	
20	Speed-Based Filtering	Where camera calibration is available, the module shall support filtering of objects based on estimated speed parameters.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
21	Appearance Similarity Search	The Video Summarization module shall enable identification of similar-looking objects across video archives using appearance-based similarity search.	
22	Cross-Camera Object Correlation	The module shall support correlation of object appearances across multiple cameras to reconstruct movement timelines within a defined time range.	
23	Object Superimposition Rendering	The module shall support reconstruction and superimposition of extracted objects over the original scene to enable simultaneous visualization of events occurring at different timestamps.	
24	Timeline Compression Capability	The module shall generate condensed summarized video outputs from long-duration recordings to significantly reduce investigation time.	
25	Geo-Spatial Object Visualization	The module shall display object movement across cameras on the configured map / e-map interface with associated timestamps.	
26	KPI & Trend Visualization	The module shall generate analytical indicators including traffic patterns, visitor/pedestrian counts, object frequency, and general activity trends derived from extracted objects.	
27	ANPR Data Correlation	Where ANPR integration is enabled, the module shall correlate vehicle metadata with summarization workflows for unified investigation.	
28	Summary Export Capability	The module shall support export of summarized video outputs and associated metadata in standard formats without altering original evidentiary recordings.	
29	Detailed Investigation Reporting	The module shall generate detailed reports for searched objects including number of appearances, time range, and camera locations, with linkage to playback within the VMS.	
30	Performance Benchmark	The module shall be capable of generating summarized output for up to two (2) hours of Full HD recorded video within ten (10) minutes under recommended hardware configuration.	
64.	**AI Based Video Analytics**		
1	Video Analytics	Intelligent Video is an advanced solution that performs intelligent video analysis and fully automates video monitoring. It automatically tracks and identifies objects, analyzes motion and extracts video intelligence from IP camera or video streams.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		The output of this system is analysis and video data mining in real-time events or store in a database.	
	Intrusion Analytics (TripWire Detection)	provides automated perimeter monitoring and secure area protection. It should be able to capture intrusion on any time within marked boundary.	
	Crowd Density & Heatmap Analytics	Crowd Detection analytics is completely AI Engine Deep learning-based analytics (CNN-based models) Identify the Real-time crowd density detection (Low/Medium/High/Critical)	
		Application has Configurable thresholds and alerts.	
		Application triggered event based on different density levels like Low / Medium / High / Critical means overcrowded.	
		System shall detect and classify crowd density in configurable zones	
		Application triggered Real-time alerts when thresholds exceed limits.	
		Capability to work in: Indoor and outdoor environments Day/Night conditions	
	Anomaly Detection (Reverse Flow/Panic)	Application should detect anomaly like reverce flow of crowd/panic moment.	
		Generate color-coded heatmaps showing like High traffic zones.	
		Application should triggered alert and event on overcrowding.	
		Application should triggered alert and event on Sudden crowd surge.	
		Application should triggered alert and event on Restricted area crowd formation	
		Application should generate reports like: Footfall count Peak crowd hours Zone utilization	
	AI Video Security (Unattended Object)	Application should detect unattended object in the field of view of the camera.	
		Application should Monitoring predefined zones for any type of objects left.	
		Application should triggered alert and event on object left.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
	AI Video Security (Weapon)	AI-based Weapon Detection Video Analytics System capable of detecting visible weapons in real-time using IP cameras.	
		System shall detect weapons including: pistols, rifles, Knives and trigered real time alert and event.	
	AI Video Security (Fire & Smoke)	The Smoke and Fire Detection feature detects flames and smoke in the camera's field of vision within a virtually monitored area of interest. This analytics detects flames, reflected fire light, smoke clouds, and ambient smoke and alerts users in real-time or at regular intervals.	
		Application should triggered alert and event on Fire & Smoke.	
	AI Video Security (Loitering)	Loitering Detection should detect individuals or groups loitering in predefined zones.	
		Application should detect Human loitering.	
		Application should generate real-time alerts and maintaining event logs for loitering events.	
		also mail alert or alarm should be directly integrated in VA in real time basis.	
		Vendor will provide MIS application in which daily and monthly report will be generated for intrusion detection and object classification in standard format like PDF,CSV and Excel	
2		Video Analytics should process multiple IP cameras parallel.	
3		The Video Analytics (VA) shall be designed to provide Intelligent Video Analysis for 24/7 surveillance with support for 3rd party devices like IP cameras.	
4		The VA configurator shall have easy to use graphical user interface with live alarms list for easy parameter fine tuning and feedback.	
5		The system shall be designed to work for 24x7 unattended operations	
6		This is server-based analytics which processes RTSP streaming of IP camera.	
7		Video Analytics software processes images, video files, IP Cameras.	
8		Analytics software should process multiple IP cameras on single system.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
9		Multiple analytics should set on multiple cameras at time.	
10		The VA shall support cameras using any of the video compression formats H.264/MPEG4/MJPEG.	
11		The system should allow the use of a pool of video analytic algorithm on any cameras without limitations. It should be very easy to change an algorithm from a camera to another.	
12		The system should allow multiple analytics configure to single or multiple cameras.	
13		The System should work on offline mode like Video Clips.	
14		Video Analytics should work in both Day & Night mode.	
15		Video Analytics support IR cameras.	
16		Video Analytics should use databse like MySQL.	
17		Video Analytics should store event unique id, event name, evidence image, evidence video, date & time inside database.	
18		Video Analytics should communicate with any third party hardware using Relay devices.	
19		Highly efficient video analytics can run on a variety of cameras and platforms	
20		Video summary (Incident Video) can reduce a long-archived video to a manageable video with just actual events	
21		VA can have support of network LED light relays.	
22	AI Enabled	Based on Artificial Intelligence: AI-based Video Analytics shall be enabled with a collection of indigenously developed AI techniques, based on advanced image and video processing, computer vision and pattern recognition. Leveraging our numerous proprietary models, AI and underlying deep neural networks (DNNs), enables the platform to efficiently compute automatic object/ pattern detection, multi-level classification, etc. These models have been generated with a wide range of real-life visual datasets, to provide unparalleled accuracy, using optimal computing bandwidth suitable for various application domains. Classification like Human, Pet, Vehicle available.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
23	Camera Agnostic	Agnostic to any make and model of camera. It is built on robust technology and can work with any video data, whether real-time or archived, and generated from any source like VMS, NVR.	
24	Unprecedented Scalability	Highly scalable software architecture. Highly optimised AI codebase that supports multi-threaded processing of the algorithms, and multiple analytics functions to run in parallel, in each camera in the surveillance system. The footprint is very small with reduced computational and memory requirement, because of its indigenous design and innovative Architecture.	
25	Integrated with Intelligent VMS	Video Analytics should integrate with any make & model of Video Management Software (IVMS). This homogenous, unified video computing architecture helps integrate with any make and model of VMS.	
26	Software Interface	Easy-to-use, intuitive and feature-rich desktop, handheld and web user interface.	
27	Field-proven Technology	The AI-based analytics framework and the applications are field-tested under a wide range of environmental and lighting conditions. Proven to work more reliably in high population density conditions, compared to other competing solutions. Field-proven with real-life deployments across various domains, cities, enterprises and other critical Installations.	
28	API's	Pre-integrated with VA, yet a rich API is also available to integrate the VA platform with an existing surveillance installation, or a third-party VMS, as per the choice of the user.	
29	Automatic eAlerts & Event Messages		
		XLS Output Report: User can export all events inside XLS.	
		Email: Email functionality available to report any incident happen for mention analytics.	
		HTML Reports: HTML reports available on UI.	
		Database / ODBC: MySQL Database support availalble.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		REST JSON API: Using API we can communicate with any third part hardware/software.	
		Date & Time based search options are available.	
		Search by Camera Name / Location option is available.	
		Search by Event Name option is available.	
		Search by classification like Human, Pet, Vehicle	
30	Physical Alerts	Sound & Audio: Buzzer alerts available with system. VA can having support of network LED lights for buzzer and lights	
31	Visual Flashing Alerts	Flashing event alert on screen: Flashing event alerts available on UI.	
32	Event Details	The system Graphical User Interface should be bi-lingual: it shall support both English & Graphical User interface (GUI) should provide following information: - a. Image of the generated action event b. Video of the generated event c. Event Descrtpition d. Date, Time of the event.	
33	Storage	The System shall store JPEG/MJPEG images of each action perform in video & also store event video.	
		The system shall store the event data into a MySQL.	
34	Integration : Hardware, VMS, Relay Devices, Third Party NVR, DVR		
		Available with API/SDK for partners and external systems.	
		Integrated with analog, IP/network and digital cameras (it can also take video input from many DVR and NVR/video management solutions)	
		Enables security professionals to rapidly search for past incidents from archived video	
		Increase productivity and efficiency of the security professionals	
		Video Analytics should communicate or intgrate with any Video Management System (VMS).	
		Video Analytics should communicatr with VMS and select specifide cameras for processing.	
		Video Analytics should detect incident and same incident share with VMS system.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		Video analytics should communicate or intgrate with relay devices.	
35	System requirement		
		Operating System: Linux: Ubantu 20.04 LTS 64-bit Operating System	
		Database: MySQL	
65.	**Facial Recognition System**		
1		Face Detection and Recognition, Video Capture Module, Face Recognize must be a Deep Learning and AI-based face detection, search and recognition solution with an accuracy as high as +99%.	
2		Facial Recognition for missing person: Application should identify missing person on live IP camera using predefine face database. Using AI and deep learning, face recognition shall achieve accuracy as high as +99%	
3		Recognition is available in both real-time and off-line modes and enrolment is available from both video and still images. Facial recognition is achieved by analysing multiple images per face with millisecond response times depending on system resources.	
4		Face Recognizer is available with a REST API/SDK for OEM partners and application builders. Easy integration of alerts is achieved through http/JSON and an open architecture.	
5		The System should automatically detect a Face in the camera view.	
6		The system shall be designed to work for 24x7 unattended operations	
7		The System shall automatically detect the face in the captured video feed in real-time.	
8		The System shall store JPEG image of face detected image and train image into DBMS like MySql etc. database along with date	
9		The system should be able to handle multiple faces simultaneously i.e. if there are more than one face in the camera view the system should be able to detect and recognize all faces.	
10		FRS recognize face with a minimum of 300 lux of light intensity on face.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
11		FRS recognition speed should be less than 1-2 seconds	
12		FRS should have capability for recognition of Frontal face along with Non frontal face and in case of non-frontal recognition, solution be capable of detect, recognize and log faces. Face resolution 70 pixels min, 100-300 recommended. Min 30 pixels between eyes, 50-150 recommended.	
13		FRS Architecture should support Enrolment and Recognition of faces in Desktop and Central server respectively and simultaneously.	
14		System should be able to detect and recognize the face from all ethnicities.	
15		Face Recognition System (FRS) shall work on real time with IP cameras.	
16		The system shall detect and recognize faces from images.	
17		The system shall detect and recognize faces from Video Clips.	
18		The system shall detect and recognize faces from IP Cameras, Input: RTSP/HTTP stream from network/IP cameras	
19		The system shall have the best suited technology employed for 1:1 (one to one) and 1: N (one to many) matching application, when they enter the field of view of CCTV Cameras.	
20		The system shall work on partial occlusion of face, glasses, scarfs, changes of facial expression etc.	
21		The system shall be able work on moderate face rotation either horizontal or vertical, Angle variations from frontal face – yaw +/- 25 degrees, pitch +/- 25 degrees, roll +/- 20 degrees	
22		The system shall be able to add photographs obtained from law enforcement agencies to the criminals' repositories along with option details for sex, age, scars, tattoos etc for future searches	
23		Live video should display detected face with bounding box and recognized face with its name on UI.	
24		The system shall have the provision to take multiple samples of same face belonging to same person	

SNo.	Parameter	Specifications	Compliance (Yes/No)
25		Real Time Face Detection & Recognition Solution: This application detects and analyses the faces captured in real time from a face recognition camera. The application does real time video screening and shows the matching results instantly. The application also gives anonymous people analytics.	
26		The facial recognition system should be accessible from 5 different desktop/ laptops at any given time.	
27		FRS must support a user management module that enables different user level groups to support various permission levels.	
28		The system shall have option to enrol face images from CCTV cameras/video source.	
29		The system shall have option to enrol face images from video source.	
30		The system shall have option to enrol face images from image source.	
31		The system shall have option to detect Age of face detected/recognize.	
32		The system shall have option to detect Gender of face detected/recognize.	
	Alert Generation		
1		The system should have option to input certain face description according to the hot listed categories like “VIP”,"CRIMINAL",“SUSPECIOUS”, “NORMAL”,"STAFF", ”MISSING” etc. by authorized personnel.	
2		The system should be able to generate automatic alarms to alert the control room personnel for further action, in the event of detection of any face falling in the Hot listed categories like VIP, CRIMINAL, SUSPECIOUS, MISSING.	
3		FRS Capture face images from live CCTV feed and generate alerts if a blacklist match is found.	
4		Email Alert:-The system should be able to generate automatic email alarms to alert the control room personnel for further action, in the event of detection of any face falling in the Hot listed categories. i. Criminal/Suspicious Email Alert- Automatic Email will send to care taker if any CRIMINAL/SUSPECIOUS	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		person appears in front of Camera view. ii. Staff Email Alert- Automatic Email will send to caretaker if any STAFF person appears in front of Camera view. iii. VIP: Automatic Email will send to caretaker if any VIP person appears in front of Camera view. iv. Unknown: Automatic Email will send to caretaker if any UNKNOWN person appears in front of Camera view. v. Along with Email App will send recently detected/recognize image, Persona Name, Category like VIP,STAFF,SUSPECIOUS/CRIMINAL, Date & Time.	
5		Visual Alert:-The system should be able to generate automatic visual alert by showing flashing screen alarms to alert the control room personnel for further action, in the event of detection of any face falling in the Hot listed categories	
6		Audio Alert:-The system should be able to generate automatic audio alarms to alert the control room personnel for further action, in the event of detection of any face falling in the Hot listed categories	
	Important features		
1		System is able to Moderate aging changes – Recognition	
2		System is able to Changes in facial expression – Recognition	
3		System is able to Changes in beard or hair – Recognition	
4		FRS act as Investigation Tool, which can work on recorded videos post- incident analysis	
5		FRS should detect gender of detected or recognized face. Etc male, female.	
6		FRS should detect age of detected or recognized face.	
		Report – Vehicle Log Module & Search Options	
1		System should generate report by Location.	
2		System should generate report by Date & Time combinations.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
3		System should generate report based on Watchlist category like 'Wanted', 'Suspicious', 'VIP', 'Authorized', 'Staff', 'Normal'.	
4		System should generate report based on Face Name.	
5		Allows face to be tracked across multiple cameras or Locations	
6		Records and logs all license plates at a scene for later forensic investigation	
7		System should able to give OCR Image/Licence plate Image	
8		System should generate report by 'Wanted', 'Suspicious', 'VIP', 'Authorized', 'Staff', 'Normal' watchlist category.	
9		The system shall enable easy and quick retrieval of snapshots, other data for post incident analysis and investigations. For example a database could be searched using criteria like date, time, location and face name, watchlist category.	
10		The system should be able to generate suitable reports that will provide meaningful data to concerned authorities and facilitate optimum utilization of resources. System should able to give camera ID / Camera Location etc on report page, System should able to give recognize face image with confidence %, System should able to give train face Image. System should able to give Watch list category ("Wanted", "Suspicious", VIP", "Staff", Authorized', 'Normal') on report page.	
11		The system shall have option to save custom reports for subsequent use. The system shall have option to export report being viewed to common format for use outside of the FRS or exporting into other systems.	
12		The system Graphical User Interface should be bi-lingual: it shall support both English & Graphical User interface (GUI) should provide following information: - a. Image of the recently detected face. b. Image of the train face.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		c. Person name in Text. d. Date, Time and location of face. e. Event/images/Date/Additional Information of face	
	Face Status Alarm Module		
1		On successful recognition of the Face system should be able generate automatic alarm to alert the control room for faces which have been marked as "Wanted", "Suspicious", "VIP",	
		Watchlist	
1		The system should have option to input certain face description according to the hot listed categories like “VIP”, "CRIMINAL", “SUSPECIOUS”, “NORMAL”, "STAFF", ’Authorized’ etc. by authorized personnel.	
2		The system should have ability to handle initial real-time watch list of 10,000 Faces	
		Face Log Module / Search By	
1		The system shall enable easy and quick retrieval of snapshots, and other data for post incident analysis and investigations. For example, a database could be searched using criteria like date, time, location and Person Name, Camera Name, according to category.	
2		The system should be able to generate suitable MIS reports that will provide meaningful data to concerned authorities and facilitate optimum utilization of resources. These reports shall include.	
3		The system shall have Search option to tune the reports based on person name, date and time, site location as per the need of the Authorities.	
4		The system shall have option to save custom reports for subsequent use. The system shall have option to export report being viewed to common format for use outside of the FRS or exporting into other systems.	
	Storage		
1		The System shall store JPEG images of faces.	
2		The system shall store the vehicle license number into a relational SQL database (MSSQL, PostgreSQL, MySQL, Oracle, etc) along with date	

SNo.	Parameter	Specifications	Compliance (Yes/No)
	Integration : Hardware, VMS, Relay Devices, Third Party NVR, DVR		
1		Available with API/SDK for partners and external systems.	
2		Integrated with analogue, IP/network and digital cameras (it can also take video input from many DVR and NVR/video management solutions)	
3		Enables security professionals to rapidly search for past incidents from archived video	
4		Increase productivity and efficiency of the security professionals	
5		Video Analytics should communicate or integrate with any Video Management System (VMS).	
6		Video Analytics should communicate with VMS and select specified cameras for processing.	
7		Video Analytics should detect incident and same incident share with VMS system.	
8		Video analytics should communicate or integrate with relay devices.	
	Automatic eAlerts & Event Messages:		
1		XLS Output Report: User can export all events inside XLS.	
2		Email: Email functionality available to report people count.	
3		Email: Email functionality available to report any incident happen for mention analytics.	
4		HTML Reports: HTML reports available on UI.	
5		Database / ODBC: MySQL Database support available.	
6		REST JSON API: Using API we can communicate with any third part hardware/software.	
66.	**ANPR & Vehicle Detection**		
A	Vehicle Detection Module		
1		The System should automatically detect a vehicle in the camera view using video detection and activate license plate recognition	
2		The system shall detect and recognize number plates from images.	
3		The system shall detect and recognize number plates from Video Clips.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
4		The system shall detect and recognize number platess from IP Cameras, Input: RTSP/HTTP stream from network/IP cameras	
5		Detects and recognizes license plates on moving or stationary vehicles	
6		Handles different plate styles, e.g. regular/stacked	
7		Various LPR/ANPR models available: gates, entrance, roadside, traffic lights, parking lots, highway, tollway and mobile/ law enforcement vehicles	
8		ANPR should supports processing of single frames and video streams	
9		ANPR should easy to deploy with a wide variety of cameras	
10		The system shall be designed to work for 24x7 unattended operations	
11		The System shall automatically detect the license plate in the captured video feed in real-time.	
12		The system shall perform OCR (optical character recognition) of the license plate characters (English alpha-numeric characters in standard fonts).	
13		The System shall store JPEG image of vehicle and license plate and enter the license plate number into DBMS like MySql database along with date time stamp and site location details.	
14		The system should be able to handle multiple vehicles simultaneously i.e. if there are more than one vehicle in the camera view the system should be able to detect all of them, extract their license plate numbers and perform OCR on the license plate characters	
15		System should be able to detect and recognize the English alphanumeric License plate in standard fonts and formats of all vehicles including cars, HCV, LCV and two wheelers.	
16		System should able to detect single row, double row, multi row, square and rectangular plates as well	
17		The system shall be robust to variation in License Plates in terms of font, size, contrast and color and should work with good accuracy.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
18	Image Processing / offline mode	Analytics should process images and extract Number plate details.	
19	Video Processing / offline mode	Analytics should process video/clips and extract number plate details.	
20	Model Classification	Analytics should classify the vehicles like Truck, Bus, Car, Motorbike.	
21	Traffic Congestion, Predicts traffic jams and congestion ahead of time.	Application should detect traffic congestion on the road. System shall detect congestion levels in real-time: Free Flow Moderate Traffic Heavy Traffic Congested / Gridlock	
22	Smart Parking Management - Reduces roadside parking chaos and improves route flow.	Application should detect the vehicle park in non-parking area, this is zone-based tracking.	
24	ANPR-Based Vehicle Monitoring - Detects suspicious or blacklisted vehicles.	License Plate Recognizer™ is a Deep Learning and AI-based license plate detection, recognition solution. Application should detect suspicious or blacklisted vehicles using predefine watchlist functionality.	
25	Special Service Vehicle classification	Analytics should classify Fire trucks; Police vehicles; Ambulance vehicles.	
26	Axel Counting	Analytics should count number of axles for a vehicle.	
27	Watchlist	i. Compares detected plates against a watch list database and provides real-time alerts on plate matches. ii. Enables automated matching against a watch list with real time alerting	
28	Speed Detection	Application should identify the speed of vehicle and triggered events based on high-speed vehicle.	
B	Automatic eAlerts & Event Messages:		
1		System should generate alerts based on 'Authorized', 'Stolen', 'Lost', Wanted', 'Uncategorised', 'Suspicious' based on predefine database.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
2		The system should be able to generate automatic alarms to alert the control room personnel for further action, in the event of detection of any vehicle falling in the Hot listed categories	
3		XLS Output Report: User can export all events inside XLS.	
4		Email: Email functionality available to report people count.	
5		Email: Email functionality available to report any incident happen for mention analytics.	
6		HTML Reports: HTML reports available on UI.	
7		Database / ODBC: MySQL Database support available.	
8		REST JSON API: Using API we can communicate with any third part hardware/software.	
C	Physical Alerts		
1		Sound & Audio: Buzzer alerts available with system	
D	Visual Flashing Alerts		
1		Flashing event alert on screen: Flashing event alerts available on UI.	
E	Storage		
1		The System shall store JPEG/MJPEG images of each action perform in video & also store event video.	
2		The system shall store the event data into a MySQL.	
F	Integration: Hardware, VMS, Relay Devices, Third Party NVR, DVR		
1		Available with API/SDK for partners and external systems.	
2		Integrated with analog, IP/network and digital cameras (it can also take video input from many DVR and NVR/video management solutions)	
3		Enables security professionals to rapidly search for past incidents from archived video	
4		Increase productivity and efficiency of the security professionals	
5		ANPR should communicate or intgrate with any Video Management System (VMS).	
6		ANPR should communicatr with VMS and select specifide cameras for processing.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
7		ANPR should detect incident and same incident share with VMS system.	
8		ANPR should communicate or intgrate with relay devices.	
G	Graphical User Interface		
1		The system Graphical User Interface should be bi-lingual: it shall support both English & Graphical User interface (GUI) should provide following information: - a. Image of the vehicle b. Image of the number plate c. Text conversion of number plate after using OCR (Optical Character Recognition) technology d. Date, Time and location of offending vehicle e. Event/images/chart of ANPR f. Axel count g. Color	
H	Report – Vehicle Log Module & Search Options		
1		System should generate report by Location.	
2		System should generate report by Date & Time combinations.	
3		System should generate report based on license plate number.	
4		System should generate report based on vehicle type.	
5		System should generate report based on vehicle axel count.	
6		System should generate report based on vehicle make & model.	
7		Allows vehicles to be tracked across multiple cameras or Locations	
8		Records and logs all license plates at a scene for later forensic investigation	
9		System should be able to give OCR Image/Licence plate Image	
10		System should be able to give Watch list (“Wanted”, “Suspicious”, “Stolen) on report page	
11		The system shall enable easy and quick retrieval of snapshots, video and other data for post incident analysis and investigations. For example, a database	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		could be searched using criteria like date, time, location and vehicle number	
12		The system should be able to generate suitable MIS reports that will provide meaningful data to concerned authorities and facilitate optimum utilization of resources. These reports shall include.	
13		The system shall have option to save custom reports for subsequent use. The system shall have option to export report being viewed to common format for use outside of the ANPRS or exporting into other systems.	
14		Wild Character Search:- The system should provide advanced and smart searching facility of License plates from the database. There should be an option of searching number plates almost matching with the specific number entered (up to 1- and 2-character distance).	
I	Vehicle Status Alarm Module		
1		On successful recognition of the number plate, system should be able generate automatic alarm to alert the control room for vehicles which have been marked as "Wanted", "Suspicious", "Stolen", "Expired". (System should have provision/expansion option to add more categories for future need).	
2		The Instantaneous and automatic generation of alarms. In case of identity of vehicle in any category which is define by user.	
J	Storage		
1		The System shall store JPEG/MJPEG images of vehicle as well as of thumbnail of the license plate for each vehicle	
2		The system shall store the vehicle license number into a relational SQL database (MSSQL, PostgreSQL, MySQL, Oracle, etc) along with date timestamp and site location details. The necessary license/subscription/support services of the database software should be bundled with the ANPR software.	
K	Vehicle Category Editor		
1		The system should have option to input certain license plates according to category like "Wanted",	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		"Suspicious" "Stolen", “Expired" etc. by Authorized personnel.	
2		System should have option to specify maximum time to retain vehicle records in specific categories.	
3		The system should have option to update vehicle status in specific category by authorized personnel. e.g. on retrieval of stolen vehicle, system entry should be changed from "Stolen" to "Retrieved".	

Group-10: Smart Mobility, GIS & Digital Platforms

SNo.	Parameter	Specifications	Compliance (Yes/No)
67.	**ITMS Application**		
1		System should have option for multiple options for discovery including IP address based discovery, IP address range discovery, CSV based discovery for bulk discovery and it should allow options to add custom fields to support customer specific data to upload during discovery.	
2		The system should fetch topology via SNMP for ARP tables from routers, MAC tables from layer 2 switches, cisco Discovery Protocol, Link Layer Discovery Protocol, Foundry Discovery Protocol or SynOptics Network Management Protocol. The discovery should be automated and continuous.	
3		Discovery has to work intelligently by identifying the device in the network by the given IP range and categorize into network devices and servers with vendor and model details.	
4		Automatically learn devices that supports SNMP, HTTP, Ping, SMTP, POP3, WMI, JMX, SOAP, REST API, IPDC, SSH and Telnet along with any required protocol to communicate to the devices.	
5		System should support global threshold and it should have option to define individual resource/interface statistics level threshold.	
6		Threshold & Alerts: define and store static & dynamic resource utilisation thresholds, define and maintain availability thresholds for individual components, services or applications, individual service actions / automated operations (performing a transaction, running an automated procedure	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		etc.), support comparison of actual availability, actual performance with agreed levels and alerting on breaches.	
7		Configurable parameters like frequency, data duration, resolution duration, sigma based polarity value, reset points should be available.	
8		All thresholds should have set point, reset point, polarity, set point message and reset point message for ease of use.	
9		Detect & highlight faults (abnormal situations) in near real-time occurring anywhere within the monitored IT infrastructure.	
10		Provides Filtering, De-duplication, Holding, Suppression and Correlation capability to let users focus on the critical event that affects the business and business processes.	
11		Provides multi-level (preferably six-level) Severity definition, will handle events automatically and inform the designated person as per operational requirement.	
12		System should support separate Rule Engine based alarms apart from the generic threshold.	
		a. Should have capability to configure Device Group based, Node Based, Resources/Interface based, Aggregation link based.	
		b. On Selection of Nodes/Resources/Aggregation links it have flexibility to filter based on fields available in node information	
		c. Rules should have option to apply configuration on top of performance value or based on configured threshold alarms	
		d. Rules should have option configure the breach based on min, max and average values	
		e. Should have option to configure rules in repeat counters	
		f. Should have options to select custom alarm and clear alarm messages for individual configured rules	
		g. Should have option to send severity levels like error, warning and information	
		h. Notifications support based on configured rules	
13		Provides alarm suppression with hold time and aid in prevention of flooding.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
14		Sends alert via E-mail, SMS, Execute Batch file, SNMP Trap, XML notification, Pop-up window and Audio alert.	
15		Monitors all traffic from all the interfaces of the network device. Provides traffic Utilization based on individual interface level, nodes level or based on the group by location, branch, departments etc. as an Avg, Min and Max bandwidth, utilization, throughput or any custom monitoring parameters.	
16		Provision to change the polling interval to any frequency depending on the priority till the individual component / resource level like each interface might have the different polling interval in the same device based of the criticality and importance of service customer.	
17		System should have capability to configure business, non-business hours or custom time polling. These configurations should be available for every device as well as every component in the device.	
18		Provision to disable and enable the polling of specific type of devices.	
19		System should have capability to configure the maintenance period for any device. When device is in maintenance period there is no polling done and the SLA clock on the device is stopped.	
20		SLA calculation / Isolation report should be made with the consideration of both the Primary and Secondary link together instead of individual link based. The downtime calculation will be measured when both the links are down for internal reporting and link based for ISP reporting. System should provide the flexible configuration in UI itself based on user needs.	
21		Provide a notification mechanism that allows administrator to define what notification channel to be used in different times of days, and able to trigger multiple notifications to alert multiple person and actions.	
22		Provide standard reports that display current status of nodes and interfaces. Reports could be viewed on daily graph (5 minute average), weekly graph (1	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		hour average minute average), monthly graph (1 hour average) and yearly graph (1 day average).	
23		Reports & Dashboard: Pre defined Availability, Performance, Capacity Dashboards & Report. Should have option to drag and drop dashboard configuration option Should have option to add multiple type of widgets along with (Tabular, Summary, Multiple Graph options), Filter (predefined & Dynamic), Sort, Search, Group by, multi threshold, Export option to PDF, XLS etc., Generate automatically and send over Email or to a predefined folder, possible to define custom KPIs , A KPI definition must include the period-bound target value and the threshold value (to distinguish between the Green, Amber and Red zones.).	
24		Automatically generate daily reports that provide a summary of the IT Infrastructure as well as custom Reports and that are automatically sent by email at a pre-defined schedule to any recipient or save into any specific folder or drive.	
25		Supports instant diagnosis of the node status through Ping, Telnet and SNMPwalk.	
26		Support Real-Time report generation for checking continuous reachability of target device.	
27		System should provide many different types of topology representation. To perform the following :	
		1. Display physical connections of the different devices being monitored in the system	
		2. Display flat maps of the entire network or networks in a single view	
		3. Display customer maps based on user configurations	
		4. Display maps based on geo locations	
	Network Traffic Analysis		
28		The proposed monitoring solution should be able to monitor network traffic by capturing flow data from network devices, including Cisco Netflow v5 or v9, Juniper J- Flow, IPFIX, sFlow, NetStream data and also sampled Netflow data. Solution must be able to store ALL flows without any rollups or loss for retention period - for security and audit purposes.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
29		Should identify which users, applications, protocols, countries, AS numbers, top routers, and top interfaces are consuming the most bandwidth	
30		Proposed solutions should be sized for unlimited flow data.	
31		Should be able to associate traffic coming from different sources to application names	
32		Should be able to receive flows from non-SNMP-enabled devices, like VMware vSwitch	
33		Should monitor Type of Service (ToS), Differentiated Services Codepoint (DSCP), and Per-Hop Behaviour (PHB), BGP AS and NEXT HOP	
34		Should provide flow analysis with 1-minute granularity and The solution should be able to monitor up to 5 million flows per second, and should employs advanced optimization methods.	
35		Solution should support advanced SSL/TLS analysis like detecting false certificates, expired, self-signed.	
36		Solution should also feature signature-based detection techniques and allow drilldown to packets from alerts.	
37		Solution should provide DDoS reports in real time within 1 minute after detection of attack with details of IP, Ports, ASN numbers, Router Interfaces, Customers facing the attacks.	
	Service Management		
38		Low Code /No Code Platform for Integration:	
39		Tool should provide REST APIs to integrate with IT Infrastructure Management, Configuration Management, Network Management, CRM, SIEM tools to automate Events to Ticket.	
40		The proposed tool must provide Dynamic REST/WEB API integration without writing any code, just by configuration on GUI with various inbuilt Authentication method.	
41		Should be able to do 2 Way Integration with 3rd party and should be able to exchange the data at any stage of the lifecycle of the Event, Incident, Problem, Change, Request, Task, Release etc.	
42		Tool should provide Drag and Drop based Workflow Process Design and No code Input Forms design	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		using Drag and Drop method for different processes, services and workflow	
43		No code automation platform to support Rule executions (value based, Time based rule executions)	
44		Team/Individual Pressure/Load Score, Efficiency Score, Expertise Score should be present on Dashboard	
45		Tool must provide intelligent Email-to-Incident feature in which tool admin has the option to allow certain domains for automatic conversion of emails to tickets. Tool should merge all subsequent email communication for a particular email-to-incident ticket into the same ticket in the form of a message thread. Tool should be intelligent enough to understand email conversation chains for merging emails to a particular incident. Merging logic should be not only based on TicketID but also on email sender, cc responses to that email chain	
46		Tool should be able to provide real-time Email, SMS Notification alerts to notify respective users about any changes in ticket state and status. Tool should provide Email Communication Interface to allow technicians to send replies to customers / end users from the tool GUI and Record all the Email Communication in Chronological Order	
47		The integrated ITSM module should have its own Android & IOS app	
48		The proposed tool must provide GUI interface for users, requesters, customers, support staff, 3rd party vendors, Area Managers, Field Engineers, Site Engineers, Supervisors, Managers, (Helpdesk available 24x7 at customer site) etc. with options to restrict amount of information that can be accessed by each role	
49		The proposed tool should have the capability to be able to define and access the Business and Technical catalogue separately	
50		The tool should allow the administrator to create categories and multiple sub-categories (under each category) in hierarchical order for services being offered to the end users.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
51		Tool should have option to define the workflow for each service created in the Service Catalog for each process (Incident, Problem, Change, Request)	
52		The tool should provide a self service portal where End-users / requesters can log in and raise incidents	
53		End user should also be able to browse the service catalogue and should be able to raise request by providing the input to particular service request, Address etc.	
54		The proposed tool must provide an option for users to track their incidents status, check knowledge articles and chat with technicians on particular incidents	
55		Users must have an option to Log, Classify, Categorize & Prioritize Requests	
56		The proposed tool must provide an option to design the request management input parameter template for each service in service catalogue	
57		The proposed tool must provide an option to design dynamic workflows, lifecycle, Tasks, Notification action for each service which can be requested	
58		The proposed tool must record Problem Record Date and Time, Problem Source, Contact Detail, Symptoms and Status	
59		Tool should allow problem records to be classified according to priority and category	
60		Tool should allow a problem record to be escalated based on pre-established rules with option to manually overridden conditions	
61		Tool should allow users to create, edit & delete Change Request through web interface, Each CR should have Unique and any authorized user should be able to raise RFC	
62		The proposed tool must provide Change records Categorization, classification according to Change Class (Permanent, temporary, Recurring), Change Type (Normal, Standard, Expedited, Latent, Emergency), Change Category, service category, Impacted Service, Impact, Urgency, Priority	
63		The Change records in the proposed tool must contain State & Status information along with	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		Dynamic Workflow definition with color coding for each status	
64		There should be records for Benefits, Effects, and Required resources & Cost required to perform change	
65		The proposed tool must have a powerful knowledge management functionality	
66		Knowledgebase Management should be integrated with the NMS/EMS system	
67		The proposed tool must provide Role based, Team Based & User Based access control on KB articles/FAQ/Information/KE/Solutions etc.	
68		In FAQ/Solutions type of knowledge, system should allow to add multiple questions/multiple solutions within single knowledge article	
69		Tool should have option to promote knowledge to analysts (Service Desk) and end users (Service Portal)	
68.	**Geographic Information System (GIS)**		
	Business Requirements of GIS for Project		
1		The MSI shall provide Geographical Information System (GIS) to map physical locations of all the field components, location of incidents, locating site of faulty devices and corresponding geographic analysis etc. of the system.	
2		The MSI shall undertake detail assessment for integration of the proposed system with the GIS system.	
3		It should also help higher management of department, to analyse the events on a spatial perspective.	
4		The GIS system - procurement of latest, base map from service provider like Here Map etc., shall be sole responsibility of the SI/contractor/bidder. The base map shall be with scale of 1:2000 for entire city jurisdiction of the city.	
5		Details of available layers related to administrative boundaries will be provided by Authority / department.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
6		The base map shall include rivers, water bodies, land use, land cover, Transport network (Rail and Road), POI. Administrative boundaries (districts, city, wards) for project requirements for entire City. All administrative boundaries shall be collected from Authority / departments.	
7		MSI is required to update GIS maps (including the additional layers of data as required for proposed solution) on annual basis.	
8		Necessary vector data, mapping of project proposed assets on separate GIS layers shall be sole responsibility of the SI/contractor/bidder.	
9		SI shall ensure that GIS application is integrated with Video analytics System to support the officials to navigate on the map and use it for better spatial understanding.	
10		SI shall ensure that GIS application is integrated with PA System to support the officials to navigate on the map and use it for better spatial understanding.	
11		Use of GIS tool which allows easy map editing for wide area monitoring.	
		Functional requirements of GIS	
12		The MSI shall accurately map the spatial attributes such as resources, objects, sensors and elements etc. on the map. It should provide an integrated dashboard with an easy to navigate user interface for managing different types of users and GIS based analysis.	
13		Basic Web GIS based functionality (Out of Box Dashboard, Ready for deployment)	
14		1) Layer Management: - The GIS application should have facilities to manage / group the layers. It should have options for displaying layers as display on or off. Further transparency and visibility scale shall be fixed for each layer.	
15		2) Measurement Tool: - This tool should help user to measure Length, Area over the map	
16		3)Identification Tool: - This tool should allow user to view details of the selected feature of the active layer on the map	

SNo.	Parameter	Specifications	Compliance (Yes/No)
17		4) Swipe Tool: - This tool should help user to view changes in between two active layers by swiping each other	
18		5)Navigation Tool: - Map displaying navigation tool includes display with different zoom function like fixed zoom, in/out zoom, by rectangle, by scale, to full extent, zoom to layer extent, zoom backward/forward, pan etc.	
19		6) Query Tool: - Using this tool user can select feature in a layer using s SQL based expression as per layer attribute. It also has spatial query feature to select feature in between layers. And the quarried features can be exported as standard XLS, PDF, CSV formats.	
20		7) Bookmark Tool: - This tool should allow user to save particular zoom/location of layers over the map and revisit the same zoom/location.	
		Standard Web GIS based functionality	
21		1) Buffer Analysis: - This functionality should allow user to create buffer around a feature as per desired distance value and can get another feature from other available layers (i.e. road network, POI, Assets etc.). The result can be exported as standard XLS, PDF, CSV formats.	
22		2) Overlay Analysis: - Overlay is a GIS operation that superimposes multiple data sets (representing different layers like administrative boundary, road network/node, land parcel, other proposed layer etc.) together for the purpose of identifying relationships between them. The result can be exported as standard XLS, PDF, CSV formats.	
23		3) Proximity Analysis: - Using this functionality user can analyze locations of features by measuring the distance between them and other spatial features in the area (i.e. distance of road network from any GIS feature and other related spatial layer etc.). The result can be exported as standard XLS, PDF, CSV formats.	
24		4) Network Analysis: - Using this functionality user can get optimum route between two points/nodes of network data (like road network and other	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		related network spatial layer) layer and export it as standard XLS, PDF, CSV formats.	
25		5) Map Print: - This tool help user to print map as per their requirement with proper scale and Symbology.	
26		6) Info-Graphics: - Shall be able to provide management with easy-to-understand, easy-to-use reports that use appropriate info graphics (Charts) to monitor the performance and usability of the project	
		Traffic Trend Analysis	
27		Heat map analysis to showing the trend of Traffic by using traffic Volume data (from ITMS application)	
28		Re Routing In case of accident, emergency incident, GIS can suggest the alternate route	
29		Dissemination of customized Geo spatial information to concern stakeholders (Traffic Police, Municipal corporation & Others)	
		Dashboard	
30		Map Handling Module Map viewer will show all the roads within the municipal limits with footpath surface as well as it will show traffic lights as point location User can identify bus stand, bus route, and petrol pumps location on map.	
31		Query Module With queries user can identify position of road divider, bus stand, bus routes, location of petrol pumps etc.	
32		Routing Network & Routing will enable user to find out alternative route in case of Jam, emergency or certain festivals (Integration with ITMS applications), user can also user routing for identifying routes of all petrol filling vehicle	
33		Spatial Query: Spatial analysis will enable user to get information of assets & relevant features based on selected area	
34		Reports It will be generated with query results	
		Integration Scope	
35		The GIS application shall be integrated with ICCC to support the Control Centre and ICCC operator to navigate on the map and use it for better spatial understanding.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
36		All the CCTV camera, and other sensor's locations shall be mapped on to the geospatial map as a separate GIS layer. Operator shall be able to see the video feed and other output from specific camera(s) / sensors by clicking on the camera icon on the geospatial map.	
37		The system shall have provision to visually display an alarming sensor on map and visually differentiate sensor alarm severities on map through different colour and icon identifiers.	
38		The ICCC operator shall have provision to view alarm details (including description, video, etc.) and investigate the alarm from the map	
39		The system shall have provision view sensor and related name from the displayed map.	
40		The system shall allow map information to be displayed on the map including but not limited to	
41		Sensors type and name	
42		Sensor range (e.g. camera – orientation, range, field of view angle)	
43		Locations and zones	
44		Resource tracks	
45		Allow Authorized user to zoom in/out on different regions of map	
46		The system shall have provision to have multiple layers on the map including	
47		Sensors, Cameras, VMS etc.	
48		Incident intensity map in the city	
49		Violation intensity map in the city	
50		High Traffic Density map in the city	
51		Filters for incidents / violation / traffic by road type, date, time, type, reason etc. on the Map	
52		Major Buildings / Structures / Roads	
53		Should support Geo Spatial Standards like GML & KML/KMZ etc	
	Specification of Cots Based GIS Enterprise and Desktop Platform		
54		To achieve this, department requires a deployment of a COTS GIS Enterprise & desktop platform. In	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		Enterprise Platform, Server-side geo processing for spatial, non-spatial, Image analysis, 3D analysis is required for this project without any dependency over script or workflow generated from Desktop. This GIS enterprise platform should work as a base system for development and all required components i.e. GIS, Image Analysis should be get accessed by the end user at browser only. The Enterprise system should be GIS enabled system and capable of cataloguing and disseminating data through a web-based environment. The detailed technical specifications are provided below.	
55		Software should be Fully Compliant Make in India product	
56		Licensing policy should be open. No additional cost / authorization process is not required for redeploying it in new machine / cloud / VM. This shall provide flexibility to end customer. No restriction during hardware upgrade/ scaling in future	
57		The GIS server should have GIS, Image Processing and 3D components in a single deployed server only without any additional cost. There should be no dependency / importing functionalities from GIS Desktop for any tools. This component should run as Geo-processing at server side only.	
	The proposed solution should have		
58		GIS, Image Processing, 3D components with all extensions (Mentioned in below) in a single Deployed COTS Desktop Platform	
59		GIS, Image Analysis, Processing and 3D components in Single deployed COTS based Enterprise Platform	
	Specifications for COTS GIS Enterprise Platform		
60		The proposed single deployed GIS Enterprise Platform should be Industry standard COTS GIS platform and must be OGC compliant. The proposed single deployed GIS platform should have all functions of GIS and Image analysis, geo-processing, classification, change detection, in a single installed software only. The platforms should	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		also have advance modules like network analysis, change detection.	
61		The Proposed solution should be an integrated solution only having GIS, 3D Analytic and Image Processing components in single COTS Enterprise software. The overall proposed solution should be of Single GIS Platform only	
62		The GIS Enterprise platform should have both GIS and Image analysis components, which going to be deployed at site. It should support 64 bits. It should based on a Services Oriented Architecture (SOA). The Enterprise GIS software must be OGC certified and must have the capability to serve and consume OGC complied web services including WMS, WFS, WCS, CSW, INSPIRE, etc.	
63		OEM undertaking should be submitted for further customization of application based on GIS and Image processing Custom based web application, as per project needs of present and future. No restriction during hardware upgrade/ scaling in future.	
64		Server deployed Software should run as a native 64-bit application and should support Windows & Linux 64- bit.	
65		The deployed enterprise platform should have capabilities like geo-processing and analysis, spatial and statistics analysis and Image analysis functions. It should support server end Geo processing and Image analysis functions i.e. supervised classification, Enhancement, Vegetation Indices, Normalized Burn Ratio Index (NBRI), Normalized Difference Built-up Index (NDBI), buffer, clip, erase. Provision should be available by server for sending the request using the web client and display the processed data on web using OGC certified services. No dependency of Desktop tools or workflow generated from desktop.	
66		The web GIS application should open on any browser and should support cross platform. It should have Rest API for integration with other applications	

SNo.	Parameter	Specifications	Compliance (Yes/No)
67		The GIS Enterprise platform should provide a map centric for managing geospatial content of organization. It should serve as project centric approach to Create, Access, Analyse, Manage and disseminate geo-spatial content with capability of user management and role-based access control.	
68		GIS Enterprise Platform should have rich display and navigation tools like zoom in, zoom out, fixed zoom in, fixed zoom out, pan, real time pan, bookmark, Geo link multiple views, swipe, flicker, search by location, cursor location value, etc.	
69		The GIS enterprise software should support draping of vector and raster: WMS, WMTS, KML/KMZ. Facilities to view Shape File, DGN, GPX & Geo-tiff, TIF. Provision to process and display CEOS SLC and Hybrid Polarimetric data of SAR, DTED, DEM. It should support various data such as Terrain (DEM, Tiff, DTED etc..), BIM & CAD (Revit, CAD, 3D-Max, Sketch-up, Maya etc..), 3D Building and animation file i.e CZML Collada - *.dae, *.obj, *.gltf. Photogrammetry Meshes data derived from UAV. Display of model generated form Drone, Satellite Stereo Pairs, LiDAR, Point Clouds (LiDAR data *.las, *.laz). Support of Vector data (GeoJSON, KML, Shape etc.), OGC (WMS, WFS, WCS, etc.), Capable of consume multiple third party OGC map services for visualization	
70		It should have capability to import / export data in various formats like .dwg,dxf, .dgn, .shp (shape files), coverage file, .mif (MapInfo), .gml, .kml, .gpx. , Geo PDF GeoJSON, H4, H5 formats, MBtiles etc. Should support ODBC compliance interface with industry standard RDBMS like PostGRE SQL, Oracle, SQL server, Access etc.	
71		The deployed GIS enterprise Platform should have capabilities like geo processing and analysis, spatial and statistics analysis and Image processing functions in a single window. It should have out of box Geo processing and Image analysis functions like Clip, Erase, Spatial Join, Relate, Buffer, clip, erase, intersection, dissolve, union, summarize, Image classification for ex supervised, High pass,	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		Low Pass filter, NBRI, NDBI, 3D viewer with 3D based analytic tools as out of box functions.	
72		Software should have the facility for reports generation, customized map layout, high resolution printing in different formats (jpg, pdf) with desired map scale and customized templates.	
73		Should have capability to store the applied legend, colour, symbology and further applied in other GIS projects. Further, provision should be there to take backup of the project, export and import the custom annotation and labelling pattern from one project to other. Thematic mapping like Bivarte, Multi-bivarte, chart mapping should be available as out of box. Geocoding and Reverse Geocoding should be available.	
74		Integrated deployed Platform should support Time aware data for Trends / Time Series Analysis. Provision should be there for Online and Offline GPS integration.	
75		It should have network analysis module to perform Routing analysis, Service Area Analysis, etc. Capabilities like Dynamic Labelling and Rule based Labelling should be available	
76		The software should have function to perform different operations like: mathematical, logical, string operations on the field of table of vector layer or selected objects of vector.	
77		The integrated software should allow visualization of data in 2D/3D in enterprise application. Provision should be available to host the 3d project from to browser mode. Facilities to import Satellite images, LIDAR, Building model. The system should have facilities to store the 3d model which can be used in future without doing any pre-processing.	
	Specifications for COTS GIS Desktop Platform		
78		The proposed deployed COTS GIS Desktop Platform should be Industry standard COTS GIS platform and must be OGC compliant. The proposed deployed GIS platform should have all functions of GIS and Image feature extraction, geo-processing, image mosaicking, Photogrammetry, sub setting,	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		classification (supervised, unsupervised) changes detection (In-built Image processing capability) in a software. The platform should also have advance modules like network analysis, terrain analysis.	
79		The deployed Platform should have capabilities like geo-processing and analysis, spatial and statistics analysis and Image processing functions in a single window. It should have out of box Geo processing and Image analysis functions like Clip, Erase, Spatial Join, Relate, Buffer, clip, erase, intersection, dissolve, union, polyline to polygon, summarize, polygon auto numbering based on line feature and direction, Image classification(supervised, unsupervised), Image segmentation , Recode, Enhancement , Layer stacking, Geo-referencing ,Collage Image, Mosaicking, High pass, Low Pass filter, Fast Fourier transformation as out of box functions	
80		The Proposed COTS Platform should have features of image analysis, spatial analysis, 3D analysis, Network analysis and Data Reviewer included without requiring any separate extenstion	
81		The desktop software should be able to share 3D Tiles datasets as web layers to web platform.	
82		To provide the capability to digitize three-dimensional (3D) feature data in a stereo viewing and mapping system.	
83		Should have capability to Computes 3D points from stereo pairs and outputs a point cloud as a set of LAS files	
84		The GIS Platform should have ready to use Pre Trained Deep Learning Models ready to be used in Server and desktop levels	
85		The software should feature in built extension enabling the application of traditional AI techniques for spatial data generation, including extraction, classification, detection from both structured and unstructured data.	
69.	**Data Lake & Analytics**		
1		Domain Compatibility: The proposed Data Lake solution shall provide analytics and insights to	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		address business and operational challenges specific to smart city use cases	
2		Data Ingestion: The platform shall efficiently ingest structured, semi-structured, unstructured, and streaming data from multiple sources. It shall support real-time ingestion of video, images, and metadata from approximately 2,600 cameras, ensuring scalable, high-throughput, and fault-tolerant pipelines with minimal latency for seamless data flow into the data lake.	
3		Data Storage and Management: The platform shall store and manage large volumes of structured, semi-structured, and unstructured data using scalable architectures such as data lakes, data warehouses, and NoSQL databases	
4		Data Processing and Analysis: The solution shall support complex data processing and analytical capabilities, including data cleaning, transformation, integration, aggregation, data mining, machine learning, and predictive analytics. Data processing and transformation will be performed for all 2,600 cameras/55 Use cases under the smart city infrastructure	
5		Customizable Dashboards and Reporting: The platform shall provide interactive dashboards, visualizations, and reports, enabling users to explore data, analyze trends, and derive actionable insights to support informed business decision-making.	
6		Real-Time Analytics: The platform shall process and analyze data in real-time or near real-time to detect patterns, anomalies, and actionable opportunities, enabling timely insights and proactive decision-making.	
7		Data Lake Management: The platform shall provide a GUI-based solution to manage and monitor data lake clusters, infrastructure health, and services, with integrated alerting mechanisms for proactive issue detection and resolution	
8		Integration and Interoperability: The platform shall support customizable, automated pipelines to integrate batch and streaming data from enterprise	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		applications, databases, files, web applications, network devices, and sensor systems	
9		Scalability and Performance: The platform shall support horizontal and vertical scaling to handle increasing data volumes, ensuring high performance, low latency, and fast, responsive analytics across all workloads	
10		Data Governance: The platform shall enforce data governance policies including data quality, privacy, compliance, and lineage. It shall ensure secure, auditable access, encryption, and masking of sensitive data, accessible only by authorized users.	
11		User Authentication and Security: The platform should be empowered by login screen should be CAPTCHA and OTP enabled for secure user login. Monitor privileged users, Capability to define clear roles and access management rules to User ID's	
12		Fast Computation: The platform shall support in-memory processing and be capable of handling billions of records with high efficiency, ensuring low-latency computation and rapid data processing within milliseconds	
13		Fault Tolerance: The platform shall automatically recover from failures or errors with minimal human intervention and support agentless discovery, ensuring high availability, reliability, and continuous system operations.	
14		User-Friendly Interface: The platform shall provide an intuitive and easy-to-use interface, enabling seamless navigation and customization to support diverse user roles, preferences, and operational requirements.	
15		Backup and Restoration: The platform shall support backup and restoration of metadata and user data, ensuring data protection, integrity, and quick recovery in case of system failures or data loss.	
16		Metadata Management: The platform shall provide comprehensive metadata management capabilities, including data cataloguing, scheme management, data lineage tracking, and business glossary support to improve data discovery, understanding, and governance across the smart city ecosystem	

SNo.	Parameter	Specifications	Compliance (Yes/No)
17		Data Quality Management: The platform shall include automated data quality checks, validation rules, and profiling capabilities to ensure accuracy, completeness, consistency, and reliability of data ingested from multiple smart city sources, including camera and IoT data.	
18		API and Data Access Services: The platform shall provide secure and scalable APIs for data access and sharing, enabling seamless integration with external applications, dashboards, and third-party systems while enforcing access control and governance policies.	
19		Data Lifecycle Management: The platform shall support data lifecycle management, including data retention, archival, and purging policies, ensuring efficient storage utilization and compliance with regulatory and organizational requirements.	
	Distributed Data Lake & BI Capabilities		
20		Distributed Architecture: The platform shall provide a distributed data lake architecture capable of storing and managing large volumes of data in a scalable and resilient manner.	
21		Scalability: The solution shall support horizontal scalability to handle increasing data volumes and concurrent users without performance degradation.	
22		High Availability: The platform shall ensure high availability with redundancy and failover mechanisms, ensuring uninterrupted data access even during hardware or network failures.	
23		Security and Authorization: The solution shall implement robust security mechanisms, including encryption, role-based access control, and auditing to prevent unauthorized data access.	
24		Data Partitioning and Optimization: The platform shall support intelligent data partitioning, indexing, and optimization techniques to improve query performance and efficient data retrieval.	
25		Data Replication: The solution shall support data replication across nodes or clusters to ensure data durability, fault tolerance, and high availability.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
	Business Intelligence & Dashboard Capabilities		
26		Multi-Source Data Integration: The dashboard shall support integration with multiple data sources such as databases, data lakes, and data warehouses.	
27		Customizable Dashboards: The platform shall allow users to customize dashboards, including layout, themes, visual styles, and configurations.	
28		Advanced Data Visualization: The solution shall support multiple visualization types, including charts, graphs, geospatial maps, and heatmaps for better insights	
29		Unified Monitoring Interface: The platform shall provide a single interface to monitor faults, incidents, performance, and overall IT and network infrastructure.	
30		Interactive Analytics: The dashboard shall support interactive features such as filtering, sorting, drill-down, and drill-through capabilities.	
31		Machine Learning Integration: The platform shall enable integration of ML models for predictive analytics and forecasting within dashboards.	
32		Real-Time Analytics Visualization: The solution shall support real-time data processing and visualization for continuous monitoring and analysis.	
33		Role-Based Access Control: The dashboard shall enforce access control policies to restrict data visibility and functionality based on user roles	
34		Collaboration Features: The platform shall support collaboration by allowing users to share dashboards, reports, and insights securely.	
35		Performance Monitoring Data Collection: The solution shall collect and store performance metrics across IT, network, and application layers for end-to-end monitoring.	
36		Integration with Analytics Tools: The platform shall integrate with tools such as Jupyter Notebooks, Apache Spark, and streaming platforms for advanced analytics workflows.	
37		Alerting and Notifications: The system shall provide configurable alerts and notifications based on predefined thresholds and events.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
	AI Ops & Intelligence Capabilities		
38		Kubernetes-Native Deployment: The platform shall support seamless deployment of AI/ML models on Kubernetes-based environments for scalable and containerized execution.	
39		AI/ML-Based Real-Time Analytics: The solution shall enable real-time analytics for smart city use cases such as surveillance, law enforcement, waste management, and IoT data processing.	
40		Modular Architecture: The platform shall be built on a modular architecture, allowing flexible deployment and customization of components based on business requirements.	
41		End-to-End Pipeline Management: The solution shall support design, deployment, and management of complete ML pipelines.	
42		Workflow Orchestration: The platform shall coordinate workflows across different stages of the ML lifecycle, ensuring seamless execution.	
43		Scalable Model Serving: The solution shall support scalable deployment and serving of AI/ML models across distributed environments.	
44		Model Version Control: The platform shall provide versioning capabilities for managing multiple versions of ML models.	
45		Performance Monitoring: The system shall continuously monitor model performance and key evaluation metrics.	
46		Model Metadata Management: The platform shall maintain metadata including model versions, dependencies, and configurations.	
47		Automated Data Pre-processing: The solution shall automate data preparation tasks such as cleaning, transformation, feature engineering, and handling missing values.	
48		Automated Model Selection: The platform shall automatically select appropriate models based on data characteristics and use case requirements.	
49		Model Training Framework: The system shall support model training using techniques such as	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		cross-validation, training/testing split, and holdout validation.	
50		Centralized Model Repository: The platform shall provide a centralized repository to store, manage, and retrieve trained models.	
51		Hyperparameter Tuning: The solution shall support optimization techniques such as grid search, random search, and Bayesian optimization.	
52		Evaluation Metrics: The platform shall support evaluation metrics such as accuracy, precision, recall, F1-score, and AUC-ROC.	
53		Automated Model Deployment: The solution shall enable automatic deployment of high-performing models into production environments.	
54		Model Lifecycle Management: The platform shall support continuous monitoring, retraining, and updating of models over time.	
55		60-Degree Governance: The system shall provide a unified view across multiple data sources, enabling surveillance, prediction, segmentation, and decision-making.	
56		Intelligent Predictive Maintenance: The solution shall predict equipment or system failures using machine learning-based anomaly detection.	
57		Anomaly Detection: The platform shall identify abnormal patterns in data to prevent incidents and improve operational efficiency.	
58		Behavioral Analytics: The solution shall analyze user and system behavior to detect trends and anomalies.	
59		Pattern Recognition: The platform shall identify hidden patterns in large datasets for better insights and forecasting.	
60		Event Correlation: The platform shall correlate multiple events and data sources to identify root causes of issues.	
61		Adaptive Learning: The solution shall continuously improve model accuracy by learning from new data.	
62		Automated Alert Generation: The platform shall generate alerts based on anomalies, thresholds, and predictive insights.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
63		Integration with Data Lake: The AI/ML capabilities shall be tightly integrated with the data lake to leverage centralized data for analytics and intelligence.	
	Data Protection, Disaster Recovery & Data Lake Management		
64		Data Lake Backup & Restoration: The platform shall support backup and restoration of data lake user data, including replication across clusters or data centers. It shall support incremental backups, scheduling, retention policies, and encryption.	
65		Application Backup & Restoration: The solution shall support backup and restoration of application data across RDBMS systems such as Oracle, MySQL, PostgreSQL, DB2, and MS SQL Server.	
66		Flexible Configuration & Monitoring: The platform shall allow configurable backup and replication strategies, including full, incremental, and differential backups, along with monitoring of backup status, failures, and exceptions.	
67		Disaster Recovery (DR): The solution shall support automated DC-DR synchronization across clusters or data centers with point-in-time recovery, replication scheduling, and data compression capabilities.	
68		Geo-Redundancy: The platform shall support geographically distributed data replication to ensure business continuity in case of regional failures.	
	Data Lake Management Capabilities		
69		Cluster Management: The platform shall provide a user-friendly interface for deploying, managing, and scaling data lake clusters, including node addition/removal, health monitoring, and upgrades.	
70		Configuration Management: The solution shall provide centralized configuration management for all data lake services, enabling easy configuration updates and visibility across the cluster.	
71		Service Management: The platform shall support management of big data services such as HDFS,	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		YARN, MapReduce, Hive, HBase, NiFi, Kafka, and Spark through a unified interface.	
72		Metrics Collection and Monitoring: The system shall collect and display metrics related to resource utilization, network performance, and service health, with visualization and alerting capabilities.	
73		Role-Based Access Control (RBAC): The platform shall provide fine-grained access control mechanisms to manage user roles and permissions securely.	
74		Stack Management: The solution shall support multiple open-source data platform stacks and allow customization of stack configurations based on requirements.	
75		Directory Integration: The platform shall integrate with enterprise identity systems such as LDAP and Active Directory, including Azure AD supp	
	Proactive Monitoring & Intelligence		
76		Proactive Monitoring: The platform shall continuously monitor cluster metrics such as node health, resource utilization, network activity, and job execution statistics.	
77		Time-Series Analysis: The system shall analyze historical performance data to identify trends and patterns related to system behavior and failures.	
78		Failure Detection & Root Cause Analysis (RCA): The solution shall analyze historical and real-time data to identify root causes of failures and recurring issues.	
79		Anomaly Detection: The platform shall use machine learning models to detect anomalies and deviations from normal system behavior.	
80		Fault Prediction: The solution shall provide predictive analytics to forecast potential system issues based on historical patterns and correlations.	
81		Dynamic Threshold Management: The system shall support adaptive thresholding to adjust alert thresholds based on workload patterns and environmental changes.	
82		Real-Time Alerts & Notifications: The platform shall provide real-time alerts via email or integrated	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		ticketing systems when anomalies or failures are detected.	
83		Capacity Planning & Forecasting: The solution shall provide predictive insights for storage, compute, and network capacity planning.	
84		Audit Logging & Compliance Tracking: The platform shall maintain detailed logs for all administrative and operational activities to support compliance and audits.	
85		Multi-Cluster Management: The solution shall support centralized management of multiple data lake clusters across environments.	
86		Data Integrity Validation: The platform shall ensure data consistency and integrity through validation mechanisms during backup, replication, and restoration processes.	
	Workflow Management		
87		Batch Pipeline Processing: The platform shall ingest data from multiple batch sources into storage systems such as data lakes, data warehouses, or file systems. It shall support formats including CSV, ORC, and Parquet with incremental data loading capabilities.	
88		Stream Processing Pipeline: The platform shall enable real-time data ingestion and processing from sources such as sensors, logs, and external systems using streaming platforms. It shall support filtering, transformation, aggregation, and analytics for real-time use cases.	
89		Job Scheduling and Orchestration: The platform shall include a job scheduler to execute workflows based on dependencies, priorities, and resource availability.	
90		Resource Allocation: The platform shall allocate compute resources such as CPU, memory, and storage dynamically based on job requirements.	
91		Job Monitoring and Logging: The platform shall monitor workflows and capture execution status, logs, errors, and performance metrics.	
92		Job Prioritization: The platform shall prioritize jobs based on business importance and resource requirements.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
93		Notifications and Alerts: The platform shall provide notifications and alerts for job completion, failures, and exceptions.	
94		Scalability: The workflow engine shall scale horizontally to handle large volumes of jobs and workflows across multiple clusters.	
	Data Exploration & Intelligence		
95		Data Exploration and Visualization: The platform shall provide interactive dashboards, charts, and visualization tools with filtering and drill-down capabilities.	
96		Collaborative Analytics: The platform shall enable sharing of dashboards, reports, and datasets for collaborative analysis.	
97		Intelligent Business Insights: The platform shall leverage machine learning to generate predictive and actionable insights.	
98		Use Case Enablement: The platform shall enable multiple smart city use cases through integrated analytics.	
99		Visualization Capabilities: The platform shall support visualization types including bar, pie, line, heat map, scatter, table, temporal heatmap, and advanced search.	
100		Pre-Built BI Dashboards and Widgets: The platform shall provide preconfigured dashboards and analytics widgets as out-of-the-box features.	
101		Dynamic Dashboard Filtering: The platform shall enable automatic filtering and interaction across dashboard components.	
102		System Sizing: The platform shall be sized based on available data sources and integration requirements.	
103		Data Volume Handling: The platform shall support a minimum data capacity of 50 TB with scalability for future growth.	
	Use Cases, AI/ML Analytics & BI Visualization		
104		Business Intelligence Reporting: The platform shall enable collation of data from multiple sources and	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		generation of comprehensive BI reports to support data-driven decision-making across smart city operations.	
105		KPI Dashboard and Visualization: The platform shall provide development of static and dynamic dashboards, including KPI visualization, enabling real-time monitoring and performance tracking.	
106		Predictive Analytics (AI/ML Use Cases): The platform shall leverage historical data and pattern analysis to build predictive models capable of forecasting future outcomes and identifying potential issues based on trends and correlations.	
107		360-Degree Governance View: The platform shall provide a unified 360-degree view by integrating data from multiple sources and applying advanced analytics for use cases such as law enforcement, smart surveillance, prediction, and enhanced city services.	
108		Drill-Down and Ad-Hoc Analysis: The platform shall enable users to perform drill-down analysis and ad-hoc querying for deeper insights into data trends and patterns.	
109		Real-Time Decision Support: The platform shall provide real-time insights and alerts to support proactive decision-making and incident response.	
110		Automated Reporting: The platform shall generate automated, scheduled, and on-demand reports with configurable formats and distribution mechanisms.	
70.	**Digital Twin for Kumbh Area**		
1	Digital Twin Platform & Architecture	The Digital Twin solution shall provide a real-time digital representation of the city's physical assets and surrounding environment by continuously ingesting data from connected sensors, cameras, IoT devices, and integrated city systems. The platform shall maintain synchronization between the physical and virtual models wherever such data sources exist, ensuring the twin remains current and actionable.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		The solution should be implemented on an open, modular and distributed architecture, avoiding proprietary dependencies.	
		The platform shall support both cloud and on-premises deployments (cloud-native/hybrid architecture) and shall leverage containerization and microservices to ensure scalability and flexibility.	
		The system must support horizontal scaling and load balancing, capable of handling large volumes of IoT data and concurrent users without performance degradation.	
		It shall provide high availability and redundancy (no single point of failure), with support for failover clustering to meet 24/7 operational requirements.	
		The platform shall implement robust security measures across all components, including user authentication, role-based authorization, and data encryption in transit and at rest.	
		The system shall be designed to accommodate future expansion, allowing integration of new sensor types, additional city zones, and new functional modules without significant changes to the core system.	
		The solution should adhere to relevant industry standards and best practices for system architecture and cybersecurity (ISO 27001, SOC2 Type 1 & 2) to ensure a secure and reliable operation.	
2	IoT and Sensor Data Integration	The system shall ingest real-time data from diverse IoT sensors and data sources deployed in the city, including but not limited to crowd density sensors, footfall counters, air quality monitors, noise level sensors, energy meters, traffic detectors, weather stations, and surveillance systems.	
		It should support industry-standard IoT communication protocols and data formats (such as MQTT, HTTP/REST, WebSockets, JSON, etc.) for seamless integration with various sensors and IoT gateways.	
		The platform must be capable of processing streaming data at scale, with minimal latency, so that updates in sensor readings and events are	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		reflected on the digital twin visualization in near real-time.	
		The solution shall allow bi-directional integration where appropriate, enabling the digital twin platform not only to receive data from sensors but also to send control commands or configuration updates to IoT devices (e.g., actuators, smart lighting systems) through supported protocols.	
		The system should provide connectors or adapters to integrate with existing city IoT platforms or middleware (for instance, integration via open APIs or SDKs with city data platforms, command & control systems, or enterprise service buses).	
3	3D/2D Geospatial Visualization	The platform shall offer both 2D and 3D geospatial visualization capabilities for the city digital twin, including interactive maps and high-fidelity 3D models of city infrastructure and assets.	
		Users should be able to navigate the virtual city easily (pan, zoom, rotate in 3D) and visualize various assets like roads, buildings, parks, utilities, and IoT device locations in their geospatial context.	
		The system should allow overlay of real-time data and sensor statuses on the map/model (e.g., showing live traffic conditions, crowd heatmaps, air quality index per zone, etc.), with intuitive icons or color-coding for different status or alert levels.	
		It shall support multiple map layers and thematic views (for example, a traffic layer, an environmental sensor layer, utility network layer, etc.), which can be toggled by the user for clarity.	
		The visualization module must support importing and displaying standard geospatial and 3D data formats (such as shapefiles, GeoJSON, KML for maps; CityGML, IFC or glTF for 3D city models), ensuring interoperability with existing city data sources.	
		The platform should provide the ability to drill down from city-wide view to specific facilities or buildings (and even floor-level details if available), seamlessly transitioning between different levels of detail in the digital twin.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
4	Simulation & Predictive Analytics	The Digital Twin solution shall include simulation tools to model and analyze hypothetical scenarios in the urban environment (e.g., simulating traffic rerouting, new infrastructure development, emergency evacuations, or public event crowd management) before those changes are implemented in the real world.	
		The system should leverage historical and real-time data along with AI/ML algorithms to perform predictive analytics, forecasting future trends such as traffic congestion, public transport ridership, energy consumption, or environmental quality under various conditions.	
		Users shall be able to run "what-if" analyses by adjusting input parameters (such as the timing of traffic signals, availability of transit routes, or occupancy limits of a public venue) and the platform will project the outcomes on key metrics and city KPIs.	
		The platform shall support predictive maintenance use cases by analyzing data from sensors, cameras, public address (PA) systems, and emergency call boxes (SOS), as well as other connected assets such as water pumps, power grids, and transit vehicles. The system shall leverage AI/ML models to predict potential failures or maintenance needs and proactively alert operators in advance.	
		Simulation and analytics results should be presented within the platform via visual dashboards or reports, and the system should allow exporting these results for further analysis or presentation.	
5	Interoperability (GIS, BIM, SCADA & Legacy Systems)	The solution shall integrate with Geographic Information System (GIS) platforms to import, overlay, and export geospatial data. It should support standard GIS services and formats (WMS/WMTS for map tiles, WFS for features) allowing use of existing city maps and spatial datasets in the digital twin.	
		The platform shall support integration of Building Information Modeling (BIM) data for incorporating detailed 3D models of buildings and infrastructure. It should accept standard BIM files (e.g., IFC format)	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		and convert them into the digital twin environment for visualization and analysis.	
		The system should provide interfaces to SCADA systems and other industrial control or operational systems used by city utilities (power, water, transportation). This includes support for relevant protocols or APIs (for example, OPC UA for industrial data, or API connectors to specific SCADA software) to ingest real-time operational data into the twin.	
		The digital twin platform must allow integration with legacy databases and applications used by various city departments. For instance, it should be able to consume data from CSV/Excel files, SQL databases, or existing city management systems to ensure all relevant data can be unified in the twin.	
		Emphasis is on open standards and data exchange: the solution should avoid proprietary data lock-in, and instead utilize widely-adopted data standards and ontologies for smart city data, facilitating easier integration and future interoperability.	
6	Role-Based User Interface & Dashboards	The system shall provide a comprehensive, intuitive dashboard interface for monitoring the city's digital twin, accessible through standard web browsers (and optionally via a mobile application for remote access).	
		It should support multiple user roles (e.g., administrator, operator, city planner, emergency responder), with role-based access control to ensure each user sees and interacts with data relevant to their authority and needs.	
		Users should be able to customize their dashboard view by selecting relevant data widgets, maps, 3D views, charts, and KPIs to display. The interface should support configuration of these elements without requiring developer intervention.	
		The solution's UI/UX must support real-time updates (e.g., live dashboards that update automatically as new data comes in, without manual refresh) to allow operators to respond quickly to changing conditions.	
		The application should support multi-language user interface options (at minimum English, and	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		optionally local languages as required), so that it can be used by officials in their preferred language.	
		For mobility and ease of access, the platform should provide either a responsive web design or dedicated mobile app that allows authorized users to view alerts and key data from the digital twin on tablets or smartphones.	
7	API and Integration Capabilities	The digital twin platform shall expose a robust set of APIs for external integration, enabling third-party systems and developers to interact with the platform's data and functionalities. These should include RESTful APIs (HTTPS/JSON) for querying data and sending commands into the system.	
		APIs should allow retrieval of both real-time status and historical data from the digital twin, including the ability to query sensor values, asset status, alerts, and simulation results.	
		Webhook or publish/subscribe mechanisms (such as MQTT topics or WebSocket streams) should be available for pushing real-time events and updates from the digital twin to subscribing systems, ensuring external applications can get instantaneous updates.	
		The platform's APIs must be well-documented and secured (with authentication tokens, API keys or OAuth 2.0 mechanisms, and role-based permission checks for each endpoint). All data exchange should enforce encryption (TLS) to protect data in transit.	
		The system should utilize open data schemas and standards in its API payloads and data storage, wherever applicable (for example, using GeoJSON for spatial data, adhering to IoT data models like oneM2M or FIWARE NGSI-LD for context data), to maximize compatibility with external tools and adherence to smart city standards.	
8	Scalability & Performance	The solution architecture shall be capable of scaling to city-wide deployments, handling thousands of sensor inputs and events per second, and supporting a large number of simultaneous users monitoring the system.	
		The system should support horizontal scalability (adding more servers/instances to handle increased	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		load) without significant downtime or reconfiguration, ideally using cloud-native scaling features if deployed on cloud infrastructure.	
		Performance should be optimized so that typical user interactions (loading dashboards, running a simulation, retrieving data) occur with minimal latency. The UI should load within a few seconds even as data volume grows, and real-time data points should reflect on the dashboard with a delay of no more than a few seconds from live generation.	
		The platform must support high-volume data storage and efficient retrieval (using big data technologies or time-series databases) to ensure historical data queries and analytics do not hinder real-time performance.	
		It should also be resilient under heavy load or network issues, ensuring graceful degradation (the system remains operational at reduced capacity rather than failing outright in extreme conditions).	
9	Data Management & Normalization	The platform shall be able to ingest data from heterogeneous sources and normalize it into a unified data model, so that data from various sensors and systems can be compared and analyzed coherently even if they originate in different formats or units.	
		All incoming data should be tagged with time stamps, source identifiers, and geo-location (if applicable) and stored in a centralized data repository, forming a coherent spatio-temporal database of the city's operational data.	
		The system shall support long-term data storage and trend analysis with efficient indexing and querying capabilities. The platform shall retain at least one (1) year of data in the live database for immediate access, while archiving an additional four (4) years of historical data in the archive database. The system shall provide configurable options to archive, retrieve, or purge data in line with organizational data management policies.	
		Data integrity and quality must be maintained through validation rules and filtering of anomalous or corrupt data. The system should log data	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		ingestion status and provide diagnostics for any data source that falls out of expected ranges or becomes unavailable.	
		The data model of the digital twin should be extensible, allowing new types of data or assets to be added (with their attributes and relationships) without refactoring the entire system. This ensures that as city needs evolve, the digital twin's data schema can adapt accordingly.	
10	Alerts and KPI Monitoring	The digital twin solution shall provide a configurable alerting mechanism that monitors incoming data and system events against predefined thresholds or conditions. When conditions are met (e.g., air quality index exceeding a safe limit, crowd density above threshold, device failure detected), the system should automatically generate an alert in real-time.	
		Users should be able to define and customize alert rules (including compound conditions combining multiple data points) through the interface, without requiring programming. Each alert type should allow configuration of severity level, responsible personnel or group, and the notification method.	
		The system shall support multiple notification channels for alerts, such as on-screen popups in the command center dashboard, email and SMS notifications, and push notifications on the mobile app, ensuring timely awareness of critical events.	
		The platform should include a KPI management dashboard where key performance indicators related to city operations (e.g., average response time to incidents, daily energy consumption, percentage of green cover, etc.) can be defined, calculated from the underlying data, and visualized.	
		Users (with appropriate permissions) should be able to configure which KPIs are tracked and how they are calculated (selecting data sources and formulas) and set target values or thresholds for each KPI. The system should visually indicate the status of each KPI against its target (e.g., using color codes or trend arrows).	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		The solution should provide reporting capabilities, enabling extraction of periodic reports on alerts (e.g., weekly summary of all alerts, with response times) and KPI trends (e.g., monthly performance reports), to support management reviews and compliance reporting.	
11	Natural Language Processing Support	The platform shall provide a conversational AI capability that enables users to query system information, alerts, and key performance indicators (KPIs) using natural language input. The conversational interface shall interpret user intent, retrieve relevant real-time or historical data from the platform, and return accurate, contextual responses without requiring users to navigate dashboards or perform manual searches. The feature shall support authorized access, respect user roles and permissions, and operate across all configured modules within the solution (e.g., operations, service performance, queue analytics, asset status, or other platform KPIs).	
12	Vulnerability Testing	The system shall be certified on 'VAPT' (Vulnerability Assessment and Penetration Testing).	
13		The GIS software must also support Photogrammetry for drone, aerial and high-resolution satellite images.	
14		It must support generating DEM, True-Ortho, 3D Mesh model and 3D Gaussian Splats automatically	
15		It must read the images from World View 3 and 4, Legion and other Maxar imagery directly from the folders for Reality mapping. It must also support images from other satellite makes such as Airbus, Planet, BlackSky, Kompsat, etc..	
16		It must support processing of drone/ aerial imageries from single as well as multi-headed oblique sensors to generate accurate True-Orthos and photorealistic 3D Mesh models.	
17		It must have the facility to generate Tie points automatically and edit tie points manually.	
18		It must generate a detailed processing report to validate input parameters, accuracy statement, etc..	
19		It must generate True-Ortho in TIFF format and Mesh models in SLPK, OBJ and 3D Tiles format.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
20		It must have all the photogrammetric functionalities within the same GIS application with the same GUI as the GIS desktop application.	
21		It must also have the toolsets to exctract 3D vector features from the reality mapping outputs within the same GIS application.	
22		The software must support publishing the outputs such as True-Ortho and Mesh models as tile, image and scene layers directly to the Enterprise GIS. proposed.	
23		The software should provide a digital representation (digital twin) of the city, where all urban developments are visualized in one place.	
24		It should allow users to visualize citywide plans and projects in a unified interface.	
25		The platform should support uploading and managing 3D models as part of a centralized 3D system of record.	
26		It should allow integration of images (e.g., blueprints) into projects.	
27		The software should support rich 3D scene editing, including adding and enhancing buildings and environments.	
28		The software should allow users to import and configure data within the urban model.	
29		It should support integration with BIM tools (e.g., Revit, IFC formats) for detailed building planning.	
30		The platform should maintain a centralized repository for models, plans, and project data.	
31		The platform should allow stakeholders to collaborate on shared citywide plans and projects.	
32		It should support open discussions and scenario evaluations within user groups.	
33		The software should provide tools to gather feedback from stakeholders and the public on shared plans.	
34		Software should support importing and exporting multiple 3D and CAD formats including OBJ, FBX, DAE, DXF, DWG, IFC, KML, and KMZ.	
35		Software should support exporting models with textures organized into reusable folders for easy sharing across platforms.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
36		Software should support exporting scenes and models to formats such as images, web scenes, and 360°/VR-ready outputs.	
37		Software should allow customization of export processes, including adding metadata and instancing information using Python scripts.	
38		Software should support exporting models to game engines such as Unity and Unreal Engine for immersive visualization.	
39		Software should support real-time 3D visualization of urban environments for design evaluation and presentation.	
40		Software should support rapid generation of urban design scenarios using procedural rules and GIS data.	
41		Software should support handling and visualization of large-scale city models efficiently.	
42		Software should support basic visual analysis within the 3D environment using rule-based logic.	
71.	**Mobile App for Pilgrims / Visitors**	**This is to be provided complimentary**	
	Engagement Application		
1		The application shall accept requests or inquiries from the citizens and track those requests from different channels of Web Portal, Smart Phone Application (City App) & social media (Facebook, Twitter.)	
2		Solution should support in handling all service requests through portal and Mobile App for efficiently managing the citizen grievance request	
3		The operator should be able to chat/reply to any queries raised through mentioned channels via the same channel, including pilgrim assistance and emergency guidance.	
4		The application shall allow the user to select service request category type or use auto-filled profile and GPS location information for incident creation. A unique service transaction number should be assigned for each incident after a service request is created.	
5		The application shall capture different types of input data, including but not limited to: date,	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		Citizen/pilgrim contact detail issue type, issue description, time of day the grievance occurred,exact pilgrimage location (ghat/sector/camp/route), etc.	
6		The platform shall provide GIS-based visualization of service requests over a city base map integrated with large-gathering operational layers (such as Kumbh sectors), including ghats, camps, routes, medical facilities, police posts, and public amenities, with the capability to display service request details and related operational information directly on the map.	
7		The application should provide information regarding the exact geo-location of the service request to enable faster field response during dense pilgrim gatherings.	
8		The application must have the ability to display the citizen's or pilgrim's previous interactions from different channels and view previous service request status.	
9		The application should have the ability to display "top" grievance types based on historical trends ranked according to the most viewed and most relevant service request.	
10		The application should have the ability to view and attach files such as images,videos and voice recordings from pilgrims, PDFs, and other supporting document	
11		The application should prevent a request from being closed until all associated actions are completed, ensuring accountability for critical pilgrim safety and service incidents	
12		The application should have the ability to dispatch a service request to the workforce, department, external agency, or Kumbh field response team through ICCC integration.	
13		The application should provide a set of standard reports that will provide statistical reporting for open, closed, escalated, priority, completion time, based on address/ghats and location.	
14		The dashboard module should provide a quick and easy view of overall grievance details including	

SNo.	Parameter	Specifications	Compliance (Yes/No)
		pilgrim incident trends, crowd-day spikes, departmental response efficiency, and feedback analytics integrated with ICCC.	
15		The application should allow the administrator to define SLAs for all the incidents.	
16		The application should allow the administrator to add, edit, and delete various departments, including temporary large operational units and volunteer agencies.	
	Mobile App		
17		The Citizen/City App shall integrate citizen and pilgrim service requests and provide location-based, real-time notifications related to city services, major public events and gatherings including Kumbh, traffic and route diversions, bathing-day schedules, safety advisories, and other critical alerts based on the ward, sector, or selected user location.	
18		Key Features of the app should include: • Incident Reporting(including lost person, crowd congestion, medical emergency, sanitation, water, electricity, safety) • Complaints Tracking • e-Governance Services • Bills Payment • News • Events-spiritual/Kumbh event information • Notifications & crowd/traffic advisories • All Announcements • • Emergency & one-tap SOS to nearest police/medical camp with GPS	
19		Citizen app shall allow pilgrims to report incidents across various grievances such as lost person/missing companion, crowd congestion, medical emergency, sanitation or toilet issues, drinking water shortage, waste accumulation, electricity outage, fire incident, stampede risk, suspicious activity, traffic or route blockage, accommodation/camp issues, and other safety-related concerns, integrated with ICCC for automated emergency response and field dispatch.	
20		City App should allow to make SOS calls from Click to call feature.	

SNo.	Parameter	Specifications	Compliance (Yes/No)
21		City App should allow citizens to pay utility bills and taxes	
	Web Portal		
22		It should provide a single view to the citizen and visiting pilgrims for engaging with the city departments.	
23		It should provide live update of the City Service and Kumbh operational advisories also act as a foundation for Citizen to register the identity and download the Citizen App.	
24		Portal should allow citizen to use different City services by selecting services categories	
25		The Web portal should provide the citizen the facility to report Civic grievances by selecting grievance categories and subcategories by attaching Image or Video and geo-tagging to support the Grievance request	
		The citizen can view the history and status of all the complaints that have been requested.	
26		The Citizen should be able to see the GIS view of the city and can find POIs such as ghats,temples, camps, toilets, medical centers, police, parking, transport routes,nearby attractions and help desks as when required.	
27		The web portal should have Content Management System to create content and publish content and it will integrate with all public Channels for News and other feeds	
28		The web portal should have CMS that shall provide a role- based user access mechanism where an administrator can create and manage users, user groups, roles, and role permissions.	
29		The CMS should support login module using which content authors will be able to login.	
30		Login module should have forgot password mechanism. In case user forgets the password/wish to reset a link should be sent to user's registered Email address from where password can be reset.	
31		CMS should support integration with Directory Services (supporting LDAP) to manage users and their preferences. CMS should also support latest security certificates like SSL 3.0	

SNo.	Parameter	Specifications	Compliance (Yes/No)
32		CMS should be able to publish content to any external portal apart from its native portal by Integrating with the required platform.	
33		CMS shall support the creation, modification, and deletion of templates to enable easy management of site and page layout and navigation	
34		a) Preview only on CMS (not visible to users) b) Save as unpublished (draft) c) Preview on Portal d) Send for approval e) Approve f) Publish after approval (i.e., after successful completion of the approval workflow) g) Unpublish (save as unpublished, not visible to users) h) Publication scheduling i) Publication expiration date (automatic unpublish)	
35		CMS shall contain a content approval workflow to enable the approval of modifications (create, modify, delete) before publication (i.e., before becoming visible to the public)	
36		CMS shall support Administrator (or a designated user with an appropriate permission level) to assign and reassign users to workflow tasks (i.e., define the targets within the workflow)	
37		CMS shall support the creation and application of styles using Cascading Style Sheets (CSS) enabling the swift alteration of the look and feel (colour, font, image size and positioning, link attributes, table properties). Graphics should be avoided altogether regarding navigation (e.g., no navigation buttons -	
38		these should be text, which gets its look and feel through CSS).	
39		The CMS should have the capability to create and deploy content on different portals with same or different branding through integrating with the other portals	
40		The CMS shall support multilingual (English & Hindi) capabilities.	