Odisha Computer Application Centre

RFP for Selection of Implementation Agency for Integrated City Surveillance System at Puri, Odisha for Home Department, Government of Odisha

RFP Reference No.: OCAC-SEGP-INFRA-0023-2025-26009
Date: 31/01/2026

PART-2

ODISHA COMPUTER APPLICATION CENTER
[Technical Directorate of E & IT Department, Government of Odisha]
N-1/7-D, Acharya Vihar, P.O. – RRL, Bhubaneshwar-751013
EPBX: 674-2567280/2567064/2567295/2567283
Fax: +91-674-2567842
E-mail ID- contact@ocac.in, Website: www.ocac.in

Table of Contents

Disclaimer

The information contained in this Request for Proposal document ("**RFP**") whether subsequently provided to the Bidders, ("**Bidder/s**") verbally or in documentary form by Odisha Computer Application Center (henceforth referred to as "**OCAC**" in this document) or any of its employees or advisors, is provided to Bidders on the terms and conditions set out in this Tender document and any other terms and conditions subject to which such information is provided.

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

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

Authority and their employees and advisors make no representation or warranty and shall incur no liability to any person, including the Bidder under law, statute, rules or regulations or tort, the principles of restitution or unjust enrichment or otherwise for any loss, cost, expense or damage which may arise from or be incurred or suffered on account of anything contained in this RFP or otherwise, including the accuracy, reliability or completeness of the RFP, and any assessment, assumption, statement or information contained therein or deemed to form part of this RFP or arising in any way in this Selection Process. Authority also accepts no liability of any nature whether resulting from negligence or otherwise howsoever caused arising from reliance of any Bidder upon the statements contained in this RFP. Authority may in its absolute discretion, but without being under any obligation to do so, can amend or supplement the information in this RFP.

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

The Bidder shall bear all its costs associated with or relating to the preparation and submission of its Bid including but not limited to preparation, copying, postage, delivery fees, expenses associated with any Proof of Concept (PoC), demonstrations or presentations which may be required by Authority, or any other costs incurred in connection with or relating to its Bid. All such costs and expenses will remain with the Bidder and authority shall not be liable in any manner whatsoever for the same or for any other costs or other expenses incurred by a Bidder in preparation for submission of the Bid, regardless of the conduct or outcome of the Selection process.

Glossary

Terms	Meaning
ANPR	Automatic Number Plate Recognition
AP	Access Point
ATCS	Adaptive Traffic Control System
BOM	Bill of Material
CCTV	Closed Circuit Television
CCC	Command and Control Center
CSP	Cloud Service Provider
DBA	Database Administrator
DC	Data Center
DR	Disaster Recovery
DRC	Disaster Recovery Center
EMS	Enterprise Management System
FRS	Functional Requirement Specifications
GUI	Graphical User Interface
IaaS	Infrastructure as a Service
ICCC	Integrated Command and Control Center
ICT	Information and Communication Technology
IoT	Internet of Things
IP	Internet Protocol
IT	Information Technology
KPI	Key Performance Indicator

Terms	Meaning
Meity	Ministry of Electronics & Information Technology
MoHUA	Ministry of Housing & Urban Affairs
MPLS	Multi-Protocol Label Switching
IA	Implementation Agency
IPSEC	IP Security
MTTR	Mean Time to Repair
ONVIF	Open Network Video Interface Forum
O&M	Operation and Maintenance
OEM	Original Equipment Manufacturer
OFC	Optical Fiber Cable
OS	Operating System
PaaS	Platform as a Service
PDU	Power Distribution Unit
PoP	Point of Presence
PTZ	Pan Tilt Zoom
RF	Radio Frequency
RFP	Request for Proposal
REST	Representational State Transfer
RoW	Right of Way
RTO	Recovery Time Objective
RPO	Recovery Point Objective
SaaS	Software as a Service
SDK	Software Development Kit
SLA	Service Level Agreement

Terms	Meaning
SMPS	Switched Mode Power Supply
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SOP	Standard Operating Procedure
SRS	System Requirement Study
TPA	Third Party Auditor
TRAI	Telecom Regulatory Authority of India
TRS	Technical Requirement Specifications
UAT	User Acceptance Testing
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator
VA	Video Analytics
VM	Virtual Machine
VMD	Variable Message Display
VCA	Video Content Analysis
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network
VMS	Video Management Software/System
WAN	Wide Area Network
CONOPS	Concept of Operations

1. Introduction

The Government of Odisha, through the **Home Department** and **Odisha Computer Application Centre (OCAC)**, intends to implement an **Integrated City Surveillance System (ICSS)** for the city of **Puri**. Puri is one of India's most significant pilgrimage destinations, attracting millions of devotees throughout the year, with extraordinary footfall during **Shri Jagannath Rath Yatra**, **Snana Purnima**, **New Year**, and other major festivals.

To enhance situational awareness, crowd safety, traffic management, law enforcement support, and coordinated emergency response, a holistic and integrated surveillance ecosystem is required. This system must cater to both **routine city operations** and **surge-event scenarios** such as Rath Yatra, where crowd density, vehicular movement, and public safety risk dramatically increase.

The proposed ICSS shall act as a **central enabler** to support all key stakeholders—**Puri Police**, **District Administration**, **Puri Municipality**, **SJTA**, **OBCC**, **Fire Services**, **Health & Disaster Management**, and other field agencies—through reliable situational intelligence, analytics-driven alerts, and seamless coordination.

This Volume describes the **functional requirements, system architecture, technical specifications, operational workflows, integration needs, and service expectations** for the Implementation Agency (IA). The solution is expected to be robust, scalable, event-ready, and designed to support the unique cultural, religious, and geographic characteristics of Puri.

1.1 Project Background

Puri hosts multiple high-density events annually, with the **Rath Yatra** being one of the largest religious gatherings in the world. Existing surveillance infrastructure deployed during previous events is limited, temporary, and lacks unified monitoring and analytics capabilities.
To overcome these challenges, the Home Department propose establishing a **permanent, event-ready surveillance system** equipped with:

- High-definition CCTV coverage across critical zones
- AI-based analytics (crowd density, FRS, ANPR, loitering, abandoned objects, etc.)
- A centrally managed **Integrated Command & Control Centre (ICCC)** at Puri
- Temporary/portable deployments for surge scenarios (festival periods, VIP movements)
- Integration with existing ITMS, SJTA systems, emergency response, and law enforcement platforms

This project aims to ensure **public safety, better governance, faster response times**, and data-driven decision-making, while supporting efficient crowd and traffic management during Puri's major events.

1.2 Objectives of the Project

The key objectives of the Puri ICSS are:

- Enhance citizen safety through real-time monitoring and automated incident detection.
- Support crowd management, especially during Rath Yatra and large processions.

- Improve traffic management using ANPR, vehicle counting, and route-based monitoring.
- Provide unified situational awareness to all stakeholder departments.
- Strengthen emergency response through integrated communication, alerts, and visual feeds.
- Create a scalable surveillance platform that can accommodate future expansion and new use cases.
- Ensure a resilient system architecture with cloud-based DR, redundancy, and cybersecurity compliance.
- Enable 24×7 operations with effective O&M, SLAs, and manpower support.

Volume II outlines:

- Functional requirements
- Detailed scope of work
- Use cases and analytics requirements
- System architecture
- Application, platform, and hardware specifications
- Integration requirements with other systems
- Implementation methodology
- Operation & Maintenance requirements (5-years)

This Volume will serve as a reference for the **technical proposal** and will be used for **solution evaluation**, **PoC assessment**, and **commercial bid alignment**.

1.3 Stakeholder Departments

The ICSS shall support and interoperate with the following departments:

- Home Department, Government of Odisha
- Puri Police
- District Administration, Puri
- Odisha Computer Application Centre (OCAC)
- Shree Jagannath Temple Administration (SJTA)
- Odisha Bridge & Construction Corporation (OBCC)
- Puri Municipality
- NHAI & Works Department
- Fire & Disaster Response
- Health Department

The stakeholder departments listed above are tentative and are added to let bidders understand the scope and coverage of this project.

1.4 Expected Outcomes

- Improved crowd safety during Rath Yatra and other major events.
- Reduced incidents and faster emergency responses
- Enhanced coordination among agencies through a unified ICCC

- Real-time and predictive analytics for proactive decision-making
- Compliance with national security and data protection standards
- Improved tourism and visitor experience through safe mobility

2. Scope of Work & Payment Schedule

The Selected Implementation Agency (IA) shall be responsible for the **design, supply, installation, commissioning, integration, testing, operations, and maintenance** of the **Integrated City Surveillance System (ICSS)** for the city of **Puri, Odisha**, including support for major annual events such as **Shri Jagannath Rath Yatra**, **Snana Purnima**, **New Year**, and other surge occasions along with city surveillance throughout the year.

This section outlines the detailed Scope of Work (SoW) and the associated Payment Schedule for the IA.

2.1 Overview of Scope of Services

The IA scope of work shall include but not limited to the following broad areas. Details of each of these broad areas have also been outlined in respective Section of the RFP.

- Team Mobilization and Project Inception.
- Assessment, Scoping and Survey Study: Conduct a detailed assessment, scoping study and develop a comprehensive project plan, including:
  - Conduct site survey for finalization of detailed technical architecture, gap analysis and project plan.
  - Conduct site surveys to identify need for site preparation activities.
  - Obtain site Clearance obligations & other relevant permissions.
- Design, Supply, Installation, Commissioning and Testing which includes the following components:

  a. Integrated Command and Control Center
  b. City Surveillance System
  c. Video Summarization System
  d. Automatic Number Plate Recognition System (ANPR)
  e. Red Light Violation Detection System
  f. Parking Surveillance
  g. Speed Violation Detection System
  h. Variable Message Display
  i. Public Address System
  j. City Communication Network
  k. City Systems / Applications
  l. Data Center & Disaster Recovery Center

- Establishment of network based on Lease line/MPLS connectivity and Internet connectivity for operations in Puri.
- Provisioning of Hardware and Software Infrastructure which includes design, supply, installation, and commissioning of IT and Non-IT Infrastructure at On-premises Data Center (DC), Cloud Hosted Disaster Recovery Center (DRC) This consist of:

m. Basic Site preparation services.
n. IT Infrastructure including server, storage, other required hardware, application portfolio services.
o. Integrating Command and Control Center including operator workstations etc.
p. Establishment of LAN and WAN connectivity at command centers and DC limited to scope of infrastructure procured for the project.
q. Network Switches, Routers etc.
r. UPS for the systems/components under the scope of this RFP.

1. Integration of the envisaged ICT systems with existing Integrated Command & Control Center (ICCC) Project:
    a. Integrated Command and Control Center.
    b. City Surveillance System.
    c. Video Summarization System
    d. Automatic Number Plate Recognition System (ANPR)
    e. Red Light Violation Detection System
    f. Parking Surveillance
    g. Speed Violation Detection System
    h. Variable Message Display
    i. Public Address System
    j. City Communication Network
    k. City Systems / Applications
    l. Data Center & Disaster Recovery Center
2. Capacity Building for Authority, Police Department and other end user departments which includes preparation of operational manuals, training documents and capacity building support, including:
    a. Training of the authorities, police personnel, field staff and operators on operationalization of the system.
    b. Support during execution of acceptance testing.
    c. Preparation and implementation of the information security policy, including policies on backup and redundancy plan.
    d. Developing manual/automatic (as applicable) standard operating procedures for operations management and other services to be rendered by Integrated City Surveillance.
    e. Preparation of KPIs for performance monitoring of various utilities monitored through the system envisaged to be implemented as per the project requirements.
3. Preparation of system documents, user manuals, performance manuals, Operation manuals etc.
4. Operations and Maintenance services for the software, hardware and other IT and Non-IT infrastructure installed as part of the project after Go-Live for a period of 5 years from the date of Go-Live.

2.2 Overview

The Implementation Agency (IA) shall deploy the team based out of Puri proposed for the project upon signing of agreement and ensure that the Project Inception Report is submitted to Authority within 15 days of signing of the agreement, covering following aspects:

- Names of the Project Team members, their roles, and responsibilities
- Approach and methodology to be adopted to implement the Project (which should be in line with what has been proposed during the bidding stage but may have value additions/ learning in the interest of the project).
- Responsibility matrix for all stakeholders
- Risks the IA anticipates and the plans they have towards their mitigation
- Detailed project plan specifying dependencies between various project activities/sub- activities and their timelines.
- Installation locations geo mapped preferably on google earth to visually identify the geographical area.

The IA shall conduct a comprehensive As-Is study of as existing infrastructure, systems, and associated processes in the city in line with project requirement. The IA shall study the existing business processes, functionalities, existing ICT systems and applications.

Additionally, the IA should provide detailed TO-BE designs specifying the following, at the minimum:

- High Level Design (for all components installed) for Application architecture, Logical and physical database design, Data dictionary and data definitions, ER diagrams and other data modelling documents and Physical infrastructure design for devices on the field.
- Application component design including component deployment views, control flows, etc.
- Low Level Design (including but not limited to) for all components installed Application flows and logic including pseudo code, GUI design (screen design, navigation, etc.), Database architecture, including defining data structure, data dictionary as per standards laid down by Government of India/ Government of (State).
- Location of all field systems and components proposed at the junctions, (KML /KMZ file plotted on GIS platform like google earth etc.)
- Height and foundation of Cameras and Standard Height and foundation of Poles, cantilevers, gantry, and other mounting structures for other field devices.
- KPI design to visualize important events on real time basis.
- Location of Junction Box.
- Location of Network Provider's Point of Presence (PoP).
- Design of Cables, Ducts routing, digging and trenching.
- Electrical power provisioning.

2.2.1 Key activities under the scope of the IA:

- CONOPS design finalization and sign off with Authority.
- Project Planning, Procurement, and execution.
- AS-IS and TO-BE Assessment, Survey and Gap analysis for components under the scope.
- Development of use cases and Standard operating procedures (SoPs)
- Site Preparation including required civil work and site clearances.
- Solution design, development, implementation, customization, testing of entire system.
- Deployment of use cases.

- Training- general awareness, Use cases, SoP management, governance, CCC operations, System maintenance.
- Business Process Reengineering and KPIs for the selected applications/ services
- STQC Certification and system audit (STQC certification to be provided cameras OEM and system VAPT audit to be done by Cert-in empanelled agency)
- UAT & Go-live
- Capacity Building
- Operation & Maintenance (O&M) for 05 Years from phase-wise Go-live date
- Security audit and compliance

2.2.2 The bidder shall be responsible for carrying out detailed survey prior to submission of the bids to finalize with infrastructure requirement, electrical power, network bandwidth requirement, operational & administrative challenges etc.

2.2.3 The bidder shall furnish the survey report along with their realistic assessment of AS-IS situation and assumptions (if any) for the desired output, as part of their technical bid.

2.2.4 Field equipment installed through this Project would become an important public asset. During the agreement period, the IA shall be required to repair / replace any equipment if damaged / faulty.

2.2.5 Convergence: Authority has already initiated many projects, which have state of the art infrastructure at field locations deployed under them. The infrastructure should be made scalable for future convergence needs. The Authority has envisaged to create a state-of-the-art infrastructure and services for the citizens of Puri City.

Hence it is imperative that all infrastructure created under the project shall be leveraged for maximum utilization. Therefore, the bidder is required to ensure that such infrastructure shall allow for accommodation of equipment that is being procured under other city projects. The equipment like junction boxes and poles deployed under the Integrated City Surveillance System in Puri City project at the field locations shall be utilized to accommodate field equipment created under the other projects of Authority. The procedure for utilization of the infrastructure shall be mutually agreed between the Authority and IA.

The IA shall note that the activities defined within scope of work mentioned are indicative and may not be exhaustive depending on the respective city specific requirement later provided by them.

IA is expected to perform independent analysis of any additional work that may be required to be carried out to fulfil the requirements as mentioned in the RFP and factor the same in their techno-commercial bid response.

2.3 Responsibility Matrix

R/A=Responsible/Accountable
C= Consulted
I = Informed

#	Key Activities	Implementation Agency (IA)	SGTA /Municipal Corporation	Home Department	Other Stakeholder Departments	Project Management Consultants (PMC)	Existing ICT Vendors of Authority
1	Project Kick Off	R/A	C	C	I	C	I
2	Deployment of manpower	R/A	C	C	I	C	I
3	Assess the requirement of IT and Non-IT Infrastructure	R/A	C	C	C	C	C
4	Involving and facilitating with departments for business process assessment	I	-	R	A	R	-
5	Providing As-Is information	-	R/A	R/A	-	-	R/A
6	Assessment of Business processes	R/A	C	C	C	C	I
6	Acceptance of changes and ownership of business process post assessment	I	-	R	A	R	-
8	Assessment of Software/ Application requirements	R/A	C	C	C	C	I
9	Assess the Integration requirement	R/A	C	C	C	C	C
10	Assess the connectivity requirement all locations (Field level+ CCC/DC/Viewing Centers/DR site)	R/A	C	C	C	C	I
11	Providing relevant data sets for identified use cases	-	-	R	A	C	C
12	Assessment of available city data sets	R/A	C	R	I	C	I
13	Preparation and finalization of use cases	R/A	R	R	R	C	I

#	Key Activities	Implementation Agency (IA)	SGTA /Municipal Corporation	Home Department	Other Stakeholder Departments	Project Management Consultants (PMC)	Existing ICT Vendors of Authority
14	Assessment of training requirement	C	C	R	A	C	I
15	Develop the Concept of Operations (CONOPS)	R/A	C	R	R	C	I
16	Formulation of Solution Architecture	R/A	C	C	C	C	I
17	Preparation of Detailed Drawing	R/A	C	C	C	C	I
19	Development of test cases (Unit, System Integration and User Acceptance)	R/A	C	R	R	R	R
20	Preparation of bill of materials	R/A	C	C	C	C	I
21	Approval of material for procurement	C	-	R/A	-	C	-
22	SoP preparation	R	C	A	A	C	I
23	Material Procurement including software licenses	R/A	C	C	I	C	I
24	Physical Infrastructure setup	R/A	C	C	I	C	I
25	IT and Non-IT Infrastructure Installation	R/A	C	C	I	C	I
26	Development, Testing and Production environment setup	R/A	C	C	I	C	I
27	Software Application customization (if any)	R/A	C	C	I	C	I
28	Development of Bespoke Solution (if any)	R/A	C	C	I	C	I
29	Implementation, testing of Solutions and urban services	R/A	C	C	I	C	I

#	Key Activities	Implementation Agency (IA)	SGTA /Municipal Corporation	Home Department	Other Stakeholder Departments	Project Management Consultants (PMC)	Existing ICT Vendors of Authority
30	Integration of GIS and other sub-systems in existing ICCC	R/A	C	C	C	C	I
31	Providing data for migration in the specified format	C	-	R	A	C	C
32	Data Migration	R/A	C	C	I	C	I
33	Training contents preparation	R/A	-	C	-	C	-
34	Integration with city level/Third party services/application (if any)	R/A	C	C	I	C	R/A
35	SoP and KPI implementation	R/A	C	C	C	C	R/A
36	User Acceptance Testing	R/A	C	C	I	C	I
37	Helpdesk setup	R/A	C	C	I	C	I
38	Preparation of manual/ documents for system installation, system operation, User guide, SoPs	R/A	C	C	I	C	R/A
39	Role based training(s) on the Smart Solutions	R/A	C	C	I	C	I
40	Go Live	R	C	R/A	I	C	I
41	Operation and Maintenance of IT, Non-IT infrastructure and Applications	R/A	C	C	I	C	I
42	SLA and Performance Monitoring	R/A	C	R	R	C	I
43	Logging, tracking and resolution of issues.	R/A	C	C	I	C	I

#	Key Activities	Implementation Agency (IA)	SGTA /Municipal Corporation	Home Department	Other Stakeholder Departments	Project Management Consultants (PMC)	Existing ICT Vendors of Authority
45	Application enhancement	R/A	C	C	I	C	I
46	Patch & Version Updates/upgrades	R/A	C	C	I	C	I
47	Future Integration with other services/infrastructure	R/A	C	C	I	C	I
48	Business process re-engineering	R/A	C	C	C	C	I
49	Use-cases enhancements	R/A	C	C	C	C	I

Note:
1. Authority may modify the above matrix as per project requirements, which shall be adhered to, by all the stakeholders as mentioned above.

The IA shall ensure that all identified and approved use-cases are implemented along with Standard Operating Procedures (SoPs) to measure city performance against key outcomes that they bring to various city stakeholders.

An indicative list of use cases is mentioned in subsequent sections of this RFP**.** These use cases shall be key acceptance criteria during UAT. For this purpose, the bidder needs to factor costs associated with use case implementation into their pricing and ensure that domain use cases are ready before UAT phase. Finalization of use cases shall be done in design phase in coordination with the Authority. The solution proposed by bidder should be integrated with the existing deployed solution by the city and needs to provide scalability option to implement new use cases as and when new smart systems are deployed in the city.

The IA shall provide supporting documents in the technical bid justifying the approach & design of offered solution.

2.4 Project Deliverables, Milestones and Timelines

T = Issuance of Work Order.

Milestone No.	Milestone Name / Phase	Description / Scope of Work	Timeline	Payment Terms
M0		T= Issuance of Work Order		
M1	**Deployment of Critical Surveillance Infrastructure (Phase-1)**	• Submission of SRS and FRS document Construction & commissioning of ICCC at JBPC (civil + electrical + IT + non-IT) • Setup of video wall, consoles, servers, storage, VMS, analytics • Deployment along Grand Road corridor (Temple → Gundicha) • Deployment on all entry–exit corridors (Bhubaneswar–Puri, Konark, Chilika/Brahmagiri, Sakhigopal/Chandanpur) • Deployment at all parking sites & Puri Railway Station • Enabling drone-feed readiness	**T+3 Months**	**40% of CAPEX**
M2	**Integration with Existing Infrastructure (Phase-1)**	• Integration with existing SJTA ICCC & Police systems • Integration of Viewing Centre at Singhdwar • Integration of internal & external periphery cameras of Shree Jagannath Temple • Unified alerting, dashboards, SOP alignment among agencies		**10% of CAPEX**
M3	**UAT, Testing, Commissioning & Phase-1 Go-Live (Before Rath Yatra 2026)**	• End-to-end testing, analytics validation, network testing, SOP validation, DR drill, multi-agency readiness, Go-Live certification.	**T+ 4 Months**	**10% of CAPEX**
M4	**Phase-2 Deployment & Integration**	• Remaining junctions across Puri	**T + 10 Months**	**30% of CAPEX**

Milestone No.	Milestone Name / Phase	Description / Scope of Work	Timeline	Payment Terms
	(Citywide Expansion)	• Marine Drive / Beach Road surveillance • Peripheral town approaches (Pipili, Sipasurubili, Baliapanda, Batagaon, etc.) • Additional parking sites • PAS & VMD deployment citywide • Final OFC ring & redundancy establishment • Drone ingestion capability activation • Integration with Phase-1 ICCC	**(post Phase-1 Go-Live)**	
O&M Q1–Q20	**Quarterly O&M Services (5 Years – 20 Quarters)**	• Preventive & corrective maintenance, uptime management, analytics accuracy, emergency response support, dashboard availability, field repairs, replacement of damaged components, reporting.	**Quarterly – 20 Quarters**	**0.5% of CAPEX per quarter+ Quarterly O&M Payment as per Bidder's Quoted O&M Price**

- All payments to IA shall be made upon submission of invoices along with necessary approval certificates from the Authorities concerned.
- The request for payment shall be made to Authority in writing, accompanied by invoices describing the services performed, and by the required documents submitted pursuant to general conditions of the contract and upon fulfilment of all the obligations stipulated in the agreement.
- Due payments shall be made promptly by Authority generally within thirty (30) days after submission of an invoice for payment by IA. The Taxes, as applicable, shall be deducted / paid, as per prevalent rules.
- The currency or currencies in which payments shall be made to the IA shall be Indian Rupees (INR) only. All remittance charges shall be borne by the IA.
- In case of disputed items, the disputed amount shall be withheld and shall be paid only after settlement of the dispute.
- Any penalties/liquidated damages, as applicable, for delay and non-performance, as mentioned in this RFP document, shall be deducted from the due payments of the respective milestones.
- Payment against "STQC Certification and system audit" (STQC certification to be provided cameras OEM and system VAPT audit to be done by Cert-in empanelled agency) shall be released only after completion of the respective Audits as decided by the authority. All other

payment shall be released against the completion of respective milestones/task/activities.

2.5 Deemed Acceptance

The Authority shall provide acceptance for go-live of each milestone within 60 working days from the date of completion of the UAT for that milestone. The Authority shall provide the following to the IA:

- Stakeholders/Approvers involved in deliverable project output.
- Deliverable details and its impact/strategic outcome.
- Deliverable Timeline calendar with alerts to all Stakeholders/Approver
- Sign off timeline calendar with alerts to all Stakeholders/Approvers

In case the Authority fails to respond and provide feedback on above stated submission, the deliverables shall be DEEMED ACCEPTED.

Post the elapse of the 60 days' approval period, the IA shall not be asked to rework on the said project outputs/outcomes. However, in case the Authority confirms to the IA with an alternative date, then that date would hold valid for the deemed acceptance. Such revisions shall be limited to 2 (two).

Any subsequent rework post acceptance/deemed acceptance would form the subject of a formal "Change Control/ Change Request", which has been detailed in Article 57- Change Control Note (CCN) of Volume III.

3. Design Considerations

3.1. Introduction

The bidder shall design the Advance Surveillance System & Smart Components solution incorporating guiding principles, foundational design aspects for the functionalities/ components as mentioned below, which are further detailed out in this RFP.

- Integrated Command and Control Center.
- City Surveillance System
- Video Summarization System
- Automatic Number Plate Recognition System (ANPR)
- Red Light Violation Detection System
- Parking Surveillance
- Speed Violation Detection System
- Variable Message Display
- Public Address System
- City Communication Network
- City Systems / Applications
- Data Center & Disaster Recovery Center
- Cyber Security Solution
- Data Management

The IA shall submit a detailed technical solution, including CONOPS, logical architecture, data architecture, integration architecture, network architecture, security architecture and deployment architecture. IA shall describe how each of the functionalities/ components shall work in their overall solution. IA shall also detail the platforms and tools they propose to implement for achieving the standardization requirements as listed in the sections that follow along with compliances (wherever applicable).

Common Principles/Guidelines regarding compliance of IT systems/equipment's shall also be captured along with Perpetual licenses, Software licensing, IPv4 and IPV6 compliances, etc.

3.2. Guiding Principles

IA shall design the solution while taking into consideration the following guiding principles:

3.2.1. Scalability

Important technical components of architecture must support scalability to provide continuous growth to meet the growing demand of the city. The architecture should be scalable (cater to increasing load of internal and external users and their transactions) and capable of always delivering high performance. The solution should support vertical and horizontal scalability so that depending on changing requirements from time to time, the solution may be scaled upwards. There must not be any system-imposed restrictions on the upward scalability of data center IT components such as compute infrastructure such as Application & Web Servers, Database Servers, data storage infrastructure, bandwidth, application software, number of cameras, or other smart city components required in this project. The data center infrastructure shall be capable of serving the growing concurrent users' requirement which would be increasing as the city grows.

3.2.2. Availability

The architecture components should provide redundancy and should be resilient to technology sabotage. It should be ensured that there are no single points of failures in the key solution components, including core/data center components. To take care of remote failures, the systems should be configured to mask and recover with minimum outage. The IA shall make the provision for high availability for all the services of the system.

3.2.3. Security

The architecture should adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft, natural disasters etc. IA should make provisions for the security of field equipment as well as protection of the software system from hackers and other threats. IA's solution shall adhere to the model framework of cyber security (K- 15016/61/2016-SC-1, Government of India, and Ministry of Urban Development), while designing the solution, the system shall be highly secure as it is intended to handle sensitive data relating to the city and its residents. The Authority would carry out the security audit of the entire system upon handover and at regular intervals during O&M period.

3.2.4. Manageability

Ease of configuration, ongoing health monitoring, and failure detection are vital to the goals of the envisaged project. The system should be auto/manual configurable for various future requirements for the ease of maintenance / debugging.

3.2.5. Interoperability

The system should have interoperable capability with other ICT Systems.

3.2.6. Universal Access to IT Systems

The solution designed should ensure Universal Access to IT systems to empower citizens of Puri City with disabilities, to access various systems/components envisaged and future systems for integrations with ease.

3.2.7. Open Standards

Systems should be built on open standards and protocols. Keeping in view the evolving needs of interoperability considering that solution shall become the focal point of delivery of services and may also involve cross-functionality with the project systems of other departments The IA shall ensure that all system applications developed is easily integrated with the existing applications using open APIs. The software code should not build a dependency on any proprietary software. The standards should at the minimum comply with the published national standards such as BIS standards for smart cities, e-governance standards, frameworks, policies, and guidelines available on http://egovstandards.gov.in (updated from time-to-time). Systems implemented by the IA shall adhere to the Unified Digital infrastructure (UDI) properties defined in IS 18000 and the data principles defined in Table 1 of IS 18002.

3.2.8. Single-Sign On

The application should enable single-sign-on so that any user once authenticated and authorized by the system is not required to be re-authorized for completing any of the services in the same session. For employees of the department concerned, the browser-based application accessed on the intranet, through a single sign-on mechanism, shall provide access to all the services of the departments concerned (based on role-based access policy), Help module, basic and advanced reporting etc.

3.2.9. Application Architecture

The software applications designed and developed must follow best practice and industry standards and shall be based on approved requirements. In order to achieve high level of stability and robustness of the application, the system development life cycle must be carried out using the best industry standard practices and adopting the security constraints for access and control rights.

The system applications envisaged under the scope of this project should integrate with key initiatives of State, namely Portal Services, Citizen Contact Center, and Certifying authority, etc. as applicable and required by authority.

The systems should at least comply with the published BIS smart city standards, e-Governance standards, frameworks, policies, and guidelines available on http://egovstandards.gov.in (updated from time-to-time) and https://bis.gov.in/. The system implemented in the city shall adhere to the Unified Digital infrastructure (UDI) properties defined in IS 18000 and the data principles defined in Table 1 of IS 18002.

All IT products and services used by IA must necessarily incorporate the principle of Universal Design and global accessibility standards as approved by MeitY. In absence of any such MeitY approved standards, IA should adhere to global accessibility standards as reference (e.g., EN 301 549).

All information portals and websites developed by IA for information dissemination must necessarily be in accessible formats, adhering to the provisions of the WCAG 2.0, Web Access Guidelines. The IT systems should be built, with an aim, to provide maximum accessibility and usability to its users irrespective of device in use, technology, or ability.

3.3. Reference Functional Architecture for Integration City Surveillance System Project

The solution architecture for Integrated City Surveillance Components project shall have broad set of components/layers as indicated below. It may be noted that some of the layers/components might already exist in the city and the IA should leverage these as best as possible to reduce the cost.

A. Sensor / Field Device Layer

- The Sensors, Actuators etc. shall help the city administration to gather information or capture information from the field devices like cameras, sensors, ANPR etc.
- The exact sensors, actuators and their numbers and physical deployment locations, as well as data rates, bandwidths, and latencies, shall be driven by the applications and use cases scenarios.
- The IA should indicate/explain the plan/capability of their solution for scaling by up to 2x to meet the future requirements of the city.
- The IA should explain the security architecture, tamper detection schemes if any and non-repudiation of the data from the field devices. The security architecture should be as per appropriate international standards, 8.14 of IS18000 and Indian Government guidelines.
    - The IA should indicate the expected key performance indicators like data rate, latency, and availability.
    - The IA should explain the life cycle management of the field devices, including the periodic maintenance of such devices.

B. Network Layer

- The secured communication layer shall serve to provide connectivity to gather data from sensors including video cameras and other field devices and communicate messages to display devices, outdoor speakers, actuators, and other field devices.
- It shall support all field devices, sensors, cameras etc. at given locations as required by the use cases and application requirements.
- The IA shall suggest the required throughput, latency, and availability to meet the use cases and application needs.
- The IA should propose a methodology for scaling up of the performance metrics as the needs of the city grow by a factor of 2x. Such a scale up should be possible via seamless addition of new endpoints and appropriate provisioning of network resources.
- The IA shall detail out two main components of the communication layer:
- A Wide Area Network to bring data from across the area of interest to the compute- data center.
- A field network to interconnect all the field devices to their respective gateways to eventually get connected into the applications in the compute-data center layer.
- A standards-based field device and network management framework should be adopted and demonstrated by the IA.
- Provisioning of network connectivity/bandwidth shall be done by the IA as part of their scope, subject to TRAI regulation.
- IA shall also provide detailed bandwidth calculations with appropriate justifications.
- IA shall design the network in such a way that there are no interdependencies amongst the various components.

C. Data Center & Disaster Recovery Layer

- The on-premises Data Center layer shall house centralized computing and storage resources needed to store, process, and analyze the digital data required to derive actionable information. This layer includes general purpose compute servers, specialized GPU clusters, non-volatile storage clusters, data center network equipment and system software for Operations & Service management and Security & Trust management. This layer should have redundancy and disaster recovery capabilities.
- The layer should be sized to meet the compute throughput (Transactions(s)) and bandwidth (MB(s)) requirements as derived from the application and required use cases.
- The IA should propose a methodology for scaling up of the performance metrics as the needs of the city grow by a factor of 2x.

D. Smart Application and Integration

This layer of the individual systems of Integrated City Surveillance Components project which shall be integrated with ICCC system application shall be driven by the actual use cases and applications desired by the City. It shall broadly consist of the following components.

- Core Domain Applications: These shall be the core applications for various verticals/systems of the Integrated City Surveillance project. These shall be integrated into the existing SJTA ICCC at JBPC system application, integration with Viewing center by OBCC at Singha Dwar Police

Station and integrations with existing cameras at Temple, Railway Station and as per requirements given by authority (in terms of exchanging data, alerts, etc.), leading to generation of new insights and dashboards, especially across different vertical silos.

- ICT Services Enablement Applications: These applications shall allow lifecycle management of existing applications as well as allow onboarding and provisioning of new applications (8.9 & 9.5.6 of IS18000).

E. Service delivery and consumption

The output field devices layer will contain display devices, or bi-directional (input & output) devices connected to the network which will be used by citizens to consume - and for administrators to provide - actionable information. Such field devices include existing Command Control Center, Puri ICT intervention & the Service delivery and consumption Layer center and control units shall enable citizens and administrators to like to get a holistic view of city conditions. Such control units shall take shape of either an exhaustive command center or control applications which can be viewed over a web browser with mobile responsive.

F. Security Layer

Information and Infrastructure Security plays a very critical role in protecting the city physical assets such as field IoT devices, IT infrastructure and logical assets such as field data and citizen data. ICT security covers all layers such as Infrastructure, Data, Integration, Services and Applications. The detailed functional requirements of the security layer are as per Section 8.14 of the IS18000 and covers:

- Application security
- Data security
- API security
- Security Emergency Management
- IP Protection and data loss prevention.

IA's solution shall adhere to the model framework of cyber security (K- 15016/61/2016-SC- 1, Government of India, and Ministry of Urban Development) and other sections of this report.

4. Integrated Command and Control Center

4.1. Overview

The Integrated Command & Control Centre (ICCC) shall function as the central nerve center for monitoring, decision-making, coordination, and real-time response for the Integrated City Surveillance System (ICSS) deployed across Puri. The ICCC shall provide a unified platform for integrating live video feeds, analytics alerts, communication systems, field devices, and operational workflows to support the District Administration, Puri Police, SJTA, OBCC, and other stakeholder departments, particularly during high-intensity events such as the Jagannath Rath Yatra, Snana Purnima, New Year gatherings, and other mass congregation scenarios.

The ICCC is envisaged as a state-of-the-art, 24×7 operational facility, designed to host advanced surveillance systems, video management platforms, artificial-intelligence-based analytics engines, multi-agency communication systems, and decision support tools. The ICCC shall ensure a seamless flow of information between the field, operators, supervisors, and senior decision-makers, enabling proactive monitoring, rapid incident detection, timely escalation, and effective on-ground coordination.

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

The proposed Integrated Command & Control Centre (ICCC), Video Management System (VMS), Video Analytics (VA) and Intelligent Traffic Management System (ITMS) applications shall be from the same OEM to ensure seamless integration, unified architecture and consistent performance. The IA to ensure end-to-end accountability, simplified system integration, faster issue resolution and improved operational reliability throughout the project lifecycle by the OEM.

4.2. Functional and Technical Specifications of ICCC Application

Parameter	Functional and Technical Specification
Requirements and Certifications	• ISO 9001:2015, 27001:2013, ISO 14001:2015, ISO 45001:2018,ISO 27017:2015 and CMMI Level – 3 • The Intellectual Property Rights (IPR) of Offered Integrated Command & Control Center (ICCC) Application Platform must not reside in Country sharing Land Border with India. • The Integrated Command & Control Center (ICCC) Application Platform Offered should not be Developed/manufactured by an entity in which the majority shareholding of the entity is from a Country sharing a Land Border with India. • OEM must provide with a Declaration about the Intellectual Property Rights (IPR) & Source Code Residence/Filing in the respective Country as a Documentary Evidence. • The Integrated Command & Control Center (ICCC) Application Platform OEM whose Intellectual Property Rights (IPR) & Source Code residing in India shall be Preferable. • The OEM who is Claiming to be Make in India OEM with Local Content greater than 50%, then their Intellectual Property Rights (IPR) & Source Code must Reside in India only. Documentary Evidence to be Provided.

Parameter	Functional and Technical Specification
	• The Proposed Integrated Command & Control Center (ICCC) Application Platform should have undergone Audit as per OWASP, OWASP Top 10 Web Application Security Risks from STQC. A Security Test Report from STQC to be Submitted by the respective OEM to Substantiate the Proof of the Security testing. • The Applications must have already undergone the Security testing/Auditing
Solution & Platform	• The platform should be able to normalize the data coming from different devices of same type (i.e. Different lighting sensor from different OEMs, different energy meters from different OEMs etc.) and provide secure access to that data using data API(s) to application developers
Command & Control Center Components	• Web server to manage client requests. Client should provide web-based, one-stop portals to event information, overall status, and details. The user interface (UI) to present customized information in various preconfigured views in common formats. All information to be displayed through easy-to-use dashboards. • Application server to provide a set of services for accessing and visualizing data. Should be able to import data from disparate external sources, such as databases and files. It should provide the contacts and instant messaging service to enable effective, real-time communication. It should provide business monitoring service to monitor incoming data records to generate key performance indicators. It should also provide the users to view key performance indicators, standard operating procedures, notifications, and reports, spatial-temporal data on a geospatial map, or view specific details that represent a city road, building or an area either on a location map, or in a list view. The application server should provide security services that ensure only authorized users and groups can access data. • System Platform – The platform should provide a common data integration layer which can collect and contextualize information from disparate data sources regardless of protocol. The platform should support templatization to allow "build once-deploy everywhere" functionality. • Workflow and Incidents Lifecycle engine – This function should allow users to define and modify new workflows. • The workflow could cut across multiple systems via the interfacing modules. Workflow for operational alerts and escalations should be triggered automatically without human intervention. Workflow approvals should have facility to approve from any device with e-

Parameter	Functional and Technical Specification
	signature. This function should provide facility to trigger a corrective action workflow and define the stakeholders for the same. Should manage the life cycle of incidents and related entities via pre-define workflows. The workflow could cut across multiple systems via the interfacing modules. Workflow for operational alerts and escalations should be triggered automatically without human intervention. • Incidents Planning – should manage the planning preparations of an incident including resource allocation, tasks management etc. • Analytics and MIS – should provide users with business analytics reporting and tools to organize, evaluate and efficiently perform day to day operations • Centralized data archiving for operational data : Should provide facility for centralized storage of operational data (time-series or transactional) with high granularity and data compression capability • Mobility: should enable app-based access to monitor alerts, KPI ,KOPs, SOPs and reports to mobile users. Should support popularly user's smartphone /tablets. App content should be presented in context to the user role.
Convergence of Multiple feeds / services	• System needs to have provision that integrates various services and be able to monitor them and operate them. The solution should provide option to integrate existing deployed solution by City and also need to provide scalability option to implement new use cases. System should support DDE and OLE for integration with Process control systems and sensors System should have capability to • source data from various systems implemented in Puri City to create actionable intelligence
Standardized Data Aggregation and normalization capabilities	**System Use Cases and Integration:** • It is envisaged that the Integrated Command & Control Centre will implement multiple Smart System use cases over a period. • The potential Systems to integrate, as per current and future scope, are: o New CCTV Surveillance (Video Management System) o Existing CCTV Surveillance (Video Management System) o ANPR (Automatic Number Plate Recognition), RLVD (Red Light Violation Detection), Speed Detection Application o Facial Recognition Software o AI-based Video Analytics o Other Utility Services (if any) • **Architecture:** ICCC Platform should follow a **System of Systems** approach and integrate with existing sub-systems as well as future sub-systems.

Parameter	Functional and Technical Specification
	• **Unified Interface:** Should have the ability to integrate with sub-systems natively, driving a **unified user interface** for ease of operations and facilitating central control across multiple operations. • **Control Capability:** The Platform should have the ability to take over the specific allowable control of the integrated sub-systems through a single user interface, empowering the operator to manage critical incidents and events by directly initiating control over the sub-system. • **Data Acquisition:** The data store function shall acquire data both automatically and manually. Automatic data acquisition shall be met through industry-standard data transports. • **Operational Technology (OT) Connectivity:** ICCC Platform should be able to connect to operational technologies with **bi-directional control** via an inbuilt native protocol (Optional) for managing security parameters and threats related to various utility systems. • **Supervisory Control:** ICCC Platform should have built-in supervisory control to send control signals to the end systems in case of emergency and process overrides. • **IT/Network Integration:** ICCC platform should connect to IT Applications and network Systems via point-to-point integration: • **IT Protocols:** Web-services/APIs (REST/SOAP/RPC)/SDK • **Network Protocols:** SNMP (Simple Network Management Protocol) • **Data Handling & Security:** The platform should be able to **aggregate and normalize** data from different devices and provide secure access to data using data SDK/API(s) to application developers. The message exchange between various applications via the ICCC platform should be **fully encrypted and authenticated**. **Openness and Interoperability:** 1. ICCC platform is required to provide a single common layer for all connectivity to simplify configuration, establish standards, accelerate implementation, minimize maintenance, and expand capabilities. 2. It must fully embrace the openness of open protocol communication technology, exposing data from products as an open protocol communication Client and providing the means to connect to any third-party open protocol communication Server or vice versa. 3. **Deployment & Management:** The platform should support **distributed deployment** of functions (workflows & policies) across the System's network and compute infrastructure with centralized management and control. 4. **Access Control:** The platform must provide ease of management with adequate **authentication** and **Role-Based Access Control (RBAC)** mechanisms. 5. **User Authentication:** The platform should support on-premises **Active Directory** for user authentication.

Parameter	Functional and Technical Specification
	6. **Time Synchronization:** Must have time synchronization capability and be able to integrate with **GPS or IRNSS**. 7. **Data Flow:** The platform should have provisions for the flow of **normalized data** in a predefined manner with adequate authentication.
Developer Program Tools	• ICCC platform should provide a comprehensive API to allow interfacing and integration of 3rd party systems
Platform Upgrade and Maintenance	• **Incremental Changes and Continuous Updates:** The Platform should be able to make incremental changes in response to the staged object deployment within the same scan cycle and make **continuous updates on the fly**. • **Deployment Model:** The Platform should be able to be deployed as an **on-premises Model** as a primary service.

Platform Functionality	• **Incident Handling (SOPs):** The System should enable users to define the business rules around incidents handling and Emergency response as per agreed **Standard Operating Procedures (SOPs)**.
	• **Data Integration Layer:**
	  • The System should provide a common data integration layer for **Transactional Data (DB)** and a common data integration layer for **Time-Series Data**.
	  • This layer must collect and contextualize information from disparate data sources using **RESTful APIs**.
	  • The Platform should have **supervisory capabilities** and be able to bi-directionally monitor, command & control all types of operational technology.
	Incident Lifecycle Management:
	• The System should manage the life cycle of incidents and related entities via **predefined workflows**.
	• The workflow should be able to write interactive SOPs and cut across multiple systems via the interfacing modules.
	• Workflows for operational alerts and escalations should be triggered **automatically without human intervention**.
	• **Incident Planning:** The System should manage the planning and preparation for an incident, including resource allocation and tasks management.
	Business Analytics and Reporting:
	• The System should provide users with **business analytics reporting** and tools to organize, evaluate, and efficiently perform day-to-day operations.

Parameter	Functional and Technical Specification
	• The System should provide filterable reports and **dashboards** about critical information pertaining to incidents and **Key Performance Indicators (KPIs)** collated in a single view, which can be drilled down further for more detailed information. • **Role Management:** The System should manage roles definition for internal as well as external access. • **Data Storage:** The System should provide a facility for centralized storage of operational data (time-series) with **high granularity** and **data compression capability**. • **Mobile Workflow Access:** The System should enable operators and crew members to access the workflow tasks assigned to them and act using a **native mobile application**. They should be able to close the loop of the workflow by acknowledging the real-time status of the action assigned to them. • **Application Management:** The platform provides a **role-based access view** to applications. • **Enabling Analytics:** The platform should support real-time analytics through **Stream Analytics** and time-shifted analytics. • **Multi-Monitor Support:** The Application GUI should support a **multi-monitor application**. • **Application Client Access:** Application client access should support: • **Web-based Terminal Application:** Must use standard web technologies (like HTML/JSP/PHP, etc.) and require **no software installations**, being accessible directly from a web browser. • **Browser Compatibility:** Supported browsers shall include, but not be limited to, IE, Chrome, Firefox, and Safari. • **Mobile Device Support:** The platform shall also be able to present information on mobile devices such as tablets and smartphones while maintaining the basic UI features. • **Communication Configuration:** Application should support **Read-only OR Read/Write** communication configuration for monitoring and control operations.
Authentication, Authorization	• **Authentication and Authorization:** The System should support standard **Authentication and Authorization** mechanisms. • **Single Sign-On/Off (SSO):** The System should support **Single Sign-On (SSO)** and **Single Sign-Off**. • **Multi-Factor Authentication (MFA):** The System should support **Multi-Factor Authentication (MFA)**.
Human Machine Interface	**Modern User Interface (UI/UX) Design:**

Parameter	Functional and Technical Specification
	• The ICCC platform should have a user interface that provides displays with a **modern UI/UX design**. • The **Mobile App** should provide multi-touch and gesture controls such as panning & zooming, swipe, clutter & declutter of graphical layers, and a larger view of the process. • The platform must offer an **extensible library** of pre-designed 'intelligent' and customizable visualization objects & templates. **Client/Server Architecture and Graphics:** • The ICCC platform should have a **client/server architecture** to allow multiple client access to an Ethernet-connected server. • Multi-Platform Access: The UI/UX for the ICCC platform should support multi-monitor configurations and shall work on both OS-based native applications as well as web-browser access.
GIS Map Support	• GIS UI/UX: The platform should feature a **GIS UI/UX** that can integrate with any existing GIS solution via standard integration protocols. • System Interactivity: The platform should be interactive with all sub-systems as and when required, with a focus on map-based interaction. • Map Service Support: The System should support major GIS map providers, including: o **ESRI** o **Mapbox** o **Open Street Map** o **Google Map** o Any other compatible GIS map service. **Map Format Support:** The System should also support PDF and various image formats of Maps, including: o **KML** (Keyhole Markup Language) o **GML** (Geography Markup Language) o **JPEG, PNG, GIF**, etc. **Asset Visualization and Layering:** o It should be possible to visualize all the **Assets** (Sensors, Devices, Vehicles, Cameras, other System resources) on the map. o These Assets must be provided as **layers** with the ability to switch these layers on and off to visualize the assets of only selected layers.

Parameter	Functional and Technical Specification
	○ The platform should also have the ability to access device functionalities **directly from the map**.
Location Engine (Integration with GIS MAP)	• **Geographical Data Access:** Map services and geospatial coordinates must provide access to the geographical coordinates of specific facilities, roads, and all **System infrastructure assets** (both ICT & non-ICT Infra). • If there is an existing ICCC, please clarify if GIS engine and GIS maps are existing or any new updated solution with maps to be provisioned. • All the components to be installed as part of this RFP along with the existing systems shall be plotted in GIS map for real time view with Maps to be provisioned by the IA. If any existing map available shall be share with the IA during project implementation. • **Location-Based Tracking:** The platform should offer **location-based tracking** functionality to locate and trace devices on the map.
Visualization	**Object-Oriented Graphics and Situational Awareness:** • The platform system software shall include an **object-oriented colour graphics display generator** with full animation capabilities. • This is to provide users with a realistic and efficient visualization of the system process. • It shall provide graphical capabilities to allow the design of a highly efficient user interface aimed at helping operators to easily achieve a state of **situational awareness** in relation to the process. • **Large Video Wall Display:** The Platform should be capable of displaying the application on a very **large video wall** with **4K resolution**, regardless of the physical size or configuration of the video wall. • **Multi-Monitor and Targeted Display Support:** • Visualization should support **multi-monitor capability** without the need to open multiple instances of the application. • It should also support opening a specific part of the application at a defined location on the video wall.
Data and Analytics Engine	• **Data Archive and Logging:** The platform must provide **Data Archive and Logging** functionality to store data feeds from the device engine and external data sources. • **Multi-Dimensional Analysis:** • The ICCC platform should be able to perform **multi-dimensional analysis** on incidents data.

Parameter	Functional and Technical Specification

	• This should provide the capability to do **Trends Analysis** and provide:
	  ○ Near **real-time Stream Analytics**
	  ○ **Time-shifted** (or offline) analytics on the archived data.
	• **Reporting:** The platform should feature a **Reporting** mechanism that delivers reports based on events triggered by device engine data and external notifications.

Reporting Service	• **Advanced Data Analysis and Publication:**
	  • It should provide **data-trend analysis** and sophisticated **numerical-data analysis** using Microsoft Excel spreadsheet software.
	  • It must offer comprehensive data reporting and the capability to publish **real-time and historical information** to the Web or intranet site.
	  • **Scheduled and Compliance Reporting:** The system must produce **on-demand and scheduled reports** for regulatory compliance and management purposes.
	  • **Report Publication:** It should be able to publish reports easily to intranet or Internet servers.
	  • **Customizable Filters:** It must be possible to customize **data filters** as per users' specific inputs.
	  • **Database Connectivity:** The platform must have the possibility to connect to local or remote **Relational Database (RDB) sources** through either **Open Database Connectivity (ODBC)** or **OLE-DB**.
	  • **Report Template Management:** The system requires **Report Template Version Management**.

Events & Incident Management	• **Policy Creation via Rule Engine:**
	  • The System should allow **policy creation** to set rules using a **Rule Engine** that control the behaviour of infrastructure items.
	  • Each policy should have a set of conditions that activate the behaviour it provides.
	  • **Policy Types:** The System should allow for the creation of the following policy types:
	  • **Default**
	  • **Time-based**
	  • **Event-based**
	  • **Manual Override**
	• **Automated Event-SOP Linkage:** The System should support the creation of sudden critical events and automatically link them to **Standard Operating Procedures (SOPs)** without human intervention.

Parameter	Functional and Technical Specification
	• **Multi-Incident Management:** The system should support for managing multiple incidents with both **segregated and/or overlapping** management and response teams. **Incident Criticality and Collaboration:** • The system should provide a facility to capture the **criticality of the incident** and allow it to be modifiable in real-time by multiple authors with role-associated permissions (read, write). • Incidents should be captured in **standard formats** to facilitate incident correlation and reporting. • **Event-Based Policy Triggers:** The System should provision the ability to define a set of conditions that can be used to trigger an **event-based policy**. • **Critical Infrastructure Tracking:** The system must identify and track the status of **critical infrastructure/resources** and provide a status overview of facilities and systems.
Notifications, Alerts and Alarms	**Advanced Alarm Management:** • The System should generate Notification, Alert, and Alarm messages that should be visible within the **Dashboard** and the **Enforcement Officer Mobile App** (if required). • The System must have advanced alarm management capabilities, including: o State-based alarming o Alarm suppression o Alarm shelving o Alarm grouping and aggregation (active & historical) **Centralized Message Visibility:** All system messages (notifications, alerts, and alarms) should always be visible from the **Notifications view**. This view must provide controls that the operator can use to **sort and filter** the messages it displays. **Multi-Method Notification Service:** • Systems should deliver messages to a set of subscribers. • The Notification service should support a minimum of three types of notification methods: o **Email notification** o **Short Messaging Service (SMS) notification** o **Whats app messaging** o **Mobile App-based Notifications**
	Core RBAC Structure: Users access and perform various tasks (e.g., adding locations, configuring devices, managing adapters). • Not all users can perform all tasks.

Parameter	Functional and Technical Specification
	• Each user should be associated with **one or more roles**, and each role is assigned a specific set of **permissions**. **Location-Based Restrictions:** • These roles and permissions define the tasks a user can perform. • Additionally, the system should assign **one or more locations** to each role so that the user can perform tasks **only at the assigned locations**. • **Task Granularity:** Roles and permissions define the specific tasks a user can perform, such as adding users, viewing location details, exporting devices, generating reports, and so on. • **Flexible Policy Creation:** The platform should allow different roles to be created and assign those roles to different access control policies. • **User-Area Association for Control:** • The platform should allow the association of users and areas/locations. • The system allows the creation of areas/locations (corresponding to physical zones) and allows the admin to associate different users with different areas. • This ensures that each user can control only services for the respective area/location for which they have been given access. • **LDAP Support:** The System should support **LDAP** (Lightweight Directory Access Protocol) to be used as an additional data store for user management and authentication.

Dashboard and Analytics	• **Benchmarking and Data Access:**
	  ○ The ICCC platform should allow users to define **benchmarks** against performance parameters.
	  ○ Performance reports shall have the option to generate reports **with or without benchmark comparison**.
	  ○ The platform should have the capability to provide access to **near real-time, real-time, and historical data** from various connected devices for reporting and analytics.
	• **KPI Dashboards and Drill-Down:** The ICCC platform should provide **filterable reports and dashboards** about critical information pertaining to incidents and **KPIs** (Key Performance Indicators) collated in a single view, which can be **drilled down** further for more detailed information.
	• **Integrated Dashboards and Navigation:**
	  ○ The ICCC platform should provide **integrated dashboard and KPI tracking capabilities** for various System functions.
	  ○ Dashboards should be designed to allow the user to easily **navigate user interfaces** for managing profiles, groups, message templates, communications, tracking receipts, and compliance.

Parameter	Functional and Technical Specification
	○ The ICCC should also have capabilities to configure and monitor key performance indicators on a **real-time basis**. • **Historical Data and Consolidated Reporting:** ○ The ICCC platform should provide **historical reports, events data, and activity logs**. ○ The reports can be exported to **PDF or other formats**. ○ The offered platform for Reporting and dashboard solution should have a consolidated **Single Window reporting, correlation, and Analytics solution** for all non-video applications.
Data Security	• **Data Security and Efficiency:** Access to the platform data should be **highly secure and efficient**. • **API Key Security:** Access to the platform's API(s) should be secured using **API keys**. • **Security Standards Support:** The software should support key security standards to help protect the data across all domains, including: • **SSO** (Single Sign-On) • **HTTPS over SSL/TLS** (Secure Sockets Layer/Transport Layer Security) • **Key Management**
CCC Operations	• **Full Platform Integration:** The ICCC platform shall be a fully integrated **custom-built software platform** that provides seamless integration and control mechanisms with various **Information Technology (IT)**, **Operational Technologies (OT)**, and **IoT sensors/applications/platforms**. • **Dynamic GIS Integration:** The solution shall integrate with **GIS and map information** and be able to dynamically update information on the GIS maps to show the real-time **status of resources**. • **Integrated User Interface:** The solution shall provide a single, **integrated user interface** for all the smart elements implemented. • **Management Dashboard and Status Tracking:** • The solution should provide operators and managers with a **management dashboard** that offers a **real-time status**. • This status must be automatically updated when actions, incidents, and resources have been assigned, pending, acknowledged, dispatched, implemented, and completed. • The above status attributes shall be **color-coded**. • **Operational Awareness:** The solution shall provide the **"day to day operation," "Common Operating Picture,"** and **situational**

Parameter	Functional and Technical Specification
	awareness to the center and participating agencies during these modes of operation. • **Scalability:** It shall improve **scalability** for large and geographically distributed environments. • **Comprehensive GIS-Enabled View:** It shall provide a **complete view** of sensors, facilities, ERP, video streams, and alarms in an easy-to-use and intuitive **GIS-enabled graphical interface** with a powerful workflow and business logic engine. • **Standardized Interface:** It shall provide a **uniform, user-friendly, and standardized interface**. • **Configurable and Role-Based Dashboards:** The dashboard content and layout shall be **configurable**. Information displayed on these dashboards shall be **filtered by the role** of the person viewing the dashboard. • **Incident Hierarchy and Analysis:** The solution shall allow the creation of a **hierarchy of incidents** and be able to present the same in the form of a structure for analysis purposes. • **Remote Access:** The solution shall be available via a **VPN** as a **web-based interface** or a **thin-client interface**. • **Flexible Display Views:** It shall be possible to combine the different views onto a **single screen** or a **multi-monitor workstation**. • **Comprehensive Audit Trail:** The solution shall maintain a **comprehensive and easy-to-understand audit trail** of read and write actions performed on the system. • **Document and Artifact Attachment:** The solution shall provide the ability to **attach documents and other artifacts** to incidents and other entities. • **Real-Time Control and Authentication:** • The solution shall provide **real-time schematics** to control the assets/operations audit logs. • The platform shall have the capability to **authorize and authenticate the operator** upon every write command issued from the ICCC platform. • **Realistic Visualization for Situational Awareness (Reiterated):** The ICCC platform system software shall include an **object-oriented colour graphics display generator** capabilities to provide users with a **realistic and efficient visualization** of the system process. It shall provide graphical capabilities to allow the design of a highly efficient user interface aimed at helping operators to easily achieve a state of **situational awareness** in relation to the process.
Incident view terminal	**Common Operational Picture (COP) Content:** The Common Operational Picture should comprise a comprehensive view of the incident or a group of

Parameter	Functional and Technical Specification
	related incidents as on a specific date and time. This view should include, but not be limited to, the following elements: • Tasks assignment and their status • Departments involved • Resources deployed • Incident status across relevant parameters of the incident • Timeline view of the situation • Suggested actions from the system with their status
Business Rule Engine	**Automatic Information Update and Refresh Cycle:** • The Platform should automatically update the information based on alarms and incidents that are presented to it via the **business rules engine**. • The polling and platform database refresh cycle shall be **configurable** to match the status of the situation (e.g., whether there is an emergency, crisis, or just monitoring only). **Incident Workflow and Alarm Handling:** • The Platform should feature **Incident Workflow Management**. • The ICCC platform must have a built-in alarm handling facility based on **configurable cause-and-effect rules**. • **Rules Engine Mode Differentiation:** The business rules engine shall be able to distinguish between an **"early warning or anticipation"** mode of operation and an **"emergency or crisis"** mode of operation.
Workflow Function	• **Cross-Functional Workflows:** The platform shall have **cross-functional workflows** with the ability to communicate and coordinate actions between **People, devices, and systems**. • **Corrective Action and Stakeholder Definition:** The Workflow function should provide a facility to trigger a **corrective action workflow** and define the relevant **stakeholders** for that workflow. • **Task Lifecycle Management:** The Workflow system should be able to **create, assign, track, and report** on the entire lifecycle of tasks during an incident. • **Task Decomposition:** The workflow system should allow a specific task to be decomposed into **sub-tasks**. • **Dynamic Task Assignment:** The workflow engine must have the ability for **dynamic assignment of tasks** based on roles, name, designation, or any other attribute present in the resource database. • **Dynamic Criticality Adjustment:** The criticality of a task within a workflow should be **dynamically changed** depending on the response SLA (Service Level Agreement). For example, a delay in

Parameter	Functional and Technical Specification
	response should automatically elevate the task to a high-priority task. • **Resource Queue Management:** The workflow should be able to perform **Queue Management** for the resources performing similar functions. * Queue Management must allow **automatic, semi-automatic, and manual** modes of task dispatch. * Algorithms supported should include, but not be limited to, **FIFO (First-In, First-Out), LIFO (Last-In, First-Out), and Round-robin**.
Standard Operating Procedure	Here are the corrected and properly formatted final specifications, detailing the comprehensive requirements for the **Standard Operating Procedure (SOP) Management** tool within the ICCC platform. **Standard Operating Procedure (SOP) Management** These requirements define the necessary tools and functionalities for creating, managing, and executing SOPs: • **SOP Authoring Tools:** * The ICCC platform should provide for authoring and invoking an unlimited number of configurable and customizable SOPs. * This should be achieved through a **graphical drag-and-drop design tool** (preferably using the workflow engine). * It should also have the capability to define SOPs by adding procedure/incidence steps instead of only using drag-and-drop. • **SOP Definition:** 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. • **User Interaction with SOPs:** The users should be able to **add comments** to or **stop the SOP** (prior to completion). • **SOP Audit Trail:** There should be a 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. • **SOP Activity Types:** The SOP Tool should have the capability to define the following activity types: * **Manual Activity:** An activity that is done manually by the owner, who provides details in the description field. * **Automation Activity:** An activity that initiates and tracks a specific work order, requiring the selection of a predefined work order from a list. * **If-Then-Else Activity:** A conditional activity that allows branching based on specific criteria. Users must enter or select values for the Then and Else conditions. * **Notification Activity:** An activity that displays a notification window containing an email template for the activity owner to complete, which then sends an email notification. * **SOP Activity:** An activity that launches another standard operating procedure (nested SOPs). • **CSV Data Read:** The System should be able to **read data from flat CSV files**.

Parameter	Functional and Technical Specification
	• **SOP Editability:** The SOPs defined in the system should be easily **editable by an administrator** with drag-and-drop capabilities. • **Workflow Presentation:** The ICCC platform shall present the workflow and task information in a **clear and logical manner** on the incidents screen. • **Policy and SOP Search Support:** The ICCC platform system shall include a section that will contain the **policy and standard operating procedures** with **easy-to-search functions** to support the Operators during a crisis. • **Role-Based SOP Step Handoff:** The ICCC platform should be able to pass the SOP step on to the **operator workstation** for the user to respond based on their **role and responsibility** in the SOP to achieve faster response to the incidences or events.
Export Formats	• **Export Formats:** The System should allow the export of analysis and reports into a minimum of the following formats: **Image, Excel, PDF, and CSV**.
Field Responder Mobile Apps	• **Workflow Task Access (Mobile):** The ICCC platform should enable operators and the crew members to access the workflow tasks assigned to them and act using the **native mobile application (Android)**. They should be able to **close the loop of the workflow** by acknowledging the real-time status of the action assigned to them. Approximate 10 number field officer will use mobile apps to be developed for the mobile vehicles. • **SOP Step Handoff to Mobile:** The ICCC platform should be able to pass the **SOP step to the mobile application** for the user to respond based on their **role and responsibility** in the SOP to achieve faster response to the incidences or events.
Technical Support Centre	• **24x7 Technical Assistance:** The ICCC platform OEM (Original Equipment Manufacturer) should have a **24x7x365 technical assistance Support Centre in India**. It must provide an online portal and contact number to register service requests, which can be raised by the partner (Implementation Agency/System Integrator) and the customer.
Video Display (Integration with VMS, via SDKs/APIs or Dynamic web UI	• **Live and Recorded Video View:** The platform shall have the ability to view **live or recorded video** from **resizable and movable windows** through integration with the Video Management System (VMS).

Parameter	Functional and Technical Specification
for tight contextualization)	• **Workstation Video Controls:** The platform shall have the ability to perform **video controls** for the VMS directly from the ICCC workstation. • **Recorded Video Playback:** The platform shall be able to play, fast-forward, rewind, pause, and specify time to play recorded video through integration with the VMS. • **Video Snapshot:** The platform shall be able to take a video still image (snapshot) from live or recorded video through integration with the VMS. • **Video Export:** The platform shall be able to **export video** for a user-specified time and duration through integration with the VMS. • **PTZ Camera Control:** The platform shall be able to perform video controls for the video system and move **PTZ (Pan-Tilt-Zoom) cameras** by taking controls from the VMS. • **Role-Based Video Access:** The platform shall enable users to only **view and control video** for which they have been assigned permissions by the administrator.
Traffic Violation Detection System/ ITMS	• Ability to define various violations in the system with multiple parameters. • Violation detection for various types of violations such as speed, red light violation etc. • Ability to gather evidence, issuance of challan and maintain records of violation and penalty etc. • In an event when spot speed detection system captures over speeding vehicles at a particular location, the system should be able to calculate the same also forms a part of the evidence for the violation • System shall be able to classify different category of vehicles such as TW, LMV, HMV etc. • System shall have provision for setting different speed thresholds for different classification of vehicles. • All vehicles passing through the control section at a Speed greater than a determined speed limit shall be detected as violation • The system shall be capable to integrate with NIC's eChallan system to raise any traffic violation challan for the RLVD and SVD detection systems. • The system shall be able to tag any particular photo evidence, along with ANPR captured vehicle number (if available) or manually entered vehicle number and push it to NIC's

Parameter	Functional and Technical Specification
	• eChallan system along with other details such as type of violation, location, date and time etc. and raise challan on NIC's eChallan system.

5. Surveillance System

5.1. Overview

Cameras being the core of the entire Surveillance system, it is important that their selection is carefully done to ensure suitability & accuracy of the information captured on the field and is rugged, durable & compact.

These cameras should work on 24 X 7 basis and transmit quality video feeds to the existing CCCs and capture the video feeds at 25 FPS.

The authority/ Police Department may review of the requirements for video resolution, FPS and may change these numbers to suit certain specific requirements (for example, there could be a situation when certain cameras are required to be viewed at higher FPS for specific period.)

5.2. Key Issues

The main challenges of surveillance pertaining to Grand Road that IA shall be required to consider are as follows:

- Design the solution to support both permanent deployments (for year-round operations) and temporary setups (for Rath Yatra and other mega-events).
- Adopt a phased approach: pilot testing at high-priority locations → citywide expansion → optimization.
- For Grand Road coverage having width of 40 meters (near Shri Jagannath Temple) to 130 meters (near Gundicha Mata Temple) AI to propose solution with no temporary/permanent infrastructure that can be installed in the middle lane of Roads.
- For Surveillance and Crowd Density during Rath Yatra integration with drones may be proposed.
- Integration with existing ICCC of SJTA at JBPC parking and integration of existing Viewing centres situated at SinghDwar Police station.

5.3. Scope of Work

5.3.1. General Scope

The Integrated City Surveillance System (ICSS) for Puri shall be implemented in a **phased manner**, with specific outcomes and KPIs aligned to the operational priorities of the District Administration, Police Department, SJTA, OBCC, and other stakeholder agencies.

5.3.1.1. Phase-1 Outcomes

(To be completed before Jagannath Rath Yatra – July 2026)

Timeline: 3 months implementation + testing, commissioning & Go-Live before July 2026
Scope of Phase-1

Phase-1 shall include complete readiness of critical surveillance and command infrastructure required during the Rath Yatra, covering:

- **Construction and Commissioning of ICCC at JBPC**
  - ICCC core IT/non-IT infrastructure
  - Video wall, consoles, network, storage, VMS, analytics setup
  - Integration with legacy systems of SJTA and Puri Police

- **Installation of Surveillance Infrastructure along Grand Road**
  - Entire Rath Yatra corridor from Jagannath Temple to Gundicha Temple
  - Crowd density analytics, PTZs, fixed cameras, FRS-ready locations
  - Integration with Drone feeds (if provided by Police/SJTA)

- **Coverage of All Entry–Exit Points of Puri Including:**
  - Bhubaneswar – Puri corridor
  - Konark Road
  - Brahmagiri / Chilika Lake side entry
  - Sakhigopal / Chandanpur corridor
  - Other access routes based on Police finalization

- **Integration with Existing SJTA ICCC**
  - Mandir outer periphery cameras
  - Inner precinct cameras (wherever permitted)
  - Crowd and queue monitoring workflows
  - Unified alerting and dashboard merging into the new ICCC at JBPC

- **Viewing Centre at Singhdwar Police Station (Developed by OBCC)**
  - SI shall integrate this viewing center with Phase-1 ICCC
  - Ensure shared feeds, synchronized alerts & unified SOP management

- **Surveillance Coverage at Parking Sites & Railway Station**
  - Talabania, JBPC, Loknath, Gadadhar, Sonar Bangla, Helipad, etc.
  - Puri Railway Station platforms, FOBs, circulating area
  - Crowd/vehicle analytics integration

- **Peripheral Locations Around the Temple**
  - Kalpabata, Anand Bazaar side, barricade points, security perimeters
  - AI-based crowd flow alerts for choke points

Indicative KPIs for Phase-1

- **Pre-Rath Yatra Go-Live Readiness**
  - 100% of Phase-1 cameras installed, tested, and streaming to ICCC
  - ICCC (JBPC) civil, electrical, IT & analytics stack fully functional
  - Integration with SJTA ICCC completed and validated
- **Operational KPIs**
  - **Camera Uptime:** ≥ 99% for all Phase-1 critical corridor cameras
  - **Analytics Availability:** ≥ 98% during Yatra period
  - **System Latency:** < 2 seconds for live streaming at ICCC
- **Emergency Response Metrics**
  - Average Emergency Response Time recorded via ICCC logs
  - PAS/VMD activation time < 1 minute after alert generation
  - Priority corridor clearance time (Singhdwar → Grand Road → Gundicha) monitored daily
- **Incident Monitoring & Logging**
  - Real-time logging of crowd surges, missing person alerts, ANPR hits
  - KPI: 100% incident closure as per SOP-defined workflow
- **User-Level KPIs**
  - Unified dashboards for Police, SJTA, District Admin
  - 24×7 operations with 3-shift ICCC staffing by IA

5.3.1.2. Phase-2 Outcomes

(To be completed within 6 months after Phase-1)

After successful Go-Live of Phase-1 for Rath Yatra 2026, Phase-2 shall cover citywide expansion and integration of the remaining surveillance locations identified in the Document:

Phase-2 Scope Includes:

- Remaining junctions across Puri city
- Marine Drive / Beach Road coverage
- Peripheral town approaches (Pipili, Sipasurubili, Baliapanda, Batagaon etc.)
- Additional parking locations
- Installation of PAS and VMDs at strategic nodes
- Final OFC connectivity ring, redundancy, and bandwidth augmentation
- Drone video ingestion capability (if provided later)
- Integration of Phase-2 feeds into the Phase-1 ICCC at JBPC

Indicative KPIs for Phase-2:

1. 100% of Phase-2 cameras installed and integrated within 6 months
2. GIS-based incident mapping activated for all city locations
3. SLA compliance for uptime, preventive maintenance, repairs and incident response
4. Storage archival performance: < 30 seconds retrieval for 30-day-old footage
5. Analytics performance: ≥ 95% accuracy across detection models

5.3.1.3. Operations and Maintenance Phase

Over the 5-year O&M period, the ICSS shall deliver:

Operational KPIs

- **System Uptime**
  - ≥ 99% uptime for all field devices, network components, ICCC systems
- **Analytics Performance**
  - Real-time alerts for crowd density, face recognition, ANPR, abandoned objects
  - KPI: ≥ 95% alert accuracy with < 5% false positives
- **Investigative Support**
  - Access to historic video for all authorized stakeholders
  - KPI: 100% availability of requested archived video footage
- **Emergency Support**
  - Automated alerts to Police, Fire, Ambulance, SJTA
  - SOP-based dispatch tracking
- **User Dashboard Availability**
  - Unified dashboard with alert summaries, action taken, device health status
  - KPI: ≥ 99% availability
- **Crowd & Incident Management Efficiency**
  - Measurable reduction in unmanaged crowd clusters
  - Reduction in security breach incidents at Temple periphery and Grand Road
  - Faster evacuation and diversion response times
- **Maintenance KPIs**
  - Quarterly preventive maintenance reports
  - Corrective maintenance response within defined SLAs
  - Replacement of damaged components at no additional cost

5.3.2. Details of Existing IT Infrastructure

5.3.2.1. Singh Dwar Viewing center and cameras for Outer periphery of the Shree Jagannath Temple

S. No.	Item Name	Qty	Make	Model
Field Infrastructure				
1	PTZ Camera	16	Bosch	NDP-5523- Z30L-P
2	Bullet Camera	220	Bosch	NBN- 80052-BA

S. No.	Item Name	Qty	Make	Model
3	Dome Camera	41	Bosch	NDE-3503- AL-P
4	Dome Camera	2	Bosch	NDE-3502- AL-P
5	Emergency Call Box	16	NVS	IP100024IC
6	Rack	56	Standard	
7	Public Address System	206	Standard	
8	VMD	1	Standard	
CCC Infrastructure				
9	VMS Server	1	HP	ProLiant ML110 Gen 10
10	NVR	4	Bosch	DIP- 73G0-00N
11	VMS	3	Bosch	BVMS Pro
12	ECB Mike	8	Standard	
13	Core Switch	2	Belden	
14	Distribution Switch	12	Belden	
15	Firewall	1	Belden	
16	LED Panel 65 Inch	4	Delta	
17	UPS 25 KVA	2	Libert	EXS
18	UPS 20 KVA	2	Libert	EXS
19	Rack	12	Legrand	

S. No.	Item Name	Qty	Make	Model
20	Desktop with Monitor	4	HP PC, Monitor Samsung	

5.3.2.2. Singha Dwar Viewing center and cameras for inside the Shree Jagannath Temple

S.No.	Item Name	Qty	Make	Model
Field Infrastructure				
1	Ptz Camera	6	Bosch	Auto dome IP STARLIGHT 500IR
2	Bullet Camera	230	Bosch	Dinion IP 3000i IR
3	65 Inch LED TV	2	Delta	IFPD EK655i NoVo touch 65''
5	Desktop with 22-inch monitor	1	Dell	3660/i5
6	Field Switch with 4 U Rack	55	Alcatel	6465H-P12
7	6 KVA UPS	3	Vertiv	
CCC Infrastructure				
8	Server	3	Dell	Poweredge-R760
9	Server	1	Dell	Poweredge-R750
10	Storage	2	Dell	Poweredge-R650
11	VMS	1	Bosch	VMS 21
12	24 Port Switch	1	Alcatel	6860E
13	28 Port Switch	1	Alcatel	6750M
14	Video Wall (55 inch, 3 x 3), 9 Panels	4	Delta	LW5584 MR-TC
15	Videowall Controller	1	Delta	DWCD302Z80C0154-VW controller 120p
16	Joystick	2	Bosch	KBD-UXF
17	20 KVA UPS	1	Libert	ITA 2

5.3.2.3. Puri Railway Station

S. No	Make	Model	Camera Type	Qty
1	CP Plus	CP -UNP-F4521L30-DPQ	PTZ	1
		CP-UNC-VE21ZL4C-VMDS-Q	Dome	2
		CP-UNC-TE21ZL6C-VMDS-Q	Bullet	1
		CP-UNC-TA21PLT	Bullet	10
		CP-UNC-TD41L5E-MD-J	Bullet	7
		CP-UNC-TA41PL3C-L-Y	Bullet	3
		CP-UNC-TA41PL3-D	Bullet	1
2	Alcon	AL-5001-MPC-HD4CMDK-S	Bullet	9
3	Sparsh	SC-IND22BP-I(Z)(S)	Bullet	1
4	Hikvision	DS-2CD793PF-E	Bullet	2
Total				37

5.3.2.4. SJTA Control Command Center

S. No	Item Description	Qty	Make	Model
1	6 MP Fixed Bullet Camera	51	Matrix	SATATYA CIBR80FL2 8CWP
2	4MP IP PTZ Camera with 25x Optical Zoom with 100 Mtr	1	Matrix	SATATYA PTZ2040P
3	Linux based server for CCTV-64 Channel	1	Matrix	NVR6408XP2
4	HDD 10TB Enterprise Hard disk	3	Seagate	NA
5	USB Joystick for PTZ	1	Matrix	NA

5.3.2.5. Pipili Toll Booth (Entry point from Bhubaneshwar to Puri)

S. No	Camera Type	Qty	Make
1	Camera for Vehicle Image Capturing	10	Make – Sparsh, Model - SC-IST50B
2	Camera for Number plate Capture	10	Make Sparsh, Model - SC-IM22NP-I(Z)(S)(H)

**Only Camera feeds need to be integrated for the existing infrastructure mentioned in this section as per the instruction of the authority*

** In addition to the new camera license cost, additional license for existing camera to be provisioned by the IA as required for integration.*

Note: Details of Locations along with Phase – 1 and Phase – 2 is attached in Annexure – 1 of this Volume – II (RFP).

5.3.3. Assessment, Site Survey & provisioning of field level infrastructure

Prior to the site clearance, the IA shall carry out survey of all locations including field locations, ICCC/viewing centres, route plan for laying of the passive components etc. The Authority shall be fully kept informed of the results of the survey and the amount and extent of the demolition and site clearance shall then be agreed with the Authority.

5.3.4. Physical/Civil Requirements

IA shall use industry leading practices w.r.t positioning and mounting the cameras, poles and junction boxes. Some of the checkpoints that need to be adhered to by the IA while installing / commissioning cameras are as follows:

- **Surveillance objective:** Positioning the camera such that the required field of view is being captured as finalized in field survey.
- **Camera protection:** Ensuring protection of camera from weather, physical damage, animals. For protection from animals/birds spikes may be installed.
- **Best Image & video capturing:** Proper adjustments, alignments orientation & inclination for ensuring high quality of capture with best results in video & capture.
- **Vibrations Resistance:** Ensuring well placement of pole for resistance adhering to road and other safety norms**.**
- **Collusion prevention**: Barriers around the junction box & pole foundation in case it's installed in collision prone place.
- **Branding & colour coding:** Poles and junction boxes, to warn mischief mongers against tampering with the equipment at the junction.
- **Civil work**
- IA shall be responsible for carrying out all the civil work required for setting up all the field components of the system including:
  1. Preparation of concrete foundation for Poles & cantilevers as applicable
  2. Chambers with cover at every junction box, pole and at road crossings as applicable
  3. Concrete foundation from the Ground for outdoor racks as applicable

Installation of Poles/Cantilevers/Gantry

For installing the surveillance /cameras, the IA shall provide Cantilever/ Gantry/ Uni-pole (as required) with spans, at various locations (single lane road, double lane road).

Spans need to be specified depending on the number of lanes that need to be bridged. IA shall consider additional space for lateral clearance as well as a vertical clearance height as per guidelines.

5.3.5. Junction boxes/Poles

- The IA shall mount the field sensors like the cameras, active network components, controller and UPS at all field locations on poles, cantilever, Gantry as the case may be required.
- The Junction Box needs to be appropriately sized in-order to accommodate the systems envisaged at the Junctions.
- The junction box should be designed in a way that, separate compartment shall be available for separate system (i.e. Surveillance Setup, networking switches, Controller, Mini server, Active component, UPS & Battery etc.). Each compartment shall have lock & key facility.

5.3.6. Cabling

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

5.3.7. Power Requirements

IA shall provide electricity to the cameras through the aggregation point. Since this component has dependency on approval from local authorities, it is recommended that IA plans this requirement well in advance & submits the application to the concerned electricity. The applicable permissions and charges including one-time meter fees or recurring expenditure against the utilized electricity (if applicable) shall be facilitated by the Authority. DG's fuel during O&M period for ICCC/DC/DR shall be provisioned by End user.

IA shall carry out all the electrical work required for powering all the components of the system **Electrical installation** and wiring shall conform to the electrical codes of India.

Surveillance junction box: IA shall make provisions for providing electricity to the cameras (ANPR, PTZ, and Fixed) via SJB (Surveillance Junction Box), housing the UPS/SMPS power supply, with power backup as defined in this RFP.

Wired Box cameras: IA shall provision for drawing power through PoE (Power over Ethernet), while PTZ cameras shall be powered through dedicated power cable laid separately along with STP/SFTP cable.

5.3.8. Lightning-proof measures

The IA shall comply with lightning-protection and anti-interference measures for system structure, equipment type selection, equipment earthing, power, signal cables laying. Corresponding lightning arresters shall be erected for the entrance cables of power line, video line, data transmission cables.

The Internal Surge Protection Device for Data Line Protection shall be selected as per zone of protection described in IEC 62305, 61643-11/12/21, 60364-4/5. Data line protection shall be used for security systems, server data path and other communication equipment. Data line protection shall be installed as per zone defined in IEC 62305.

5.3.9. Earthing System

- The entire applicable IT infrastructure i.e. field locations, viewing centres shall have adequate earthing measures. Further, earthing should be done as per local/state national standard in relevance with IS standard.
- Earthing should be done for the entire power system and provisioning should be there to earth UPS systems, Power distribution units, etc. Authority shall provide the necessary space required to prepare the earthing pits.
- All metallic objects on the premises that are likely to be energized by electric currents should be effectively grounded.
- There should be enough space between data and power cabling and there should not be any cross wiring of the two, in order to avoid any interference, or corruption of data.

5.3.10. Network Connectivity

IA shall ensure that implementation of Network connectivity for bandwidth services are redundant in nature, high quality, seamless connectivity to all cameras at aggregation point i.e. DC/DR.

.

Connectivity to DC/DR and CCCs, Viewing Centres etc. shall be provided with scalable capacities to allow for expansion, if required, during the Rath Yatra event may be needed. Redundant connectivity to be considered at DC and DR however the field locations to be covered with single connectivity however the IA is responsible to meet the SLAs for the same. Minimum Bandwidth to be considered at field location is minimum 5 Mbps per camera and minimum 5 GBPS bandwidth to be considered at DC at CCC. IA is required to undertake estimation of bandwidth & storage requirements considering the benchmark parameters shared below.

Sr. No.	Project Components	Consideration
1	CCTV Cameras for MKM-25 Surveillance System	• Frame Rate: 25 fps for Surveillance Cameras & 50 FPS for ANPR Cameras • Resolution: 2560x1440

IA shall provide adequate bandwidth for each camera to maintain high quality video transmission to the DC / CCCs / Viewing Centres. The actual bandwidth requirement to cater to above mentioned bandwidth & storage parameters and to meet SLAs shall be estimated by the IA and proposed in the technical bid with detailed calculations. IA shall design the networking solution in such a manner that there is no single point of failures at every location and solution meets all the uptime & and quality related SLAs.

5.3.11. Operations & Maintenance

- Authority shall assist in obtaining all necessary go ahead, legal permissions, NOC (No Objection Certificate) from various departments to execute the project. IA shall have to identify and obtain necessary legal / statutory clearances for erecting the poles and installing cameras for provisioning of the required power, etc. IA shall provide & manage all necessary paperwork to pursue permission from respective authorities. The commercial/legal fees applicable to Authority for obtaining the necessary permissions (including RoW charges) shall be facilitated / borne by the authority (if applicable).
- The IA shall provide all material required for mounting of components for cameras and other field equipment.
- IA shall also get comprehensive insurance from reputed insurance company for the project duration for all the equipment's / components installed.
- IA shall ensure all the equipment's installed in the outdoor locations are vandal proof and in case the equipment's get damaged for reasons whatsoever, it shall repair/replace the same in the specified time as per SLAs at no extra cost to the Authority.
- Preventive maintenance shall be carried out half yearly along with corrective maintenance and also when calls are placed by Authority or its designated agency. The key activities, including cleaning of equipment's/components under preventive maintenance shall be specified by the IA in his technical bid.
- During implementation, if observed that any cameras require change in the field of view / orientation, it shall be done by IA without any extra cost.

Expected Outcomes, Use cases and KPI

Automatic Number Plate Recognition System (ANPR)
Day Time

#	Location Name	Time Duration	Total Vehicle Passed	Number Plate captured in Software	Correct Number plate captured in Software	Accuracy		
						Number plate captured in Software / Total Vehicle Passed	Correct Number plate Identified / Total Number plate Captured	Correct Number plate identified / Total Vehicles pass
i.		5 Minutes						
ii.		5 Minutes						
iii.		5 Minutes						
Required Accuracy								**>= 90%**

Automatic Number Plate Recognition System (ANPR)
Night Time

#	Location Name	Time Duration	Total Vehicle Passed	Number Plate captured in Software	Correct Number plate captured in Software	Accuracy		
						Number plate captured in Software / Total Vehicle	Correct Number plate Identified / Total Number plate Captured	Correct Number plate identified / Total Vehicles pass

						Passed		
i.		5 Minutes						
ii.		5 Minutes						
iii.		5 Minutes						
Required Accuracy								**>= 70%**

Note:

- IA has to ensure proper Height of the camera, Angle of Camera, Distance of Target, Lux level, Lens size, Make of Lens, appropriate WDR, BLC, HLC etc. functionality to achieve above results.
- IA has to ensure above results in 4 wheelers as well as 2 wheelers.
- IA has to ensure above results at the speed of more than 100 km/h.

5.3.12. Integration requirements

The proposed Video Management System (VMS) shall be integrated with the existing ICCC, Viewing Center and Cameras.

5.4. Functional Requirements

The functional requirements and technical specifications provided in this RFP are indicative and carry guiding rule. The IA is free to offer products and solutions which meet requirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards & best practices adopted in the industry.

The bidders are required to make sure that the offered products are in compliance with OM No. IV-24011/22/2020-Prov-I/270 dated 26.04.2024 of Ministry of Home Affairs, Govt of India forwarding thereby MeitY's communications regarding CCTVs. This includes the followings:-(i) Gazette Notification dated 06 March, 2024 on the amendments to Public Procurement Order (PPO)-2017 for CCTV/Video Surveillance Systems for Security, Ministry of Electronics and Information Technology (IPHW DIVISION), Camera should be Cyber Security Certified by STQC ER.

The IA is encouraged to design an Optimized solution which is technically superior, innovative, proven, better in terms of functionality and is cost effective. Any specified parameters mentioned in the scope/technical requirement in the RFP may be considered if it is required for meeting proposed

and dynamic requirements during the major events like Rath Yatra. The IA is fully responsible for the specified outcome to be achieved. The IA is required to provide supporting document in the technical bid justifying the approach & design of offering the solution. The technical marking is specified in the evaluation criteria mentioned in the volume 1 of the RFP document. The response should be descriptive and cross referenced.

5.4.1. CCTV Surveillance System

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

- Information to be captured by edge devices
- Information to be managed at the Command Control Centres & Viewing Centres
- Information to be made available to different Police Personnel
- Operational Requirements
- Storage / Recording Requirements
- Other General Requirements

5.4.1.1. Information to be captured by Edge Devices

Cameras being the core of the entire Surveillance system, it is important that their selection is carefully done to ensure suitability & accuracy of the information captured on the field and is rugged, durable & compact. These cameras need to work on 24 X 7 basis and transmit quality video feeds to the centralized data center and would capture the video feeds at 25 FPS. However, Police Department/Home Department/Puri Municipal Corporation/Puri District Administration shall take the regular review of the requirements for video resolution, FPS may change to suit certain specific requirements for example, there could be a situation when certain cameras are required to be viewed at higher FPS for specific period. It is estimated that not more than 10% of the cameras would be required to be viewed at higher FPS at a given point of time. Cameras should maintain minimum bitrate of 3 Mbps for bullet/fixed camera per lens & for PTZ camera per lens to transmit quality video feed (appropriately focused, clear, un-blurred, jitter free, properly lit etc.). Packet loss should be less than 0.5%.

5.4.1.2. Information to be analysed at the Command Control Centres & Viewing Centres

The proposed Video Management System should provide a complete end-to-end solution for security surveillance application. The control center shall allow an operator to view live / recorded video from any camera on the IP Network. The combination of control center and the IP Network would create a virtual matrix, which would allow switching of video streams around the system. Not all the cameras would be simultaneously viewed at Command Control Center or at Viewing Centres. Police personnel shall have following access to the video feeds of the cameras of their jurisdiction:

- Viewing rights to all the live Camera Feeds
- Viewing rights to the stored feeds
- Access to view Alerts / Exceptions / Triggers raised

- Trail Report is expected to have geolocations, direction of camera and tracking route of specific person / object / vehicle for a specific period / location
- Personalized Dashboard (depending upon grade of officer)
- Accessibility to advanced analytics on live & recorded footages
- Provide search of recorded video. Advanced search should be possible based on various filters like alarm / event, area, camera, etc.

5.4.1.3. Storage / Recording Requirements

It is proposed that the storage solution is modular enough to ensure compliance to the changes in storage / recording policy, to be evolved upon initial deployment of the system. Following storage requirements are proposed for the project:

- **The storage solution proposed is that the video feeds would be available for 30 days**. After 30 days, the video feeds would be overwritten unless it is flagged or marked by the Police / Stakeholder Department for investigation or any other purpose. The video feeds of all relevant cameras capturing the incident or flagged in question would be stored until the Police deem it good for deletion.
- The critical events/incidents video is required to be stored for 90 Days.
- For incidents that are flagged by the Police or any stakeholder department, the video of the relevant portion from all relevant cameras should be stored/archived separately for investigation purposes and a committee at Police Department can decide when this video feed can be deleted.

a. Audit trail of the system to be maintained on permanent basis / as per the backup policy defined.
b. Retrieval time for any data stored should comply with the defined service level agreements.
c. The Recording Servers / System, once configured, shall run independently of the Video Management system and continue to operate if the Management system is off-line.
d. The system shall support the use of separate networks, VLANs or switches for connecting the cameras to the recording servers to provide physical network separation from the clients and facilitate the use of static IP addresses for the devices.
e. The system shall support H.265, H.264 with better compression, H.264/H.265 formats for all IP cameras connected to the system.
f. The system shall record the native frame rate and resolution supplied by the camera or as configured by the operator from the System Administration Server.
g. The system should not limit amount of storage to be allocated for each connected device.
h. The on-line archiving capability shall be transparent and allow Clients to browse and archive recordings without the need to restore the archive video to a local hard drive for access.
i. The system shall allow for the frame rate, bit rate and resolution of each camera to be configured independently for recording. The system shall allow the user to configure groups of cameras with the same frame rate, bit rate and resolution for efficient set-up of multiple cameras simultaneously.
j. The system shall support Archiving or the automatic transfer of recordings from a camera's default database to another location on a time-programmable basis without the need for user

action or initiation of the archiving process. Archiving shall allow the duration of the camera's recordings to exceed the camera's default database capacity. Archives shall be located on either the recording server or on a connected network drive. If the storage area on a network drive becomes unavailable for recording, the system should have the ability to trigger actions such as the automatic sending of email alerts to necessary personnel.

k. Bandwidth optimization
    - The Recording Server / System shall offer different codec (H.265, H.264 with better compression, H.264) and video resolution options for managing the bandwidth utilization for live viewing on the Client systems.
    - From the Client systems, the user shall have the option of having video images continually streamed or only updated on motion to conserve bandwidth between the Client systems and the Recording Server.
    - The bidder is expected to calculate the bandwidth and storage requirement according to below table:

Parameter	PTZ Camera	Fixed / Bullet / ANPR Cameras
Resolution	2560 X 1440	2560 X 1440
Minimum Bitrate	4 Mega Pixel 25FPS or better 2 Mega Pixel 60FPS or better	3 Mbps or higher
FPS	25 FPS	25 for Fixed / Bullet Cameras 50 @2 MP for ANPR Cameras

l. The Recording Server / System shall support IP cameras from various manufacturers.

m. The Recording Server / System shall support the PTZ protocols of the supported devices listed by the PTZ's camera OEMs.

n. Failover Support**:**
    - The system shall support automatic failover for Recording Servers, this functionality shall be accomplished by Failover Server as a standby unit that shall take over if one of a group of designated Recording Servers fails. Recordings shall be synchronized back to the original Recording Server once it is back online.
    - The system shall support multiple Failover Servers for a group of Recording Servers.

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

5.4.1.4. Other General Requirements

Management / Integration functionality

a. The Surveillance System shall be a fully distributed solution, designed for large multi-site and multiple server installations requiring 24/7 surveillance. The solution shall offer centralized management of all devices, servers and users.
b. The Surveillance System should not have any limit on the number of cameras to be connected for Surveillance, Monitoring and recording. Any increase in the no. of cameras should be possible by augmentation of Hardware components and camera licenses.
c. The Surveillance System shall support distributed viewing of any camera in the system using Video walls or big screen displays.
d. The Surveillance System shall support alarm management. The alarm management shall allow for the continuous monitoring of the operational status and event-triggered alarms from system servers, cameras and other external devices.
e. It should be possible to integrate the Surveillance System with 3rd-party software, to enable the users to develop customized applications for enhancing the use of video surveillance solution. For e.g. Integrating alarm management to initiate SMS, E-Mail, VoIP call etc.
f. The Management system shall store the overall network elements configuration in central database, either on the management server computer or on a separate DB Server on the network.

System Administration functionality

a. The System Administration Server shall provide a feature-rich administration client for system configuration and day-to-day administration of the system.
b. The System Administration Server shall support different logs related to the Management Server.
    - The System Log
    - The Audit Log
    - The Alert Log
    - The Event Log
c. Rules- The system shall support the use of rules to determine when specific actions occur. Rules shall define what actions shall be carried out under specific conditions. The system shall support rule-initiated actions such as:
    - Start and stop recording.
    - Set non-default live frame rate.
    - Set non-default recording rate.
    - Start and stop PTZ patrolling.
    - Send notifications via email.
    - Pop-up video on designated Client Monitor recipients.

Client system

The Client system shall provide remote users with rich functionality and features as described below.

- Viewing live video from cameras on the surveillance system
- Browsing recordings from storage systems
- Creating and switching between multiple of views.
- Viewing video from selected cameras in greater magnification and/or higher quality in a designated hotspot.
- Controlling PTZ cameras.
- Using digital zoom on live as well as recorded video.
- Using sound notifications for attracting attention to detected motion or events.
- Getting quick overview of sequences with detected motion.
- Getting quick overviews of detected alerts or events.
- Quickly searching selected areas of video recording for motion (also known as Smart Search).

Remote Web Client

- The web-based remote client shall offer live view of minimum 128 cameras, including PTZ control (If applicable) and event / output activation. The Playback function shall give the user concurrent playback of multiple recorded videos with date, alert sequence or time searching.
- User Authentication: The Remote Client shall support logon using the username and password credentials.

Matrix Monitor

- Matrix Monitor – The Matrix Monitor feature shall allow distributed viewing of multiple cameras on the system on any monitor.
- The Matrix Monitor feature shall access the H.265 stream from the connected camera directly and not sourced through the recording server.

Mobile Client

- The bidder shall be required to provide a standardised Mobile Application to integrate smart phones and tablets for 2-way communication with the Video Management System in a secure manner. It will be responsibility of IA to configure such tablets / Smartphone with the Surveillance System and ensure that all the necessary access is given to these mobile users.
- Communication with mobile client and server shall be encrypted with Digital Certificate/VPN.

Alarm Management Module

- The alarm management module shall allow for continuous monitoring of the operational status and event-triggered alarms from various system servers,

cameras and other devices. The alarm management module shall provide a real-time overview of alarm status or technical problems while allowing for immediate visual verification and troubleshooting.

- The alarm management module shall provide interface and navigational tools through the client including;
  a. Graphical overview of the operational status and alarms from servers, network cameras and external devices including motion detectors and access control systems.
  b. Intuitive navigation using a map-based, hierarchical structure with hyperlinks to other maps, servers and devices or through a tree-view format.
  c. The module shall include flexible access rights and allow each user to be assigned several roles where each shall define access rights to cameras.
  d. Basic VMS should be capable to accept third party generated events / triggers.

Other Miscellaneous Requirements

a. System should have a facility to create CDs / DVDs or other storage media for submission to Judiciary, which can be treated evidence for legal matters. Such storage media creation should be tampered proof and IA to provide appropriate technology so that integrity and quality of evidence is maintained as per requirements of the judiciary and the evidence is considered as un-tampered in the court of law. Such provision should be available either in VMS proposed or through suitable additional hardware/software implementation. IA is required to specify any additional hardware / software required for this purpose & the same can be listed in BOM and bidder has to provide the same at the no-additional cost to the purchaser. IA will also prepare the guideline document to be followed by the Police Personnel for the retrieval of Video / images from the CCTV System so as to maintain integrity of the evidence. Such a guideline document should include methods of retrieval of data, checklist to be followed and flowchart of the entire process to be followed.
b. All the systems proposed, and operationalization of Video Management System should comply with requirements of IT Acts.

5.4.1.5. Integration with existing ICCC System

As mentioned in section 4.3 in Volume – II of this RFP.

5.5. Video Management System (VMS)

1. Video Management System (VMS) shall be used for centralized management of all field camera devices, video servers and client users.

2. VMS shall be deployed in a clustered server environment or support inbuilt mechanism for high availability and failover. (No loss of data/recording during failure of directory/recording servers.)
3. VMS shall support a flexible rule-based system driven by schedules and events.
4. VMS shall be supported for fully distributed solution for monitoring and control function, designed for limitless multi-site and multiple server installations requiring 24/7 surveillance with support for devices from different vendors.
5. VMS shall support ONVIF compliant internet protocol (IP) cameras from different vendors.
6. The offered VMS must have Open Network Video Interface Forum (ONVIF) Profile S or better compliance.
7. VMS shall be enabled for any standard storage technologies and video wall system integration.
8. VMS shall be capable of being deployed in a virtualized server environment without loss of any functionality.
9. All CCTV cameras locations shall be overlaid in graphical map in the VMS Graphical User Interface (GUI). The cameras selection for viewing shall be possible via clicking on the camera location on the graphical map. The graphical map shall be of high-resolution enabling operator to zoom-in for specific location while selecting a camera for viewing.
10. VMS shall have an administrator interface to set system parameters, manage codecs, manage permissions and manage storage.
11. Day to day control of cameras and monitoring on client workstations shall be controlled through the VMS administrator interface.
12. Whilst live control and monitoring is the primary activity of the monitoring workstations, video replay shall also be accommodated on the GUI for general review and for pre- and post-alarm recording display.
13. The solution design for the VMS shall provide flexible video signal compression, display, storage and retrieval.
14. VMS shall support H.264, H.265 or better video compression.
15. All CCTV camera video signal inputs to the system shall be provided to various command control center (s), viewing center etc., and the transmission medium used shall best suit the relative camera deployments and access to the CCTV Network.
16. VMS client shall have the capability to work with multi-monitor workstations. It shall be capable of displaying videos in up to three (3) monitors simultaneously.
17. VMS shall be capable of transferring recorded images to recordable media (such as CD/DVD and/or tapes) in tamper evident and auditable form. All standard formats shall be supported including, but not limited to:
    - AVI/WMV/MP4 files
    - JPEG Images
    - WAV audio
    - Other non-proprietary format
18. All video streams shall be available in real-time and at full resolution. Resolution and other related parameters shall be configurable by the administrator in order to provide for network constraints.

19. The VMS shall support field sensor settings. Each channel configured in the VMS shall have an individual setup for the following settings, the specific settings shall be determined according to the encoding device:
    - Resolution
    - Frame Rate
    - Bit Rate
20. The VMS shall support bookmarking the videos. Thus, allowing the users to mark incidents on live and/or playback video streams.
21. The VMS shall support the following operations:
    - Adding an IP device
    - Updating an IP device
    - Updating basic device parameters
    - Adding/removing channels
    - Adding/removing output signals
    - Updating an IP channel
    - Removing an IP device
    - Enabling/disabling an IP channel
    - Refreshing an IP device (in case of firmware upgrade)
    - Multicast at multiple aggregation points
    - PTZ functions
22. The VMS shall support retrieving data from edge storage. Thus, when a lost or broken connection is restored, it shall be possible to retrieve the video from SD card and store it on central storage. System should support to view the recordings available over cameras local storage device (such as an SD card) and copy them to the server.
23. VMS shall support automatic failover for recording.
24. VMS should also support dual recording or mirroring if required.
25. VMS shall support manual failover for maintenance purpose.
26. VMS shall support access and view of cameras and views on a smartphone or a tablet (a mobile device).
27. VMS shall support integration with the ANPR application
28. VMS shall integrate with proposed video analytic applications, & video summarization application so that the user of (video analytic application, & video summarization application) can access live/recorded video feed seamlessly.
29. VMS shall be able to accept alerts from video analytics built into the cameras, other third-party systems such as Artificial Intelligence based video analytics & video Summarization system etc.
30. VMS shall support alarm management module that shall allow for continuous monitoring of the operational status and event-triggered alarms from various system servers, cameras and other devices. The alarm management module shall provide a real-time overview of alarm status or technical problems while allowing for immediate visual verification and troubleshooting. Alarm Filtering option should be available, for example, it should be possible to “silence” alarms for a desired period.

31. VMS should not have any limit on the number of cameras to be connected for Surveillance, Monitoring and Recording. Any increase in the no. of cameras should be possible by augmentation of Hardware components & camera license.
32. VMS shall support distributed viewing of any camera in the system using Video walls or big screen displays.
33. It should be possible to integrate the VMS with 3rd-party software, to enable the users to develop customized applications for enhancing the use of video surveillance solution. For e.g., integrating alarm management to initiate SMS, E-Mail etc.
34. Certifications - ISO 9001:2015, 27001:2013, ISO 14001:2015, ISO 45001:2018,ISO 27017:2015 and CMMI Level – 3
35. The Intellectual Property Rights & Source Code of Offered Video Management Software (VMS) must not reside in a Country that is sharing Land Border with India.
36. The Video Management Software (VMS) Offered should not be Developed/manufactured by an entity in which the majority shareholding of the entity is from a Country sharing a Land Border with India.
37. OEM shall provide a Declaration about the intellectual property rights & Source Code as a Documentary Evidence & Copyrights Certificate.
38. The OEM who is Claiming to be Make in India OEM with Local Content greater than 50%, then their Intellectual Property Rights (IPR) & Source Code must Reside in India only. Documentary Evidence to be Provided.
39. The Proposed Video Management Software (VMS) Application should have undergone Audit as per OWASP Top 10 Security Risks from STQC. A Security Test Report/Certificate from STQC to be Submitted as a Documentary Evidence/Proof.
40. The offered VMS must be cyber security certified with FIPS-140-2 & FIPS 140-3 encryption from Cert-IN Empanelled Auditor for mitigating cyber security risk.
41. The system shall support the use of rules to determine when specific actions occur. Rules shall define what actions shall be carried out under specific conditions. The system shall support rule-initiated actions such as:

    - Start and stop recording
    - Set non-default live frame rate
    - Send notifications via email
    - Pop-up video on designated Client Monitor recipients

5.5.1. Automatic Number Plate Recognition (ANPR) System

#	Parameter	Minimum Requirements
1.	General	The entire ANPR process shall be performed at the lane location in real-time. The information captured of the plate alphanumeric, date-time, and any other information required shall be completed in approximately a few milliseconds. This information shall be transmitted to the Control Room for further processing if necessary, and/or stored at the lane for later retrieval.
2.	Lane Coverage	Each camera system covers at least 1 lane having width of 3.5 meter or more.
3.	Detection Zone	15 m to 20 m for ANPR data
4.	Vehicle Detection and Video Capture Module	The System shall automatically detect the license plate of all vehicles in the camera view in real time using video detection and activates license plate recognition software.
5.	Optical Character Recognition	The system shall perform OCR (optical character recognition) of the license plate characters in real time. (English alpha-numeric characters in standard fonts). OCR accuracy shall be at least 90% during daytime and 70% during night-time for standard plates. System is 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. The system is robust to variation in License Plates in terms of font, size, contrast and colour.
6.	Network	Connectivity from site to control room shall be through proper network and local storage should be provided to account for any data loss.

#	Parameter	Minimum Requirements
7.	Data capture and transfer	The OCR data of all vehicles along with the JPEG image of the vehicle etc. shall be automatically transferred immediately to the nominated server in the Control Room. Each vehicle record shall be a single file and shall contain, as a minimum, an ASCII header that contains the following: a) vehicle registration number b) date and time that the vehicle is identified. c) ANPR site location,
8.	Alert Generation	On successful recognition of the number plate, system shall be able to generate automatic alarm to alert the control room for vehicles which have been marked as "Wanted", "Suspicious", "Stolen", etc.
9.	Data Storage	The System shall store JPEG image of vehicle and license plate into a database management system along with date timestamp and site location details.
10.	Vehicle Classification	The System shall have option of identification of Colour, Make of vehicles along with count and classification
11.	Data Retrieval and Reports	The system shall enable easy and quick retrieval of snapshots, video and other data for post incident analysis and investigations. Database search could be using criteria like date, time, location and vehicle number. The system shall be able to generate suitable MIS reports as desired by the user. The system shall also provide advanced and smart searching facility of License plates from the database.
12.	Third Party System Integration	The system should be integrated with the proposed Video Management System and existing ICCC application.

6. Parking Surveillance System

6.1. Overview

Parking Surveillance being a critical component of the Integrated City Surveillance System (ICSS), it is important that all sensing and monitoring devices installed at various parking locations across Puri are selected and engineered with utmost care, ensuring suitability, durability, accuracy and reliability of the information captured from the field. These devices shall include Fixed Cameras, PTZ Cameras, ANPR Cameras, IR Illumination devices, active networking components, outdoor junction boxes, poles, UPS systems and associated cabling infrastructure.

The cameras installed at all parking locations shall work on a **24 × 7 basis** and shall continuously transmit high-quality video feeds to the ICCC at JBPC, as well as to any designated viewing centres as approved by the Authority. All Fixed and PTZ cameras deployed in parking zones shall be capable of capturing video at **25 FPS**, while ANPR cameras shall support **higher FPS (typically 50 FPS)** to ensure accurate recognition of number plates under varying lighting, speed and traffic conditions.

The Authority / Police Department may periodically undertake a detailed review of the video resolution, FPS, bitrate and related parameters for specific parking locations and may modify these requirements to suit dynamic and event-driven operational needs. For example, during peak traffic conditions, VIP visits or large festivals such as the Jagannath Rath Yatra, it may be necessary to operate certain cameras at higher FPS or higher bitrate for improved clarity and real-time monitoring.

Parking locations across Puri—such as Talabania, JBPC Parking, Old JBPC Parking, Loknath Parking, Sonar Bangla Parking, Gadadhar School Parking, Helipad Parking, Jatrika Parking, Saha College Parking, Matiota Playground Parking, Blue Lily Parking, Digabareni Multilevel Parking, Hygienic Fish Market Parking, and temporary parking created during Rath Yatra—are highly dynamic and operationally sensitive environments. These locations experience high vehicular load, irregular movement patterns, dense pedestrian flow, noise, dust, humidity, sudden lighting changes and significant congestion during peak events. Therefore, it is important that the surveillance system for these parking zones is rugged, compact, tamper-proof, vandal-resistant and capable of performing reliably under varying environmental and operational conditions.

6.2. Key Issues

The IA shall be required to consider the following key issues and constraints while designing and implementing the Parking Surveillance System across all permanent and temporary parking locations:

- **Need to support both permanent and event-based parking deployments**

All the identified parking locations must be fully covered under Phase-1. Several parking locations operate throughout the year, while others are activated only during events like Rath Yatra. The IA

shall ensure that the surveillance solution provides seamless coverage for both types of parking facilities without compromising system performance, reliability and data quality.

- **High variability in parking behaviour and vehicle density**

Parking areas experience unpredictable traffic flow patterns, sudden crowding, irregular lane formation, and high turnover of vehicles. The IA shall ensure that camera placement, angle, orientation, field-of-view, zoom settings and illumination are optimized to capture clear video under both normal and peak load conditions.

- **Ensuring accurate monitoring of vehicle entry and exit**

Parking zones require accurate identification of vehicles entering and exiting the premises. The IA shall install ANPR cameras, PTZ cameras and Fixed cameras to ensure that all license plates, vehicle types and directional movements are captured clearly. The system shall support identification of suspicious, stolen or wanted vehicles through integration with the central ANPR watchlist.

- **Environmental and operational challenges**

Parking areas often face dust, humidity, salt-laden air (near coastal areas), sudden downpours, night-time darkness, vehicle-induced vibrations and potential vandalism. The IA shall ensure that all surveillance devices deployed are weatherproof, corrosion-resistant, vibration-resistant and vandal-resistant.

- **Integration with ICCC, Analytics Engines and Viewing Centres**

The IA shall ensure that all parking surveillance feeds—video, ANPR results, metadata and alerts—are fully integrated with:

- ICCC at JBPC
- Existing SJTA ICCC (as required)
- Viewing Centre at Singhdwar Police Station
- Central VMS, Analytics Platform and ANPR Engine

- **Preventing obstruction of parking operations**

The IA shall ensure that poles, junction boxes, cabling ducts, foundations, conduits and other civil structures do not obstruct vehicle movement, pedestrian flow or emergency exits within parking premises.

- **Temporary parking sites during Rath Yatra and other major events**

The IA shall ensure the deployment of portable and rapidly deployable surveillance infrastructure for temporary parking areas created during Rath Yatra. Such infrastructure shall include portable poles, portable junction boxes, temporary OFC/Wireless connectivity, portable UPS systems and quickly deployable cameras.

6.3. Scope of Work

6.3.1. General Scope

The Parking Surveillance System shall be implemented in Phase-1, covering **all permanent and temporary parking locations** identified by the Authority. The system shall provide comprehensive monitoring of vehicular movement, pedestrian flow, security incidents, abnormal behaviour, and entry-exit activities across all parking zones.

The IA shall undertake design, supply, installation, testing, commissioning, integration, training and maintenance of all parking-related surveillance infrastructure. The solution shall include cameras, poles, junction boxes, switching infrastructure, UPS systems, civil works, network connectivity, storage, analytics integration and SOP documentation.

The Parking Surveillance System shall operate seamlessly with the rest of the ICSS, providing real-time visibility, alerts and actionable information for law-enforcement agencies and parking management personnel.

6.3.1.1. Phase-1 Outcomes (All Parking)

1. Complete Surveillance Coverage of All Identified Parking Locations
The IA shall ensure complete surveillance coverage of all permanent and temporary parking locations identified in the RFP and DPR including but not limited to Talabania, JBPC Parking, Old JBPC, Loknath, Gadadhar School, Jatrika, Nalifield, Helipad, Sonar Bangla, Blue Lily, Digabareni Multilevel Parking, Matiota Playground, Saha College, Hygienic Fish Market Parking, and any other parking zones designated by the Authority.

2. Installation of Camera Infrastructure

- The IA shall ensure installation of Fixed Bullet Cameras for monitoring entrances, exits, periphery and vehicle rows.
- The IA shall ensure installation of PTZ Cameras for wide-area coverage, zoom tracking and incident monitoring.
- The IA shall ensure installation of ANPR Cameras at all vehicle entry and exit points to capture license plate information reliably during day and night.
- The IA shall ensure installation of IR Illuminators wherever lux levels fall below required thresholds.

3. Deployment of Poles, Junction Boxes and Mounting Infrastructure

- The IA shall ensure providing and erecting 6 m high galvanized octagonal poles with lightning arresters and GI cantilever arms.

- The IA shall ensure installation of outdoor utility cabinets / junction boxes with separate compartments for surveillance, networking, UPS and power equipment.
- Ensuring tamper-resistant installation to prevent vandalism and environmental damage.

4. Networking and Switching Infrastructure

- The IA shall ensure installation of industrial-grade switches suitable for outdoor parking environments.
- The IA shall ensure laying of OFC, Cat6, power cables, conduits and patch panels.
- The IA shall ensure proper splicing, jointing, termination and labelling of all cables.
- The IA shall ensure providing redundant connectivity from parking sites to the ICCC.

5. Power and UPS Infrastructure

- The IA shall ensure installation of online UPS of minimum 2 KVA capacity with at least 1-hour battery backup for each parking cluster.
- The IA shall ensure all electrical installation shall comply with national electrical codes.
- The IA shall ensure proper earthing and lightning protection is provided for all parking sites.

6. Civil Works

- The IA shall ensure construction of concrete foundations for poles and junction boxes.
- The IA shall ensure trenching, ducting, backfilling and compaction as per standards.
- The IA shall ensure restoration of parking areas after installation activities.

7. Integration with ICCC, SJTA ICCC and Viewing Centres

- The IA shall ensure complete integration of all parking surveillance feeds—live, recorded, metadata and analytics with:
- ICCC at JBPC
- Existing SJTA ICCC (if required)
- Viewing Centre at Singhdwar Police Station
- Centralized VMS, Analytics and ANPR modules

6.3.1.2. Operations & Maintenance

1. The IA shall ensure Preventive Maintenance is carried out once every month at each parking location, including camera cleaning, tightening, power checks, UPS health verification and network testing.
2. The IA shall ensure corrective maintenance is carried out within SLA timelines; damaged equipment must be replaced at **no extra cost** to the Authority.
3. The IA shall ensure ANPR cameras continue to meet accuracy benchmarks through regular calibration.

4. The IA shall ensure all poles, junction boxes, UPS systems and switches remain operational, safe and tamper-free.
5. The IA shall ensure documentation such as maintenance logs, incident reports and asset registers is updated regularly and submitted for review.

6. In addition to Phase-1 outcomes, the IA shall ensure the following throughout the 5-year O&M period:
    a. **Legal Permissions:** The IA shall ensure timely coordination for permissions for pole erection, road-cutting, cabling and power supply.
    b. **Material and Mounting:** The IA shall ensure that all mounting accessories, clamps, bolts, brackets, conduits and holding structures are supplied and installed.
    c. **Comprehensive Insurance:** The IA shall ensure comprehensive insurance coverage for all parking surveillance equipment.
    d. **Vandalism Handling:** The IA shall ensure replacement or repair of damaged equipment at no extra cost to the Authority, within SLA timelines.
    e. **Preventive Maintenance:** The IA shall ensure monthly preventive maintenance, including:
        - Cleaning of cameras and housing
        - Tightening of mounts and poles
        - Checking earthing and surge devices
        - Verifying video quality, bitrate and FPS
        - Testing ANPR accuracy
        - Testing UPS backup duration
    f. **Corrective Maintenance:** The IA shall ensure resolution of faults within the SLA timelines.
    g. **Field of View Adjustments:** The IA shall ensure that any camera field-of-view or angle change required during implementation or operation is carried out without additional cost.

6.4. Physical / Civil Requirements for Parking Surveillance System

The IA shall use industry-leading practices with respect to the positioning and mounting of cameras, poles, junction boxes, UPS units and supporting hardware across all parking locations. Parking areas have unique challenges such as large open spaces, multi-directional vehicle movement, high pedestrian flow, dust, humidity, rainwater accumulation, and potential risks from parked or moving vehicles. Therefore, the IA shall ensure that all physical installation work is carried out in strict compliance with safety, operational and aesthetic standards defined by the Authority.

The following checkpoints shall be adhered to by the IA while installing and commissioning equipment in permanent and temporary parking sites:

a. **Surveillance Objective:** The IA shall ensure that cameras are positioned in such a manner that the required field of view—covering entry/exit lanes, parking rows, peripheral boundaries, pedestrian movement corridors, ticketing booths (if any), vehicle holding zones and blind spots—is captured clearly as finalized during the field survey. The IA shall ensure that parking-specific challenges such as irregular vehicle alignment, varying parking angles, temporary congestion, and night-time crowding are fully addressed through proper camera positioning.
b. **Camera Protection:** The IA shall ensure that all cameras deployed in parking areas are protected from extreme weather, dust, salt-laden winds, physical damage, animal interference. For protection against birds and monkeys, the IA shall install spikes or similar deterrent systems on poles and camera mounts. Adequate water drainage and splash protection shall be ensured where cameras are placed near open areas prone to flooding or heavy splashing during monsoons.
c. **Best Image and Video Capturing:** The IA shall ensure proper adjustment, alignment, inclination and calibration of cameras to achieve the highest image quality under day and night conditions. The IA shall ensure proper lux-level assessment, IR illumination alignment, minimization of glare from vehicle headlights, and prevention of over-exposure or shadow zones. The IA shall ensure that ANPR cameras are installed at optimal height, angle, distance and inclination to meet accuracy benchmarks.
d. **Vibration Resistance:** Parking areas experience vehicle-induced vibrations, especially near entry gates, internal lanes and loading/unloading points. The IA shall ensure that poles and mounts are firmly installed with adequate foundation depth, reinforcement and anchoring to ensure resistance to vibrations. The IA shall ensure that pole installation adheres to IRC and local safety norms.
e. **Collision Prevention:** Since poles and junction boxes installed in parking zones may be vulnerable to accidental vehicle collisions, the IA shall ensure the installation of protective barriers, bollards or guard rails around pole foundations and junction boxes located in vehicle movement zones.
f. **Branding & Colour Coding:** The IA shall ensure that poles, junction boxes, UPS cabinets and conduits installed in parking premises are properly color-coded and branded as per Authority guidelines to discourage tampering and to provide visibility to the public.
g. **Civil Works:** The IA shall be responsible for carrying out all civil works required for installing the field components of the Parking Surveillance System. These civil works shall include:
    - Preparation of concrete foundations for poles, cantilevers and junction boxes
    - Construction of chambers with covers at junction box locations and road/crossing points
    - PCC bases for outdoor racks or UPS cabinets
    - Ducting, trenching, excavation, compaction and backfilling as required
    - Restoration of parking pavement, tiles, footpaths or ground surfaces after installation
h. **Installation of Poles / Cantilevers:** The IA shall provide poles, cantilevers or gantry structures as required to mount parking surveillance cameras. The IA shall ensure that

clearance height, lateral clearance, infrastructure spacing and vehicle safety norms are fully adhered to. The IA shall ensure that no pole or structure obstructs parking lanes or emergency vehicle movement.

6.5. Junction Boxes / Poles:

1. **Mounting of Field Sensors:** The IA shall mount the field sensors such as Fixed Cameras, PTZ Cameras, ANPR Cameras, industrial switches, controllers and UPS units at designated locations on poles, cantilevers or existing infrastructure, as applicable to the specific parking.
2. **Junction Box Sizing and Segregation:** The IA shall ensure that each junction box is appropriately sized to accommodate all components envisaged for parking surveillance, such as network switches, power supplies, surge protection devices and UPS modules. The IA shall ensure that each junction box has clearly segregated compartments for surveillance, networking, power and battery components. Each compartment shall be provided with an independent locking mechanism.
3. **Weatherproof and Vandal-Proof Enclosures:** The IA shall ensure that all junction boxes installed in parking areas are IP-rated, rust-proof, vandal-proof and protected against environmental exposure, water ingress and tampering.

6.6. Cabling Requirements

1. **Standardized Cabling:** The IA shall provide standardized cabling for all devices and subsystems in the parking zones. The IA shall ensure that high-quality Cat6/STP cables, OFC cables and power cables are used in compliance with the required specifications.
2. **Cable Routing:** The IA shall ensure that cables from pole-mounted devices are routed through the inside of the pole wherever possible, and then through underground ducts to the junction box or outstation cabinet, thereby preventing cable exposure, tampering or accidental cuts.
3. **Cable Labelling:** The IA shall ensure that all cables—data, power, OFC, patch cords and connectors—are clearly labelled with indelible markers and identification tags suitable for long-term maintenance.
4. **Compliance with Standards:** The IA shall ensure that all cabling work adheres to relevant BIS standards, electrical standards and industry best practices. All cabling layouts, routing diagrams and ducting details shall be documented in the cable plan.

6.7. Power Requirements

The IA shall ensure that all parking surveillance components receive stable and uninterrupted power.

Electrical Permissions: Since power supply to poles, junction boxes and parking infrastructure may require coordination with local electrical departments, the IA shall ensure timely submission of applications and documentation. The Authority shall facilitate statutory approvals and fees wherever applicable.

Power Supply Architecture: The IA shall ensure:

- Power routing through Surveillance Junction Boxes (SJBs)
- UPS/SMPS provisioning for backup
- Separate power cables for PTZ cameras as required
- PoE or PoE+ powering of Fixed Cameras and ANPR Cameras

Installation Standards

The IA shall ensure that electrical installation and wiring comply with Indian electrical codes, and that all safety norms are followed. The IA shall also ensure proper circuit protection, MCB installation and load distribution.

6.8. Lightning-Proof Measures

The IA shall ensure compliance with lightning-protection and anti-interference requirements for all equipment, following IEC 62305, IEC 61643 and relevant IS standards. The IA shall ensure installation of:

- Lightning arresters for power and data cables
- Surge Protection Devices (SPD) for outdoor field equipment
- Data line protection devices for network paths
- Proper zonal protection as per IEC guidelines

6.9. Earthing System:

- The IA shall ensure proper earthing for all field equipment, poles, UPS systems and power components
- The IA shall ensure installation of earth pits as per IS standards
- The IA shall ensure separation between data and power cabling to avoid interference
- The IA shall ensure effective grounding of all metallic enclosures and components

6.10. Network Connectivity

The IA shall ensure that network connectivity for all parking locations is redundant, high-quality and capable of supporting the required FPS, resolution and bitrate for all cameras.
The IA shall ensure:

- The IA shall ensure minimum 3 Mbps for Fixed and ANPR cameras

- The IA shall ensure minimum 7 Mbps for PTZ cameras
- The IA shall ensure support for 25 FPS (Fixed/PTZ) and 50 FPS (ANPR)
- The IA shall ensure packet loss < 0.5%
- The IA shall ensure redundant links from parking locations to ICCC
- The IA shall ensure sufficient bandwidth provisioning for peak traffic during Rath Yatra
- The IA shall estimate bandwidth & storage requirements and provide detailed calculations in the technical bid.

6.11. Operations & Maintenance (Full Details)

In addition to Phase-1 outcomes, the IA shall ensure the following throughout the 5-year O&M period:

a. **Legal Permissions:** The IA shall ensure timely coordination for permissions for pole erection, road-cutting, cabling and power supply.
b. **Material and Mounting:** The IA shall ensure that all mounting accessories, clamps, bolts, brackets, conduits and holding structures are supplied and installed.
c. **Comprehensive Insurance:** The IA shall ensure comprehensive insurance coverage for all parking surveillance equipment.
d. **Vandalism Handling:** The IA shall ensure replacement or repair of damaged equipment at no extra cost to the Authority, within SLA timelines.
e. **Preventive Maintenance:** The IA shall ensure monthly preventive maintenance, including:
    - Cleaning of cameras and housing
    - Tightening of mounts and poles
    - Checking earthing and surge devices
    - Verifying video quality, bitrate and FPS
    - Testing ANPR accuracy
    - Testing UPS backup duration
f. **Corrective Maintenance:** The IA shall ensure resolution of faults within the SLA timelines.
g. **Field of View Adjustments:** The IA shall ensure that any camera field-of-view or angle change required during implementation or operation is carried out without additional cost.

6.12. Parking Video Analytics

The Parking Surveillance System shall be complemented with an intelligent video analytics layer that shall enable real-time monitoring, incident detection, automated alerting, historical analysis, vehicle behaviour assessment and operational insights across all permanent and temporary parking locations of Puri. The analytics solution shall form an integral part of the ICSS and shall be fully integrated with the Video Management System (VMS), the ANPR engine, the ICCC dashboard and all designated viewing centres.

Analytics is especially important in parking environments due to dense vehicular movement, irregular parking patterns, frequent pedestrian interaction, night-time congestion and heightened security concerns during major events like Rath Yatra. Therefore, **the IA shall ensure** the deployment of robust, accurate and scalable analytics models capable of detecting events, identifying risk situations and supporting the decision-making process of law enforcement and parking management agencies.

The Authority may periodically review analytics thresholds, detection accuracy, event types and alerting configurations, and may instruct the IA to modify or augment the analytics modules to suit specific operational requirements. Such dynamic upgradation must be supported by the offered system without requiring major architectural changes.

6.13. Functional Requirements for Parking Analytics

The functional requirements for Parking Analytics shall include but not be limited to the following categories. All analytics shall be available on both live and recorded video streams wherever applicable.

a. **Information to be captured by Edge Devices:** The IA shall ensure that cameras installed at parking locations provide high-quality input for analytics, including clear visibility of vehicles, pedestrians, number plates, parking rows, periphery zones and entry–exit lanes. The IA shall ensure optimal camera positioning, angle, illumination, bit rate, FPS and exposure settings to support analytics accuracy.
b. **Information to be analysed at ICCC and Viewing Centres:** The IA shall ensure that analytics events from parking areas are processed at the ICCC central analytics server, enabling operators to:
    - View real-time alerts from parking locations
    - Overlay events on GIS-based maps
    - Retrieve analytical data on historical trends
    - Access dashboards showing parking occupancy, crowd surges, suspicious vehicle detection and incident alerts
    - Generate behaviour and pattern analysis reports
    - The IA shall ensure that all operators have appropriate access rights based on their role.
c. **Information available to Police and Parking Management Personnel:** The IA shall ensure that designated users from Police, Parking Authorities, SJTA and District Administration can view:
    - Live parking occupancy indicators
    - Alerts related to suspicious vehicles
    - Unusual behaviour alerts (loitering, abandoned vehicles, reverse movement, wrong parking)
    - ANPR-based vehicle identification
    - Traffic congestion inside parking
    - Emergency evacuation route status

- Pedestrian movement anomalies

d. **Operational Requirements:** The IA shall ensure the analytics system supports:

- Real-time alerts
- Configurable thresholds
- Event bookmarking
- Integration with incident management workflow
- Snapshot and video export linked with analytics events
- Audit trails for all alerts and incidents

e. **Storage and Recording Requirements:** The IA shall ensure:

- Storage of analytics metadata along with video
- Ability to retrieve event-based clips instantly
- Long-term archival of analytics event logs
- Correlation of analytics events with ANPR data and recorded video

6.13.1. Parking ANPR Analytics

Automatic Number Plate Recognition (ANPR) is a critical component of Parking Analytics. The IA shall ensure the following functionalities:

a. Entry–Exit ANPR

- Detection of all vehicles entering and exiting the parking location
- OCR extraction of license plate text in real-time
- Identification of vehicle type and classification
- Timestamp, vehicle direction, camera ID, and location tagging

b. Watchlist Integration

- Detection of wanted, stolen or suspicious vehicles
- Real-time alerts at ICCC with vehicle image, event ID and time
- Ability to maintain multiple watchlists (Police, SJTA, District Administration)

c. **Accuracy Requirements-** The IA shall ensure that the ANPR system adheres to the accuracy benchmarks specified by the Authority:

- Daytime ANPR Accuracy: ≥ 90%
- Night-time ANPR Accuracy: ≥ 70%
- Accuracy applicable for 2-wheelers and 4-wheelers
- Accuracy maintained for vehicles moving up to 100 km/h (subject to parking layout constraints)

d. **Metadata Storage-** The IA shall ensure that each ANPR event stores:

- Vehicle registration number
- JPEG snapshot of the vehicle
- Timestamp
- ANPR camera location
- Direction of movement
- OCR confidence score

e. **Reports & Retrieval-** The IA shall ensure availability of:

- Daily, weekly and monthly ANPR reports
- Vehicle-based search (partial/full number)
- Time-based search
- Location-based search

6.14. Integration Requirements For Parking Surveillance System

Integration of the Parking Surveillance System with the broader Integrated City Surveillance System (ICSS) is a critical requirement to ensure seamless monitoring, real-time visibility, coordinated response, analytics-driven decision-making, and unified command operations across the city of Puri. The IA shall ensure that all components of the Parking Surveillance System—including Fixed Cameras, PTZ Cameras, ANPR Cameras, Junction Boxes, Industrial Switches, UPS Systems, Video Analytics Modules and Networking Infrastructure—are fully integrated with the ICCC at JBPC, the existing SJTA ICCC, the Viewing Centre at Singhdwar Police Station, and any other systems designated by the Authority.

The integration shall ensure that the Authority, Puri Police Department, SJTA and District Administration have unified access to real-time video feeds, analytics alerts, ANPR results, occupancy information, incident logs and historical data from all parking zones (both permanent and temporary). The IA shall ensure that the Parking Surveillance System operates as a seamlessly connected sub-system within the larger ICSS technological ecosystem.

6.14.1. Integration with ICCC at JBPC: The IA shall ensure the following

1. **Full Registration of Parking Cameras in the Central VMS**: All parking cameras shall be added to the central Video Management System (VMS) at the ICCC. The IA shall ensure that live streams, recorded video, PTZ controls, snapshots, metadata, and alarm events from parking locations are accessible at the ICCC.

2. **Real-Time Analytics Integration**: All parking-related analytics (ANPR, congestion detection, wrong parking, abandoned vehicle, loitering detection, reverse movement,

pedestrian conflict zones etc.) shall be integrated into the ICCC Analytics Platform. The IA shall ensure that alerts from parking areas are displayed in real-time on ICCC operator dashboards, video walls, and GIS maps.

3. **Incident Management Module Integration**: The IA shall ensure that any event or alert generated from parking surveillance or analytics—such as a suspicious vehicle detection, ANPR hit, lane blockage, or overcrowding—is automatically pushed into the Incident Management Module of ICCC. The IA shall ensure that incident workflows, assignments and escalations are supported for parking-related events.

4. **Unified Dashboard for Parking Surveillance**: The IA shall ensure the development and integration of a unified Parking Dashboard at ICCC, displaying:
    - Live camera feeds
    - Parking occupancy status
    - ANPR hits and vehicle logs
    - Heatmaps for vehicle density
    - Alerts and active incidents
    - Real-time status of equipment, poles, UPS, switches
5. **User Rights and Role-Based Access**: The IA shall ensure that designated personnel from Police, SJTA, District Administration and Parking Management receive appropriate access rights to view relevant parking data, as approved by the Authority.

6. **Scalability & Future Compatibility**: The IA shall ensure that the integration architecture is scalable and does not require re-engineering when additional parking locations, cameras or analytics modules are added in the future.

7. Video Summarization System

The Integrated City Surveillance System (ICSS) shall be equipped with an advanced **Video Summarization Software** that enables rapid review of long-duration video footage by compressing hours of recorded content into concise, searchable, and event-driven summaries. The summarization engine shall support efficient post-incident investigation, forensic analysis, operational review, behavioural pattern identification, and data-driven decision-making for all stakeholders including Police, District Administration, SJTA, Transport Authorities and Disaster Response teams.

Video Summarization is a critical capability in large-scale deployments like Puri due to the extensive volume of video generated across hundreds of cameras, particularly during high-footfall events such as Rath Yatra. The system must help users quickly navigate through non-critical segments, isolate key events of interest, reconstruct incidents, and identify anomalies or security threats with minimal manual effort.

The IA shall ensure that the summarization module integrates seamlessly with the VMS, ICCC dashboard, analytics engine, metadata indexing layer, ANPR system and all designated viewing centres. The summarized outputs shall be usable both for operational monitoring and for investigative workflows.

The Authority may periodically review system performance, summarization quality, metadata tagging accuracy and operator usability, and may require the IA to fine-tune or augment the summarization algorithms without requiring major platform reconfiguration.

Functional Requirements for Video Summarization Software

a. **Input Requirements from Edge & VMS-** The IA shall ensure that the summarization engine receives high-quality input streams and metadata from field cameras and the VMS, including:
    - Continuous recorded video across all camera types
    - Time-synchronized event metadata (e.g., crowd alerts, ANPR hits, intrusion detections)
    - Adequate frame rate, resolution and clarity to support object extraction and motion analysis
    - Camera identifiers, location tags and associated timestamps

    The IA shall ensure that the summarization accuracy is not compromised due to improper camera placement, insufficient lighting or poor configuration.

b. **Information to be Processed and Displayed at ICCC and Viewing Centres-** The summarization system shall generate searchable visual representations and compressed video narratives, enabling operators to:
    - View accelerated summaries of long-duration footage
    - Search for objects, persons, vehicles or activities using metadata filters
    - Navigate directly to key events detected by AI (crowd surges, intrusions, traffic violations, etc.)

- Extract short clips corresponding to selected events or time windows
- Overlay bounding boxes, heatmaps or analytical markers on summarized footage
- Review region-of-interest (ROI) summaries for specific zones such as Grand Road, Temple periphery, parking areas or critical entry/exit corridors

c. **Information Available to Police, Enforcement & Investigative Teams-** The IA shall ensure that authorized personnel can access:
- Event-driven condensed videos for rapid forensic review
- Object-based timelines (person, vehicle, colour, movement pattern, etc.)
- Time filters, event filters and custom query options
- Instant exports of summarized clips for case documentation
- Audit trails of all video retrieval and exports
- Clean-room investigation mode that isolates sensitive data

d. **Operational Requirements-** The summarization system shall support:
- Summarizing hours of video into minutes without loss of critical events
- Object detection, classification and tracking across video frames
- Motion path visualization for individuals and vehicles
- Highlighting unusual patterns or sudden behavioural deviations
- Merging summaries from multiple cameras for cross-correlation
- Operator-driven tagging and annotation of key events
- Real-time summarization capability for urgent investigations
- GPU-accelerated processing to ensure rapid output generation

The system shall remain scalable to handle increased camera counts in Phase-2 and future expansions.

e. **Storage, Recording & Metadata Indexing Requirements-** The IA shall ensure that:
- All summaries are linked to the original high-quality recordings
- Video summaries consume significantly less storage while retaining event fidelity
- Metadata is indexed for fast retrieval and cross-camera correlation
- Summaries can be stored for configurable retention periods based on operational need
- Summarization outputs do not overwrite or degrade original recordings
- Users can export summaries in standard formats (MP4/AVI) with embedded timecodes

f. **Categories of Video Summarization Functions-** The system shall support, at minimum, the following summarization categories:

1. **Time-Compressed Summaries**
   - Condensing long video sequences by eliminating idle or non-relevant segments.
2. **Object-Based Summaries**
   - Showing only objects of interest (persons, vehicles, specific attributes).

3. **Event-Based Summaries**
    - Highlighting events like intrusions, crowd surges, abandoned objects, anomalies, ANPR hits, etc.
4. **Motion Path Summaries**
    - Visualizing movement paths across a selected timeframe.
5. **Multi-Camera Correlated Summaries**
    - Creating unified summaries from multiple adjacent cameras for spatial incident reconstruction.
6. **Region-of-Interest (ROI) Summaries**
    - Summaries focusing specifically on predefined critical zones.
7. **Activity Density Summaries**
    - Displaying hotspots and activity intensities over time.
8. **Custom Operator-Defined Summaries**
    - Allowing manual selection of parameters, time ranges, object types, and behavioural filters.
    - All summarization outputs shall be available on both **live (near real-time)** and **recorded** streams wherever applicable, ensuring comprehensive operational and investigative support.

8. Automatic Number Plate Recognition System (ANPR)

The Integrated City Surveillance System (ICSS) shall include a robust and highly accurate **Automatic Number Plate Recognition (ANPR) System** for real-time detection, extraction, recognition, recording and analysis of vehicle number plates across key permanent and temporary locations in Puri. The ANPR system shall play an essential role in vehicle movement management, law enforcement, traffic monitoring, hotlist identification, incident investigation and securing major event corridors, especially during occasions such as Rath Yatra when vehicular load and enforcement requirements significantly increase.

The ANPR component shall be fully integrated with the VMS, ICCC platform, analytics modules, Parking Management System, Traffic Enforcement workflows and any existing/state vehicle databases as permitted by the Authority.

The IA shall ensure the deployment of high-performance ANPR cameras and processing engines capable of delivering superior accuracy in varying lighting, weather and environmental conditions prevalent in Puri.

The Authority may periodically review ANPR performance parameters, detection accuracy, alert rules, hotlist configurations and enforcement integrations. The IA shall be required to adjust configurations or enhance algorithmic performance without necessitating major architectural changes.

Functional Requirements for ANPR System

a. **Input Requirements from Field Devices-** The IA shall ensure that each ANPR camera installation provides high-quality image input suitable for reliable plate extraction and recognition. This includes:
    - Correct mounting height, angle and focal length to ensure optimal number plate visibility.
    - Adequate illumination using IR illuminators to support clear night-time capture.
    - Stable frame rate and bit rate for crisp motion image acquisition.
    - High shutter speed to avoid motion blur for fast-moving vehicles.
    - Clear field of view covering entry/exit lanes, choke points, parking gates and enforcement zones.
b. **Information to be Processed and Displayed at ICCC and Viewing Centres-** The ANPR engine shall process incoming video streams and generate structured information for ICCC operators to:
    - View real-time ANPR detections and recognition results.
    - Review plate images alongside full-frame snapshots for verification.
    - Monitor vehicle movement trends across city corridors.
    - Identify repeat offenders, suspect vehicles or abnormal movement patterns.
    - Access searchable logs filtered by plate number, time, location, vehicle class or alert category.
    - Receive system-generated alerts for listed or flagged vehicles.
c. **Information Available to Police, Transport & Enforcement Agencies-** Designated enforcement personnel shall be able to access:
    - Real-time alerts for blacklisted, stolen, wanted or flagged vehicles.
    - Vehicle movement history across all ANPR-equipped corridors.
    - Entry–exit timestamps, direction of travel and location-based trail generation.
    - Dashboards showing traffic patterns, peak vehicle load and corridor usage analytics.
    - Exportable data for investigation, prosecution or penalty issuance.
    - Consolidated hotlist and rule-based alert configuration interface.

d. **Operational Requirements-**The ANPR system shall support the following minimum operational capabilities:
    - High-accuracy number plate recognition under variable lighting and weather conditions.
    - Detection of different plate formats (private, commercial, government, temporary plates etc.).
    - Real-time alerting with configurable latency thresholds.
    - Ability to handle high-density traffic flow during peak hours and major events.
    - Rule-based triggers for:
        - Hot listed vehicles
        - Suspicious movement patterns
        - Wrong-way driving
        - Vehicle overstaying or unauthorized parking
    - Secure audit trails for all ANPR detections and manual verifications.
    - Scalability to support additional ANPR locations in Phase-2 and beyond.

e. **Storage, Recording & Data Management Requirements-** The IA shall ensure the following:
- Storage of ANPR metadata, plate images and full-frame proofs for configurable retention periods.
- Fast search and retrieval capability for past detections.
- Tagging of ANPR events with timestamps, camera IDs and geolocation metadata.
- Seamless linking of ANPR data with corresponding video recordings for evidence review.
- Ability to export ANPR event logs, images and video clips for legal or investigative use.
- Compliance with security, privacy and data protection requirements.

8.1. Categories of ANPR Functions- The ANPR system shall provide at least the following functional capabilities:

1. **Real-Time Number Plate Recognition**
   a. Extraction and interpretation of number plates from live video streams.
   b. Continuous accuracy improvement using AI/ML-based recognition models.
2. **Vehicle Hotlist and Watchlist Alerting-**
   a. Instant alerts for:
   b. Stolen vehicles
   c. Government watch listed vehicles
   d. Vehicles involved in criminal or enforcement cases
   e. Repeated traffic violators
3. **Traffic Flow Analysis**
   a. Vehicle counting, classification and directional analytics.
   b. Monitoring of congestion points and high-load corridors.
4. **Vehicle Trail Reconstruction**
   a. Generating a chronological movement trail of any detected vehicle across multiple ANPR points.
5. **Parking ANPR for Access Control & Payment Integration**
   a. Automatic logging of entry/exit times.
   b. Calculation of parking duration and integration with parking management systems.
6. **Event Mode ANPR**
   a. During Rath Yatra or other large events, the system shall:
   b. Support temporary ANPR setups with portable or rapid-deployment cameras.
   c. Provide real-time alerts for restricted-access zones.
   d. Enhance perimeter control at Temple areas and critical barricading points.

9. Red Light Violation Detection System

The Integrated City Surveillance System (ICSS) shall include an automated **Red Light Violation Detection (RLVD) System** to accurately identify, record and report incidents of vehicles crossing stop-lines or traffic signals during the red-light phase. The RLVD system shall support traffic enforcement, road safety management, violation analytics and real-time alerting for the Police Department and Transport Enforcement authorities.

The RLVD system shall form an integral part of the broader ICSS ecosystem and shall be fully integrated with the VMS, ANPR engine, ICCC dashboard, and designated viewing centres. The IA shall ensure deployment of high-precision sensors and video analytics capable of detecting violations in complex traffic environments, including multi-lane roads, turning lanes, high-density corridors, and event-period diversions.

The Authority may periodically review violation detection accuracy, camera configuration, sensor calibration, enforcement workflows and shall direct the IA to upgrade or fine-tune the RLVD system as required.

Functional Requirements for RLVD System: -

a. **Input Requirements from Field Devices-** The IA shall ensure that RLVD cameras and supporting sensors are installed to capture clear evidence of traffic light violations, including:

- High-resolution video streams covering stop-line, signal pole, and approach lanes.
- Time-synchronized video and signal-phase data for accurate violation identification.
- Proper positioning and lens configuration to cover all lanes of the intersection.
- Adequate illumination using IR/white-light support for night-time detection.
- Accurate embedding of date, time, location, camera ID and signal state information.

b. **Information to be Processed and Displayed at ICCC and Viewing Centres-** The RLVD system shall process incoming streams and automatically:

- Detect vehicles crossing the stop-line during the red-phase.
- Generate violation clips containing pre-event, event and post-event footage.
- Capture still images of violating vehicles and associated number plates.
- Display violation events on ICCC dashboards in real-time.
- Present violation logs with searchable filters including vehicle type, location, time, and violation category.
- Correlate violations with ANPR results for enhanced enforcement and tracking.

c. **Information Available to Police, Transport & Enforcement Agencies-** Designated enforcement personnel shall be able to:

- View validated violation events with complete evidence package (video + plate images).
- Access violation history for specific vehicles or locations.
- Monitor violation trends, peak times, and high-risk intersections.
- Export violation data for challan generation or legal processes.
- Generate daily, weekly and monthly violation analytics reports.
- Configure hotlists and auto-escalation for repeat offenders.

d. **Operational Requirements-**The RLVD system shall support:

- Automated real-time detection of stop-line crossing during red-phase.
- Lane-wise violation detection for multi-lane intersections.
- Ability to detect violations for both moving and slow-moving vehicles.
- Synchronization with signal-controller logic (whenever available).
- Handling of turning lanes, slip lanes and event-specific traffic diversions.
- Rule-based alerting based on threshold counts or repeated violations.
- Secure evidence generation suitable for challan and prosecution workflows.
- Operator interface for reviewing, accepting, rejecting or annotating events.
- Scalability to add RLVD points across more intersections during Phase-2.

e. **Storage, Recording & Evidence Management Requirements-** The IA shall ensure that:

- Each violation event is stored with complete metadata including time, location, lane, signal state and vehicle details.
- Violation data is linked to corresponding ANPR records for identification.
- Evidence clips contain pre-event and post-event context for legal admissibility.
- Retrieval time for violation footage is minimal and must support fast investigation.
- Violation data is retained as per Authority's retention policy.
- All evidence packages can be exported in standard formats for integration with e-challan systems.

9.1. Categories of RLVD Functions-

The RLVD system shall support, at minimum, the following functional capabilities:

1. **Stop-Line Violation Detection**
    a. Detection of vehicles crossing the stop-line during red signal phase.
    b. Support for multiple lanes including left, right, straight and turning movements.
2. **Signal-State Synchronization**
    a. Integration with traffic signal controllers wherever present.

b. Ability to operate in "virtual signal logic mode" where hardware integration is unavailable.

3. ANPR-Linked Violation Processing

a. Automatic extraction of number plates of violating vehicles.
b. Generation of violation events tagged with ANPR metadata.

4. **Violation Evidence Package -**Each violation shall include:
   a. Still images capturing the vehicle before and after violation
   b. Video clip highlighting the event
   c. Time, location, lane, and signal-phase overlay

5. Violation Analytics & Reporting

a. Heatmaps of high-risk intersections
b. Violation density by time-of-day and day-of-week
c. Repeat offender analysis
d. Corridor-level enforcement dashboards

6. **Event Mode RLVD Support-** During major events (e.g., Rath Yatra), the system shall:
   a. Adapt to diversion plans, temporary signals and manual traffic control.
   b. Support temporary RLVD deployments where required.
   c. Provide real-time flagging of unauthorized vehicle movement in restricted zones.

9.2. Speed Violation Detection System

The Integrated City Surveillance System (ICSS) shall include a comprehensive **Speed Violation Detection System (SVD)** to automatically detect, record, analyse, and report vehicular over-speed violations across designated corridors in Puri. These may include the Bhubaneswar–Puri highway entry, Konark Road, Chilika/Brahmagiri route, Marine Drive, major approach roads, and any other stretches identified by the Authority.

The SVD system is essential for improving road safety, deterring speeding behaviour, reducing accident rates, and enabling enforcement during high-traffic periods, including festivals, VIP movements, and special events like **Rath Yatra**. The solution shall integrate seamlessly with the VMS, ANPR engine, ICCC dashboard, Enforcement Systems, and designated viewing centres.

The IA shall ensure deployment of accurate and reliable SVD sensors and video analytics engines capable of capturing vehicle speed under varying lighting, weather, and traffic conditions.

The Authority may periodically review performance parameters such as speed thresholds, measurement accuracy, lane coverage, and may direct the IA to recalibrate or enhance the SVD system without requiring major architectural changes.

Functional Requirements for SVD System

a) Input Requirements from Field Devices

The IA shall ensure that SVD units, including radar sensors, lidar devices, or video-based speed analytics, are deployed in a manner that ensures high accuracy and admissible evidence. The input requirements include:

- Clear, unobstructed views of the roadway section under surveillance.
- Configured detection zones covering all active lanes, including turning lanes where applicable.
- Cameras or sensors calibrated to capture speed accurately for vehicles moving in multiple directions.
- Adequate illumination for night-time detection using IR/white-light support.
- Proper mounting height, angle, distance, and stabilization to avoid measurement distortions.
- Time-synchronized video and metadata for legal evidence creation.

b) Information to be Processed and Displayed at ICCC and Viewing Centres

The SVD system shall process incoming data and generate actionable outputs for operators to:

- View real-time speed violation alerts with measured speed and threshold values.
- Review violation evidence including pre-event and post-event video clips.
- Analyse lane-wise and vehicle-type-wise violation trends.
- Access historical violation logs with filters by date, time, location, vehicle type, or speed threshold.
- Correlate speeding violations with ANPR results for identification of violators.
- Generate consolidated reports for enforcement agencies.

c) Information Available to Police, Transport & Enforcement Agencies

The IA shall ensure that enforcement teams can access:

- Verified and validated speed violation events suitable for challan generation.
- Still images capturing vehicle position relative to detection zone.
- Metadata including vehicle speed, posted speed limit, violation magnitude, timestamp, and geolocation.
- Violation history for specific vehicles or corridors.
- Automated workflows for penalty issuance and case closure.
- Dashboards summarizing high-risk zones and peak violation periods.

d) Operational Requirements

The SVD system shall support the following capabilities:

- Accurate speed measurement using approved technologies (radar, lidar, video analytics, or hybrid).
- Ability to detect speed violations for both single and multi-lane roads.
- Support for bi-directional traffic monitoring.
- Real-time alerting with configurable speed thresholds for each corridor.
- Integration with ANPR to associate vehicle number plates with speed violations.
- Automatic evidence packaging for each violation including:
    - Vehicle snapshot
    - Speed measurement
    - Video clip of the event
    - Time, date, lane and location metadata
- Ability to operate reliably in harsh conditions including coastal humidity, fog, rainfall, heat, and high traffic density.
- Scalability to add additional SVD points across Puri in future phases.

e) Storage, Recording & Evidence Management Requirements

The IA shall ensure that:

- All speed violation records are stored with complete metadata and associated video clips.
- Evidence packages are securely archived and accessible for legal or investigative purposes.
- Indexing supports fast search and retrieval of violations by multiple parameters.
- Footage related to speed violations is linked to the original recorded stream for verification.
- Data retention complies with Authority policies and classification.
- Export formats are compatible with enforcement, e-challan, or court submission workflows.

9.3. Categories of SVD Functions

The SVD system shall support the following minimum functional capabilities:

1. Real-Time Speed Detection

- Accurate measurement of vehicle speed in real-time.

- Lane-based detection for multi-lane corridors.

2. Threshold-Based Violation Identification
- Automatic classification of violations based on configurable speed limits.
- Support for different thresholds by zone (urban, corridor, approach roads, parking exits).

3. Vehicle Identification through ANPR Integration
- Automatic linking of speed measurements to vehicle number plates.
- Repeat-offender identification and alerting.

4. Evidence Generation for Enforcement

Each violation event shall include:
- High-resolution image showing the vehicle during violation
- Speed measurement overlay
- Pre-event and post-event video clip
- Timestamp, lane, and location information

5. Violation Analytics & Reporting
- Heatmaps of over-speeding zones
- Peak violation timings
- Violation severity charts (e.g., 10 km/h above limit, 20 km/h above limit, extreme violations)
- Data for planning enforcement deployments and traffic calming measures

6. Event Mode Speed Monitoring

During major events such as Rath Yatra, the system shall:
- Enforce temporary or event-specific speed limits.
- Monitor restricted zones or pedestrian-heavy segments.
- Support portable SVD units deployed on a temporary basis.

10. Variable Message Display

The Integrated City Surveillance System (ICSS) shall include a network of **Variable Message Display (VMD) units** installed at strategic locations across Puri to enable real-time dissemination of public information, traffic advisories, emergency alerts, crowd control instructions and event-specific announcements. The VMD system shall serve as an essential public communication channel, especially during high-density events such as **Rath Yatra**, when timely messaging is critical for safety, mobility, and crowd management.

The VMD solution shall be fully integrated with the ICCC platform, allowing operators to broadcast messages dynamically based on real-time analytics, incident alerts, instructions from the District Administration, Police, SJTA and Disaster Response units. The IA shall ensure that the VMD units deployed are rugged, high-visibility, weather-proof and capable of operating reliably in coastal and high-humidity conditions.

The Authority may define message templates, emergency protocols, display durations, formatting requirements, content approval workflows and escalation procedures, all of which shall be supported by the VMD management system.

Functional Requirements for Variable Message Display System

a) Input Requirements and Device Capabilities

The IA shall ensure that VMD units are configured to receive real-time updates from ICCC and support:

- High-brightness LED panels with day/night auto-dimming.
- Wide viewing angles suitable for roads, junctions, pedestrian zones and event corridors.
- Adequate pixel pitch, resolution and refresh rate to ensure message readability.
- Redundant communication channels (fiber, wireless, 4G/5G fallback) for uninterrupted message delivery.
- Rugged, vandal-resistant and weather-proof enclosures with appropriate IP ratings.
- Mounting structures suitable for poles, gantries or wall-mount configurations.

b) Information to be Processed and Displayed at ICCC and Viewing Centres

The VMD Management System shall allow ICCC operators to:

- Create, edit, schedule and broadcast text-based or graphical messages.
- Select individual VMDs or groups of VMDs based on geographic zones (e.g., Grand Road, Temple periphery, Marine Drive, parking areas, city entry points).
- Display emergency alerts received from analytics systems or field forces.
- Push predefined templates for traffic advisories, diversions, crowd behaviour instructions, safety warnings, VIP movement information and weather alerts.
- Preview the message before broadcast.
- Monitor VMD health, connectivity and message playback status in real time.
- Generate logs of all messages displayed, along with timestamps and operator ID.

c) Information Available to Police, District Administration & SJTA

Authorized personnel from relevant agencies shall be able to:

- Trigger priority alerts (Emergency, Disaster, Fire, Public Safety, Crowd Alerts).
- Approve or modify messages based on their jurisdiction.
- Access message history for verification or audit.
- Monitor device health and message delivery success.
- Use role-based dashboards for traffic, crowd movement, and public safety communications.

d) Operational Requirements

The VMD system shall support:

- **Manual**, **scheduled**, and **automated message broadcasts**.
- Automated activation based on system events (e.g., crowd density exceedance, vehicle violation, emergency incidents).
- Multi-lingual messaging (English, Odia, Hindi).
- Prioritization of emergency messages over routine messages.
- Integration with PAS (Public Address System) for combined audio-visual alerts.
- Local fallback mode displaying default safety instructions in case of network outage.

- Remote configuration updates including brightness, sequencing, formatting and message queue management.
- Synchronization with event plans (Rath Yatra flow, diversions, temple opening/closing hours).

e) Storage, Logging & Audit Requirements

The IA shall ensure that:

- All messages broadcast through VMDs are logged with timestamp, operator ID, message content and display duration.
- Historical logs are searchable for audit, analytics and compliance purposes.
- Message templates are securely stored with version control.
- System retains full audit trails including modifications, approvals and cancellations.
- VMD health data (temperature, LED failures, power status, network connectivity) is recorded and available for diagnostics.

11.1 Categories of VMD Functions

The VMD system shall support, at minimum, the following functionalities:

1. Real-Time Information Display

- Traffic conditions, diversions, accidents, congestion alerts.
- Crowd management instructions at high footfall locations.
- Public safety warnings and emergency evacuation messaging.

2. Event-Specific Messaging

During festivals like Rath Yatra, the system shall display:

- Route guidance for pilgrims and visitors.
- Restricted/no-entry zone notifications.
- Emergency corridor clearance messages.
- Weather updates, heat advisory or lightning warnings.
- Lost-and-found announcements (where approved).

3. Automated Alerts Triggered by AI Analytics

- Overcrowding or density threshold breach.
- Traffic violations or road blockage detection.
- ANPR-based alerts (e.g., vehicle of interest entering a restricted zone).
- Fire/smoke detection or perimeter breach alerts.

4. Scheduled Messaging

- Pre-planned advisories for events, peak timings, temple schedule.
- Timed announcements for parking availability or bus/train movements.

5. Multi-Lingual Display Support

- Mandatory support for Odia, Hindi and English.

6. Health Monitoring & Diagnostics

- Real-time device health metrics.
- Alerts for power failure, LED malfunction or network disconnect.
- Automatic switchover to backup communication routes.

11. Public Address System

The Integrated City Surveillance System (ICSS) shall include a robust and citywide **Public Address System (PAS)** to enable real-time dissemination of audio announcements for public safety, crowd management, emergency response and event-related communication. The PAS shall serve as a critical public outreach mechanism, especially during large gatherings such as **Rath Yatra**, Snana Purnima, New Year celebrations and other high-footfall events, where timely and clear communication is essential for maintaining order and ensuring safety.

The PAS solution shall be fully integrated with the ICCC platform, enabling centralized or zonal broadcasting, automated event-triggered messages, and manual announcements by Police, District Administration or Temple Authorities. The IA shall deploy high-quality, outdoor-rated PAS components capable of delivering clear and audible sound across diverse environments including crowded streets, open grounds, parking areas, entry/exit corridors and coastal zones.

The system shall support multilingual announcements and flexible scheduling, along with operational dashboards for real-time monitoring and diagnostics. The Authority may periodically review message templates, audio clarity, coverage zones and operational protocols, and may require the IA to fine-tune configurations as needed.

Functional Requirements for Public Address System (PAS)
a) Input Requirements and Device Capabilities

The PAS units deployed across Puri shall be configured to receive live and pre-recorded audio content from ICCC and support:

- High-power outdoor-rated horns/speakers with wide sound dispersion.
- Clear audio output with configurable volume levels based on location type.
- Weatherproof, corrosion-resistant and vandal-proof construction.
- Ability to mount on poles, gantries, building walls or integrated structures.
- Redundant communication links including fiber, RF, or 4G/5G fallback.
- Integrated amplifiers, controllers and power-management modules.
- Automatic volume adjustment based on ambient noise (optional, if available).

b) Information to be Processed and Broadcasted from ICCC & Viewing Centres

The PAS Management System shall enable ICCC operators to:

- Broadcast **live announcements** through microphone input.
- Play **pre-recorded messages**, alerts, and safety instructions.
- Schedule announcements by time, frequency and zone.
- Select individual PAS units or predefined geographic clusters for targeted messaging.

- Trigger emergency notifications in real-time based on analytics or field alerts.
- Preview announcements before broadcast where supported.
- Monitor PAS device status, sound output levels and connectivity.
- Maintain logs of all announcements with timestamps and operator identification.

c) Information Available to Police, District Administration & SJTA

Authorized personnel shall be able to:

- Initiate high-priority or emergency announcements.
- Override routine messages with safety-critical announcements.
- Access a library of standard/pre-approved message templates.
- Monitor announcement history for verification and auditing.
- Coordinate zone-level announcements during crowd surges, diversions or emergencies.
- Ensure Temple-related announcements are confined to approved areas.

d) Operational Requirements

The PAS system shall support the following operational capabilities:

- Manual, scheduled and automated broadcasting modes.
- Multi-lingual announcements in Odia, Hindi and English.
- Emergency override mode that immediately interrupts ongoing messages.
- Integration with analytics systems for auto-trigger announcements, such as:
    - Crowd density threshold breach
    - Fire/smoke detection
    - Unauthorized entry in Temple zones
    - Traffic congestion alerts
- Zone-based coverage allowing operators to isolate announcements to specific areas.
- Fail-safe fallback to default pre-recorded safety messages in case ICCC connectivity is interrupted.
- Seamless alignment with event management workflows for Rath Yatra and other major festivals.
- Ability to link PAS messages with VMD instructions for coordinated multi-channel communication.

e) Storage, Logging & Audit Requirements

The IA shall ensure that:

- All announcements (live or recorded) are logged along with time, location and operator identity.
- Audio files and message templates are stored in a secure repository.
- System maintains full audit trails of overridden messages, cancellations and re-broadcasts.
- PAS health data (amplifier status, speaker fault, connectivity issues, power status) is recorded and displayed on ICCC dashboards.
- Historical announcement logs are retained as per the Authority's retention policy.

12.1 Categories of PAS Functions

The PAS system shall provide, at minimum, the following functionalities:

1. Real-Time Manual Announcements

- Live voice announcements from ICCC operators or authorized officials.
- High-priority instructions during emergencies, law-and-order situations or disaster events.

2. Scheduled Announcements

- Time-based broadcasts for crowd movement, temple schedule, traffic advisories, safety instructions and event regulations.

3. Automated Event-Based Announcements

Triggered automatically by AI or VMS events, including:

- Overcrowding
- Fire/smoke incidents
- Intrusions or suspicious activity
- Route blockages or congestion
- Hot listed vehicle entry in restricted areas

4. Zone-Based & Multi-Agency Broadcasting

- Capability to broadcast to selected zones such as:
  - Grand Road
  - Temple periphery
  - Parking areas
  - Viewing centres
  - Marine Drive
  - Entry/Exit corridors
- Agency-specific access rights for message initiation.

5. Emergency Override Mode

- Automatic override of all scheduled or ongoing messages in case of critical alerts.
- Multi-channel activation (PAS + VMD + ICCC alarms).

6. Health Monitoring & Diagnostics

- Real-time monitoring of:
  - Speaker output levels
  - Amplifier status
  - Network connectivity
  - Power supply and UPS health
- Fault alerts routed to field maintenance teams for corrective action.

12. City Communication Network

The City Communication (Leased) Network shall serve as the **foundational backbone** of the Integrated City Surveillance System (ICSS), enabling secure, high-bandwidth, low-latency, and uninterrupted transmission of video streams, analytics data, alerts, command instructions and system health information across all field locations, ICCC, viewing centres, data centres and integration points.

The network shall be designed to support **mission-critical public safety operations**, ensuring resilient connectivity during routine operations as well as peak-load conditions such as **Rath Yatra**, major festivals, VIP movements, emergencies, and disaster events. The IA shall establish a highly available, scalable, multi-layered communication network capable of supporting current requirements and future expansion across Puri.

The City Communication Network shall integrate optical fiber, wireless radios, 4G/5G fallback links, LAN infrastructure and secure VPN tunnels to ensure seamless end-to-end communication. The IA shall maintain rigorous performance, redundancy and cybersecurity standards throughout the network lifecycle.

Functional Requirements for City Communication Network

a) Core Network Architecture Requirements

The IA shall design, supply, deploy and maintain a citywide communication network adhering to the following capabilities:

- High-capacity backbone network connecting all surveillance field equipment to aggregation points and the ICCC.
- Layer-2 and Layer-3 network architecture supporting secure, scalable and deterministic routing.
- Redundant network paths ensuring "no single point of failure" for critical feeds at aggregation point ICCC/DC.
- Network designed to deliver stable transmission of HD/AI video streams.
- End-to-end encryption and security policies across all communication layers.
- Bandwidth provisioning that supports peak simultaneous camera load, analytics traffic and ICCC operations.
- Future-proof architecture capable of incorporating additional devices, sensors and locations under Phase-2 and beyond.

b) Field Connectivity Requirements

The IA shall ensure robust field connectivity through a combination of:

- Underground optical fiber laid via ducts, trenches, poles or existing city utilities.
- Aerial or pole-mounted fiber routes where underground deployment is not feasible.
- Radio/wireless network extensions using licensed or unlicensed bands.
- 4G/5G fallback connectivity for critical nodes to maintain continuity during outages for VMD (if applicable).
- Secure media converters, SFP modules, LIUs, patch panels and other field networking accessories.
- Hardened network switches installed near camera clusters and junction boxes.

All field connections must be capable of carrying high-throughput, low-latency video traffic even during congestion or peak deployment periods.

c) ICCC, Data Centre & Viewing Centre Connectivity

The IA shall ensure high-availability connectivity across:

- ICCC at JBPC (primary monitoring and analytics hub)
- Police viewing centres (e.g., Singhdwar Police Station)
- Data Center (DC) and Disaster Recovery (DR) environments
- Existing Temple Administration surveillance systems (where permitted)

Functional capabilities shall include:

- Dedicated, redundant uplinks to the ICCC.
- Site-to-site VPN tunnels with encryption for all inter-facility communication.

- QoS prioritization for real-time traffic (video, alerts, emergency audio).
- Centralized network monitoring through NMS/EMS dashboards.

d) Bandwidth, Throughput & Performance Requirements

The IA shall ensure that the communication network supports:

- Sufficient bandwidth for each camera:
  - PTZ Cameras: ≥ 3 Mbps
  - Fixed/ANPR Cameras: ≥ 3 Mbps
- Adequate upstream and downstream capacity at aggregation points.
- Latency low enough to support near-real-time surveillance and AI analytics.
- Jitter control, error correction and packet-loss mitigation.
- High network uptime as per SLA requirements for mission-critical systems.

The IA shall perform detailed bandwidth calculations and propose the optimal architecture to support full-load video and AI traffic.

e) Network Security Requirements

The City Communication Network must incorporate:

- Enterprise-grade firewalls, IDS/IPS systems and secure gateway devices.
- End-to-end encryption of video streams and data packets.
- Role-based access control (RBAC) and secure authentication mechanisms.
- Protection against unauthorized access, tampering, malware and DoS attacks.
- Network segmentation separating camera networks, management networks and application networks.
- Logging and audit trails for all network activity.

Cybersecurity design must comply with standard best practices for public safety systems.

f) Redundancy & High Availability Requirements

The IA shall ensure:

- Fiber redundancy through ring or mesh-based design.
- Redundant power supplies for all core networking equipment.
- Automatic failover between primary and secondary communication paths.
- Wireless/4G/5G backup links at priority locations.
- Multiple PoPs (Points of Presence) in geographically separate areas.
- Built-in failover for DC and DR connectivity.

The network must continue functioning without interruption during major festivals, high-load events or partial infrastructure failures.

g) Monitoring, Diagnostics & Network Management Requirements

The IA shall deploy a centralized Network Management System (NMS) that provides:

- Real-time monitoring of all routers, switches, radios, fiber links and field devices.
- Alerts for link failure, packet loss, bandwidth saturation or device malfunction.
- SNMP-based performance monitoring with threshold settings.
- Topology maps showing node connectivity and link health.
- Automated trouble-ticket creation for O&M teams.
- Historical analytics for bandwidth consumption and device uptime.

The ICCC operators must be able to track the live status of the entire network in a graphical dashboard.

h) Scalability & Expansion Requirements

The communication network shall be designed to support:

- Integration of new locations under Phase-2 (citywide expansion).
- Additional cameras, sensors, PAS systems, VMDs, analytics engines, drones and emergency equipment.
- Upgrades to higher bandwidth links without redesigning the core architecture.
- Modular replacement of networking equipment without service interruption.

i) Environmental and Reliability Requirements

Considering Puri's coastal and high-humidity environment, the IA shall ensure:

- Use of corrosion-resistant and weatherproof enclosures.
- Surge protection, lightning protection and grounding at all critical nodes.
- Heat-resistant and humidity-tolerant networking components.
- Secure mounting of equipment to withstand wind, vibrations and saline exposure.

13.1 Categories of City Communication Network Functions

The City Communication Network shall support the following functional capabilities at a minimum:

1. High-Bandwidth Video Transport

Reliable transmission of HD/AI video from all fixed, PTZ, ANPR and temporary/event cameras.

2. Real-Time Analytics Data Flow

Transport of metadata, alerts and detection events to ICCC.

3. Mission-Critical Voice & PAS Integration

Support for audio communication and PAS message triggers.

4. Multi-Agency Communication Routing

Secure data exchange between Police, District Administration, SJTA, OBCC and other approved entities.

5. Emergency Mode Continuity

Automatic activation of redundant paths during network disruption.

6. Unified Network Monitoring

Centralized health, performance and fault management of the entire network infrastructure.

Design & Implementation of Artificial Intelligence (AI) based Video Analytics

The IA shall be responsible for designing and implementing Artificial Intelligence based Video Analytics for Integrated Crowd Management System through various CCTV cameras across strategic locations with continuous learning capabilities. Following listed use cases should be part of implementation and should not be limited to:

1- Integrated Crowd Management System
   - Crowd Density Analytics
   - People Count Analytics

2- Wall / Barrier Climbing Detection

3- Fire & Smoke Detection Analytics
4- Attribute-based Search Analytics for Video Summarization
5- Vehicle Count Analytics

The above-mentioned AI based use cases shall be implemented through various cameras installed across the field locations without dependency on any type of cameras (field device agnostic) with continuous learning capabilities.

12.1.1. Functional Requirements of Integrated Crowd Management System

1. **Data Collection:**
   The system shall collect / aggregate the data / feeds from following sources, but not limited to:
   a. AI based People Count Analytics running on CCTV Surveillance Cameras deployed across strategic locations along with entry / exit points of Puri City area, transport hubs – Shri Jaganath Temple, railway stations, parking, bus stands etc.
   b. Train / railway booking / ticketing information for estimation of anticipated influx of pilgrims / visitors / tourists / travellers, integration APIs shall be facilitated by the authority
   c. Bus / Bus booking / ticketing information for estimation of anticipated influx of pilgrims / visitors / tourists / travellers, integration APIs shall be facilitated by the authority
   d. Booking information from official vendor for Odisha Tourism, for estimation of anticipated influx of pilgrims / visitors / tourists / travellers, integration APIs shall be facilitated by the authority
   e. Vehicle Count information from NHAI Tolls of the vehicles approaching Puri from various city entry / exit points
   f. Shri Jagannath Temple Surveillance feed for estimation of anticipated influx of pilgrims / visitors / tourists / travellers, integration APIs shall be facilitated by the authority.
   g. AI based Vehicle Count Analytics running on CCTV Surveillance Cameras deployed across Puri City critical/identified areas

2. **Data Processing:**

The system should be able to process the data quickly and accurately, considering multiple variables for comprehensive interpretations. The system should be able to co-relate and interpret data from multiple sources / aggregators / systems for deriving meaningful insights for data driven decision making.

3. **Prediction / Forecasting:**

The system shall utilize AI deep learning algorithms and historical data to develop predictive models for crowd management, pilgrim movements, and public safety. These models shall assist in optimizing resource allocation, identifying potential bottlenecks, and proactively addressing security concerns during the events. The system should have the ability to use the collected data to predict future crowd behaviours for effective management strategies for authority. This could include predicting influx, crowd flow, potential bottlenecks, and congestion areas. Indicative use-cases for prediction / forecasting are provided below, but not limited to:

a. Expected number of pilgrims at Location "A" who are originating from Railway Station / Bus Stand along a dedicated route as per Traffic Police Plans based on the distance, average speed etc.
b. Expected number of pilgrims at Shri Jagannath Temple, who will be entering the as per RFP section 4.3. Area / No-Vehicle Zone along a dedicated route as per Traffic Police Plans based on the distance, average speed etc.
c. Prediction of overcrowding / stampede situation across a specific region / holdup area / Temple areas camera field of view, through monitoring of density occupancy levels, permissible thresholds, historical / trend / hourly data, expected number of pilgrims approaching the intended location.
d. Forecasting of parking availability / occupancy levels based on the actual capacity, number of parked vehicles, expected vehicle count from ANPR cameras installed at city entry / exit points, vehicular inputs from NHAI Tolls etc.
e. Expected number of pilgrims / visitors / tourists entering and exiting the railway station based on railway ticketing system information, people count analytics deployed at railway stations.
f. Expected number of pilgrims / visitors / tourists entering and exiting the bus stands based on bus ticketing system information, people count analytics deployed at bus stands etc.

Please note that the above-mentioned use-cases are indicative in nature and detailed use-cases will be discussed with the selected implementation agency during requirement gathering phase.

4. Accuracy:

The system should have the capability to maintain and ensure high accuracy i.e. 90% in detections, predictions and alerts.

5. Alerts:

The system should generate timely and relevant alerts related to overcrowding, potential mishaps or deviations from the expected behaviour, and send these to the respective officials of Temple authority, Police and concerned stakeholders.

6. Dashboard:

The IA shall provide dashboard for viewing and monitoring off all alerts received from various analytics. The dashboard shall be an easy-to-use and intuitive user interface/dashboard for management personnel to read predictions, understand alerts and act accordingly. The dashboard shall have provision to map alerts received from analytics with different SoPs pre-defined by Authority with end-to-end activities tracking for alerts.

7. Analysis and Reporting:

The system should analyse the collected data and generate detailed reports summarizing patterns, potential issues, and opportunities for improvement. This can help in strategic planning for future events.

8. Alert Systems:

The system should have a feature to send alerts or warnings about potential overcrowding, safety concerns, or emergencies based on its predictions. It should send alerts to all concerned/designated officials/authorities.

AI based Crowd Management Use-Cases:

12.1.1.1. AI based Crowd Density Analytics:

The AI based Crowd Density Analytics must have the following functionalities:

a. The system should provide real-time monitoring of crowd data, such as crowd density, movement, and behaviour.
b. The analytics system should be able to accurately count the number of people within a given area in real-time.
c. The system should analyse crowd density levels to identify areas that are prone to overcrowding, stampede or potential safety risks.
d. The system should analyse crowd movement patterns across various locations to identify bottlenecks, congestion points, or areas where the flow of people needs to be better managed.
e. The system should be able to estimate the maximum capacity of an area / field of view and compare it with the current crowd size to ensure that safe limits are not exceeded.
f. The system should generate alerts and notifications to authorities when predefined thresholds or crowd density limits are reached or exceeded.
g. The system should provide historical reports and analysis of crowd data, including patterns, trends.
h. The system should have 90% accuracy for detection, counting and alerts.

12.1.1.2. People Count Analytics:

Effective crowd management across crowded places within Shri Jagannath Temple Area, entry / exit points and railway/Bus stations is very essential. In order to ensure effective crowd management, accurate people count is an important factor. Particularly in smaller areas, increase in the number of people create problems such as stampedes, fatalities, physical injury etc. Early detection of such kind of a crowd can avoid these incidents. In such sort of crowd management, counting the number of people provide accurate information about certain conditions such as blockage at some points and so on.

a. IA should implement machine learning algorithms to detect individual heads or people within the video footage/field of view of specific cameras.
b. The system should utilize the output from the object detection algorithms to count the number of heads or people present in the video frames.

c. The system should generate a visual representation of crowd density by mapping the detected individuals onto a grid or heat map. These maps should provide a clear visualization of crowded areas and can help identify high-density zones within a given space.
d. The system continuously should monitor the video feeds and generate real-time alerts based on predetermined thresholds or rules.
e. The system should store and analyse the data collected over time to gain insights into crowd behaviour, peak periods, and crowd movement patterns.
f. The system should generate alerts as per the guidelines of NDMA/SDMA for minimum count in particular areas with predictive capability of increasing or decreasing the count based on the trends analysis and inputs from other analytics/data sources.
g. The system should have 90% accuracy for detection, counting and alerts.

12.1.1.3. Fire & Smoke Detection

The IA shall implement the fire and smoke detection use cases by using Artificial Intelligence through various cameras in Shri Jagannath temple area & Grand Road with the capability of various optical analysis techniques that examine live images to detect flames and smoke. The System shall be able to provide following functionalities:

a. Real smoke detection and flame detection within video frames.
b. System can detect fire and smoke based on visual characteristics such as colour, motion, and pattern recognition. These algorithms should be trained to differentiate between normal activities and signs of fire or smoke.
c. The system shall continuously analyse the video feed from the cameras using the fire and smoke detection algorithms. This system should be capable of processing the video data in real-time to provide immediate alerts.
d. When fire or smoke is detected, the system should generate an alarm.
e. Store and analyse the data collected by the system over time. This enables the identification of patterns, trends, and areas prone to fire incidents.
f. Reports shall be generated based on the analysis to improve future fire prevention strategies.
g. The system should have 90% accuracy for detection and alerts.

12.1.1.4. Vehicle Count Analytics at Parking Area

The IA shall implement the vehicle count use cases by using Artificial Intelligence through various camera-based Vehicle count analytics in Shri Jagannath temple & Grand Road areas. Artificial Intelligence through Cameras shall be equipped with advanced computer vision algorithms that can detect and count vehicles in real-time. Artificial Intelligence through Cameras shall identify and detect vehicles entering and exiting the parking lot.

a. By detecting vehicles entering and exiting the parking lot, the AI cameras shall count the number of vehicles present at any given time. This information shall be used to determine the occupancy level of the parking lot and provide useful insights on parking demand and availability.
b. Vehicle count analytics shall also provide data on the occupancy levels of the parking lot at different times of the day. This information shall help in optimizing parking operations, making data-driven decisions on predicting parking demand during peak days.

c. AI cameras shall be programmed to generate real-time alerts when the parking lot reaches predetermined occupancy thresholds. These alerts shall be sent to parking attendants/managers/contractors and Police / Shri Jagannath temple Administration to ensure prompt action to manage the parking capacity.
d. It shall provide alerts on reaching the parking occupancy level upto 50%, 60%, 70%, 80% till 100% occupancy. It shall also be able to predict the time for various occupancy levels of parking based on historic trends.
e. The data collected through vehicle count analytics shall be stored and analysed over time. This analysis shall provide insights into parking utilization trends, patterns, and peak hours, enabling parking lot operators/contractors/Police & Shri Jagannath temple Administration to improve operational efficiency and implement effective parking strategies.
f. Dashboard view of all parking areas along with real time alerts shall be provided.
g. The system should have 90% accuracy for detection, counting and alerts.

12.1.1.5. Wall / Barrier Climbing Detection

a. System should monitor and detect both incoming and outgoing objects crossing a virtual line/boundary or tripwire in a designated zone.
b. Once wall climbing activity is detected, the system shall classify it as a potential security threat.
c. It should generate an alert when it detects an object crossing the line in the incorrect direction (as against the pre-configured correct direction)
d. The system should have 90% accuracy for detection and alerts.

Important Note:

It is to be noted that the validation of accuracy of the AI based Video Analytics shall be carried out in different time spans such as Morning, Evening, Night, etc. based on the various data sets collected for a specific time duration. Further, the validation of accuracy shall be undertaken by comparing the system generated data sets and manual observation. The threshold accuracy shall be minimum of 90% for all the above-mentioned AI based Video Analytics.

12.1.2. Technical Requirements of Integrated Crowd Management System:

1. Integrated Crowd Management System (ICMS) shall be based on advance technology & algorithms powered by Machine & deep learning techniques.
2. The user interface of ICMS shall support latest browser interfaces Firefox, Chrome etc.
3. ICMS shall be capable to support mixed architecture of deployments like On-Premises, On-Cloud or Hybrid Model for flexibility.
4. ICMS shall support distributed architecture with components like processing servers, application & database servers for best performance and results.
5. Each of the AI based video analytics use cases shall be able to run on several multi-vendor/OEM Open cameras video- feed seamlessly.
6. ICMS shall support failover architecture to avoid any single point of failure within the system/sites
7. The User Interface of ICMS shall provide a list of all the resources available in the system such as computing servers and cameras.

8. The User based access and interface of the ICMS shall be completely web interface that can be accessed from any system in the local area network (LAN) or wide area network (WAN) with login credentials. It shall allow multiple users to log in at the same time and receive real-time alerts and notifications.
9. The user / end users can log in from any personal computer device and yet should be able to access the system according to his/ her privileges
10. The events / incidents triggered from each of the AI use cases shall contain the information such as detected thresholds/limits/counts, timestamps, camera/video that generated the event, location and all other details as captured and finalised by the Authority. The User Interface shall have a grid and list view with all the events from different use cases, cameras etc.
11. The AI use cases on each camera shall allow setting up configuration of multiple detections zones such as lines /regions that can be used to define perimeters, regions of interest etc. within the field of view of camera.
12. ICMS shall support user with a hierarchical access level, with different access level for different users demarcated with respect to different locations within multi-site architectures.
13. ICMS shall support creation of custom user roles which allow specific privileges to a newly defined role.
14. ICMS shall support activity tracking features which captures user actions for audit and security purposes.
15. The System shall be a real-time video analytics engine that utilizes advanced image processing algorithms to turn video into actionable intelligence.
16. The system shall be open to offer standard integration tools like Web/REST APIs and shall be integrated with the VMS & Integrated Command & Control Centre (ICCC) applications of Puri City and VMS to be proposed by the bidder under the scope of this RFP.

12.1.3. Attribute-based Search Analytics for Video Summarization System

1. It has been decided to implement Video summarization System services which can be dynamically applied on live video feed of identified cameras and on recorded or exported video feed. The Attribute based Analytics for Video summarization system shall be based on computer vision and AI (Artificial Intelligence) technology enabling rapid video review, search, quantitative video insights and smart alerting, thereby shortening time-to-target to detect and mitigate security threats and enhancing safety and operational optimization significantly. System shall enable generation of Summarization of video sourced from both recorded offline-video files and online VMS platforms with full case management, multi-camera search, similar appearance and face recognition (as applicable)

2. The proposed solution shall work in two modes, one will be online mode where system services would be installed on minimum 100 cameras which will work with streaming camera feeds and does not required to be exported on to the Video Summarization System for processing the videos, whereas, in second mode, which is an offline mode where any 100 camera feeds can be uploaded on video summarization application for processing the Videos to conduct quick post-incident video review.
3. System shall facilitate leveraging of quantitative video analysis-derived intelligence for informed, data-driven decision-making, including advanced trend and dimensional (area, path, duration and other) KPI analysis as well as full dash boarding and scheduling capabilities.

4. System shall be able to generate live alerts thereby delivering proactive response to critical user-defines events ensuring enhanced safety and security.
5. System shall be able to perform the video analysis on the pre-recorded files. Additionally, it shall be integrated with the video management solution proposed by the IA and existing VMS of Puri ICCC project. The proposed system shall be able to run on existing CCTV Surveillance Cameras/VMS system available in Puri ICCC project.
6. System shall automatically extract all the moving objects (People/Vehicle/Animal) from the original video and efficiently reconstructs and without altering the original image/video/data simultaneously displaying events that have occurred at different times.
7. System shall rapidly search people and vehicles of interest, using a range of appearance and movement filters, across video feeds from multiple cameras.
8. System shall instantly locate people, vehicles and items of interest by searching for similar looking objects or by using facial recognition (as applicable).
9. System shall dynamically visualize Key performance (KPI) Indicators (Traffic Patterns, Visitor/Pedestrian count, general trends & Insights) derived from extracted video objects and their classification for comprehensive business intelligence.
10. System shall summarize the daily alerts and send the notifications.
11. Minimum Object Search Criteria, but not limited to:
    a) Time Range – Shall be able to limit the search criteria to specific time ranges
    b) Source – Shall be able to limit the objects to specific CCTV Camera feed or offline pre-recorded video files
    c) Classes – post-analysis, reviewed video shall be shown based on People, Two- Wheeled Vehicles, Other Vehicles and Animals with following categories:
        - People Class: Man, Woman, Boy, Girl etc.
        - 2-Wheeled Vehicle Class: Bicycle, Motorcycle etc.
        - Other Vehicles Class: Car, Pickup, Van, Truck, Bus, etc.
        - Animals Class: Dog, Cat, Bird, Horse, Elephant etc.
    d) People Attributes – Shall be able to select the attributes within the people class to refine the search such as:
        - Bags: Backpacks, Handheld Bags
        - Hats: Hats, No Hats
        - Upper Wear: Short/No Sleeves, Long Sleeves
        - Lower Wear: Long, Short
    e) Colour - Identify objects according to any combination of various colours like Brown, Red, Orange, Yellow, Green, Lime, Cyan, Purple, Pink, White, Grey, and Black
    f) Size - Select objects based on their actual (real-life) size specified in meters.
    g) Dwell - Select objects dwelling for longer than a certain time period in a scene
    h) Area - Identify objects included or excluded within one or more user-defined areas.
    i) Path - Identify objects traveling along one or more user-defined paths
12. System shall generate near-real-time alerts based on any of the above-mentioned search and filter criteria.
13. Video Summarization System/Software should have capability to perform all the functionality on recorded video feeds (feeds of Minimum 2 MP Camera) of existing Puri ICCC project and cameras feeds to be established under the scope of this project, any other feeds from any other projects/stakeholders. The software shall essentially evolve to automate the suspect activity capture, other analytics and escalation; eliminate the need of human observation. The IA along with the respective OEM has to take entire responsibility of the analytics outcomes as

envisaged in the project without any issues (like bad image quality, bad video quality, camera focus, environmental disturbance etc.)

14. Performance Parameters:
    a) System shall be able to detect the minimum face size of at least 30x30 pixels.
    b) System shall be able to detect the faces across the multiple CCTV video sources
    c) System shall be able to detect selected objects from minimum 10 CCTVs at a time
    d) System shall use extensive AI Technology and perform video processing on suitable GPUs.
    e) System shall be integrated with the appropriate database software for maintaining the various alerts and analysed video feeds.
    f) System shall be able to provide video Summarization for 2 hrs. video in less than 2 mins with selected objects highlighted.

15. IA is expected to provide video summarization solution using AI & deep learning in such a way so that during the first week of operation the accuracy of provided alerts will be of at least 80% accuracy (true alerts/total alerts). In future, IA should train their AI & deep learning model in such a manner so that the accuracy can increased by at least 5% week on week until accuracy be achieved to 100% within first month of operation considering the significance of Shri Jagannath temple area & Grand Road area. IA shall provide all the new updates/patches of updates during the project life cycle.
16. The proposed solution should have the provision to add 50% additional cameras scope for offline/online mode which will be deployed during the project life cycle depending upon the requirements from the Authority.

13. Contact Centre/Help Desk

The contact centre needs to be operational in Puri ICCC with a capacity of 15 contact centre operators (4 no of Manpower in 3 shifts 24*7*356 and 1 no of reliver for back up (total 3 for 3 shifts)) for City Helpline (toll free number shall be provided by authority). This contact center infrastructure has been established and utilised in Puri city.
The authority has decided to augment the capacity 15 contact centre system operators. The IA shall be responsible for:

a. Deployment of contact centre solution for 15 operators through provisioning of the required contact management software/CRM, IT infrastructure (desktops/workstations), IP Phone or microphones as deem fit to meet and exceed the project requirements however additional operators may be asked during critical/important events/occasions. The bidder is required to submit price discovery for these items in the relevant section of the RFP.
b. Deployment of contact center operators for a period of

1. Deployment of Contact Center Solution:

The proposed system should have following functionalities:

a. Automatic call distribution System shall assist, support and guide Pilgrims/visitors/citizen of Puri City
b. Should have voice recording for both Inbound and Outbound Calls
c. Should have Realtime dashboard as per user requirement

d. Should have historical reporting of all calls attended, missed, etc. along with following reporting facility:
   - Should provide real-time and historical reports
   - Inbound Call History
   - Inbound Call Received by Agents & Call Duration
   - Outbound Call History
   - Outbound Call Dialled Number with Duration
   - Agent Call Received History
   - Day/Month Wise Inbound/Out-Bound Call Details
   - Total Dropped call Details
   - Abandoned call report
   - Should have Time-Line Display in real-time reports
   - Should have Interactive Dashboard
   - should provide Contact Summary Report
   - Should provide agent based, skill-based reports
e. Should have automatic identification of incoming number based on landline and mobile number mapping.
f. Should have call recording mapped to incident tickets.
g. Should have inbound and outbound capability
h. Should have call control, multiscreen web chat, email, live data reporting, phonebook, multiline support, speed dial facility.

The proposed system should have following technical Specifications:

a. IP Push to Talk Radio: Instant communication to critical first responders via push to talk over IP. This shall enable All communication across various business sites.
b. The radio over IP solution must integrate any analogy or digital radio system, any to any Push To Talk (PTTT) communications.
c. The system shall create virtual talk groups (VTGs) to facilitate Push-to-Talk (PTT) communications between users of multiple types and technologies of Land Mobile Radios with users of PCs, landline phones, cellular and android phones, and IP phones.
d. IP PBX should support the flexible connection of Analog, Digital & IP (H.323 and SIP) Desk Phone in any combination, Mobile WLAN and Soft Phones within one system.
e. The system shall provide a High Availability option of adding a secondary hot standby server to provide high availability with no single point of failure. If a primary server fails, the secondary server automatically takes over service without communication interruption.
f. The solution must send encrypted data for PTT communications.
g. The system shall provide a web service API to integrate System with third party applications including ICCC system.
h. The system shall support role-based management to provide compartmentalized functions for personnel who need to perform different roles.
i. System should be capable to the system shall provide an easy-to-use Web interface. Authorized personnel shall be able to access the System Server from any location by using a supported browser and a network connection.
j. The system shall provide Loop Prevention: As multiple dispatchers patch channels together, there is always the possibility of creating a channel loop that causes audio feedback into the

communication path. The system should automatically identify potential audio loops and resolve them before they become an issue.

k. The System shall provide an audit trail for analysis, critique, and operations management. Detailed activity logging shall allow administrators to determine which user actions were performed and when they were performed.
l. Agent Desktop should display live skillset-related statistics as below:
m. It should display number of calls waiting
n. It should display max wait time before being connected to an agent
o. It should display the number of Agents available and not ready
p. It should Display Agent statistic chart
q. Supervisor should be able to change Agent status from ready to not ready and vice-versa,

The required IT infrastructure including workstations / laptops / desktops along with microphone or IP phones shall be provided by the Implementation Agency for operationalisation of 30-seater Contact Center.

2. Deployment of Contact Centre operators

The IA is required to provide suitable manpower for contact centre operations. The exact role of these personnel and their responsibilities would be defined and monitored by authority and respective departmental personnel. IA shall be required to provide such manpower meeting following requirements:

a. All such manpower shall be minimum graduate pass.
b. All such manpower shall be without any criminal background / record.
c. Authority reserves the right to carry out background check of the personnel proposed on the Project for verification of criminal record, at the beginning of deployment or during deployment.
d. IA shall have to replace any person, if not found suitable for the job.
e. All the manpower shall have to undergo training from the IA for at least 15 working days on the working of project. Training should also cover dos & don'ts and shall have few sessions from Authority and Stakeholders/End User Department officers on right approaches for contact center operations.
f. Each person shall have to undergo compulsory 2 days training every month
g. Operational Manpower shall work in 3 shifts, with no person being made to work/operate for more than 8 hours at a stretch.
h. Detail operational guideline document shall be prepared during implementation which shall specify detail responsibilities of these resources and their do's & don'ts.
i. The current estimation of the manpower required from the IA is as follows:

S. No.	Description	Quantity
1	Contact Centre Manpower for Integrated City Surveillance System (ICCC) Helpline Number a. 15 resources including 1 Team Leaders in each shift b. 3 shifts in a day of 8 hours each	15

S. No.	Description	Quantity
	c. Additional / back up manpower in case of any leaves / absence shall be considered by IA	

14. Technical Requirements

The functional requirements and technical specifications provided in the below sections and at other sections in this RFP are indicative and carry guiding rule. The IA is free to offer products and solutions which meet requirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards & best practices adopted in the industry. The IA is encouraged to design an optimized solution which is technically superior, innovative, proven, better in terms of functionality and is cost effective. The IA is fully responsible for the specified outcome to be achieved. All cameras RTSPS, AES 256 encryption, SHA256 and RSA2048, Firmware Anti-rollback, TRNG and encrypted firmware.

Pre-Qualification Criteria for Camera OEMs			
Sr. No	**Component**	**Selection Criteria**	**Compliance (Yes/No)**
1.	OEM Capability and Authorized Service Support	• OEM of IP CCTV cameras should have supplied at least 50,000 IP CCTV cameras in India or globally during the last 05 years. • OEM of IP CCTV camera should have successfully completed at least one order for supply of minimum 10,000 numbers of IP CCTV cameras per order during the last 05 years. *Note: <xxx> - Numbers to be decided during procurement process* • OEM (or via authorized service partner / distributor) should have authorized service centre in India since last 03 years.	
2.	Mandatory Certifications	• OEM shall hold valid certifications: • ISO 9001 (Quality Management) • ISO 14000 (Environmental Management) • OHSAS 18001: 2007 or ISO 45001 (Occupational Health & Safety).	
3.	Compliance with Indian CCTV Standards	All IP / CCTV models must comply with Essential Requirements for Security of CCTV issued by MeitY (effective 6th June 2024) and BIS (effective 9 April 2025).	
4.	Testing & Certification	• Testing for Essential Requirements shall be through STQC-approved labs. • Safety testing through BIS-approved labs.	

Pre-Qualification Criteria for Camera OEMs			
Sr. No	**Component**	**Selection Criteria**	**Compliance (Yes/No)**
5.	Public Procurement / Make in India	OEM should comply with applicable Public Procurement Orders (MeitY) and "Make in India"/local content norms wherever applicable.	
6.	ONVIF & Prohibited Standards	• OEM for Cameras must be listed on the ONVIF website • Products must be ONVIF compliant (not merely conformant). • Products shall not implement GB28181 / GB/T 28181-2011 standards or possess China Compulsory Certification (CCC). • Online verification of OEM in ONVIF website must be available. OEM must not be banned, suspended or blacklisted by ONVIF within the last five years from the date of publishing the bid.	
7.	Ownership & Traceability	MAC addresses and serial numbers of cameras and key components must be registered in the name of the OEM supplying the equipment.	
8.	Cybersecurity & Code Integrity	• Cameras, firmware, SDK, APIs shall be free from malicious code (viruses, trojans, spyware, worms). • No code shall tap network data or inhibit designed functions. • OEM will be liable under IT Act, 2000, IT Amendment Act, 2008 and BNS, 2023 for malicious software or backdoors.	
9.	Other PQ Norms	• Vendor must submit Data sheet & catalogue for all the product quoted by them. Quotation without data sheet & catalogue will be summarily rejected. • If any information is found to be false during the evaluation of the offer, it is bound to be rejected. • The Bidder/OEM should have local service support for after sales & service. Any problems reported by the department should be attended to within 48 hours. Failing to do so will attract Penal charges for the period the system was not fully functional.	

14.1.1. Fixed Cameras (Outdoor Box/Bullet) for Surveillance

Outdoor Fixed Camera or Bullet Camera - 4MP			
Sr. No	**Parameter**	**Specifications**	**Compliance (Yes/No)**
1.	Image sensor	1/3"Progressive Scan CMOS or better	
2.	Max Image Resolution	2560x1440 or better	

3.	Lens	5 to 50 mm lens, Auto/DC/P-Iris, motorized varifocal or better	
4.	True Day and Night	Yes	
5.	Wide Dynamic Range	True WDR/DWDR of 120dB or better	
6.	Minimum Illumination / Light Sensitivity	Colour 0. 08 Lux or better, B/W 0 Lux or better	
7.	IR Distance	IR distance-50m Or better	
8.	Shutter Speed	Auto/Manual, 1/1~1/10000s	
9.	Video Compression	H. 265 or better	
10.	Resolutions and frame rates (H. 265)	Minimum 4MP with 25/30fps or better	
11.	Video Streams	Individually configurable minimum 03 H. 265 or better video streams	
12.	Streaming Method	Unicast, Multicast along with multi stream support	
13.	Local storage	SD Card Slot with 128 GB or better Support with provided 128 GB card	
14.	Image Settings	Brightness, Sharpness, Contrast etc.	
15.	Supported Protocol	HTTP, HTTPS/SSL/TLS, TCP, ICMP/RTSP, RTP, UDP, IGMP, RTCP, SMTP, FTP, DHCP, UPnP/ARP/DNS, SMTP, Ipv4, Ipv6, 802. 1x(EAP)	
16.	Ethernet Port	RJ-45 (10/100Base-T) Mbps or Better	
17.	ONVIF	Profile S, G or Profile S, G, T	
18.	Operating Temp	-10 °C ~ 55 °C, Up to Humidity 90%	
19.	HLC, BLC	Auto (Both the attributes must be available and shall function in auto mode in either of the case)	
20.	IR - Internal/External	IR 50 meters to be considered Internal or external	
21.	Housing	IP 66 or better Rated IK 10 rated for outdoor use	
22.	Certifications	BIS-IS13252 And Cyber Security Certified by STQC as per IoTSCS and meet the essential requirement issued by MeitY.	
23.	Power Requirement	POE/POE+	
24.	Mounting Accessories	For pole and surface mount with L/C Brackets	

25.	Audio	1 Channel Audio IN/ 1 Channel Audio Out or Built In MIC/ 1 Channel Audio Output, Support two-way audio (Optional)	
26.	MTBF	Min 50000 Hours or better	
27.	Misc.	The Camera to be provided by the OEM/bidder should not be complying to GB28181, GB/T28181-2011 standards and there should be no option to activate or deactivate GB/T 28181 standards in the camera web page/settings.	
28.	Warranty & support	Camera Warranty Should include with 5-year comprehensive warranty with no additional cost for change, replacement of parts, labour, consumable, shipment, insurance etc. 24x7 support with 4 hours of response time & 48-hour resolution time.	

14.1.2. PTZ Cameras for City Surveillance

PTZ Camera - 4MP, 30x Optical Zoom			
Sr. No	**Parameter**	**Specifications**	**Compliance (Yes/No)**
1.	Image sensor	1/3 -in. Progressive CMOS or better	
2.	NUMBER OF PIXELS/Resolution	4MP @ 25/30fps	
3.	Optical Zoom	30X or better	
4.	Digital Zoom	16X or better	
5.	Min. Illumination	Colour 0. 08 Lux or better, B/W 0 Lux or better	
6.	WDR	True WDR/DWDR 120 db or better	
7.	Focal Length	4. 5 mm - 135 mm or 4. 3 mm - 129 mm or 4. 8 mm - 144 mm or 6 mm - 180mm	
8.	Max Aperture	F1. 5 - F5. 0	
9.	IR Distance	100 m or better	
10.	Defog	On/Off	
11.	PAN Travel	360° endless	
12.	TILT Travel	TILT Travel: 0 to 90°, auto flip 90°/180 for tilt travel starting from 0 to 90° for both the axis	
13.	Manual PAN Speed	Up to 180°/s or better	
14.	Manual TILT Speed	Up to 120°/s or better	
15.	Preset Speed	Pan: 240°/s; Tilt: 200°/s or better	
16.	Presets	256 or better	
17.	Image Rotation	Flip	
18.	Language support	English	
19.	Video Compression/Codec	H. 265 or better	

20.	Streaming Capability	Individually configurable minimum 03 H. 265 or better video streams (multicasting)	
21.	Frame Rate	4 Mega Pixel @ 25FPS or better 2 Mega Pixel @ 60FPS or better	
22.	Day and Night	Automatic, Colour, Mono	
23.	White Balance	Auto / Manual /ATW/Indoor/Outdoor/Daylight lamp/Sodium lamp	
24.	Ethernet	RJ-45 (10/100Base-T)	
25.	Protocols	IPv4, IPV6, HTTP, HTTPS, FTP, SMTP, UPnP, SNMP, DNS, DDNS, NTP, RTSPS, RTP, TCP, UDP, IGMP, ICMP, DHCP, 802. 1x (EAP)	
26.	Streaming Method	Unicast, Multicast along with multi stream support	
27.	Local Storage	SD Card Slot with 128 GB or better	
28.	Power	DC24 (1. 5A) / 24 VAC, 3 A (±10%), PoE+ (802. 3at)/PoE+	
29.	Mount	Wall / Pole Mount	
30.	Working Temperature	-10 °C ~ 55 °C, up to Humidity 90%	
31.	ONVIF	Profile S, G or Profile S, G, T	
32.	Certifications	BIS-IS13252 And Cyber Security Certified by STQC as per IoTSCS and meet the essential requirement issued by MeitY	
33.	Mounting Accessories	For pole and surface mount with L/C Brackets	
34.	Housing / Protection level	Weather-proof IP66 or better, Vandal-proof IK10	
35.	Audio	1 Channel Audio IN/ 1 Channel Audio Out or Built In MIC/ 1 Channel Audio Output, Support two-way audio (Optional)	
36.	HLC, BLC	Auto" (Both the attribute must be available and shall function in Auto mode in either of the case)	
37.	MTBF	Min 50000 Hours or better	
38.	Misc.	The Camera to be provided by the OEM/bidder should not be complying to GB28181, GB/T28181-2011 standards and there should be no option to activate or deactivate GB/T 28181 standards in the camera web page/settings.	
39.	Warranty & support	Camera Warranty Should include with 5-year comprehensive warranty with no additional cost for change, replacement of parts, labour, consumable, shipment, insurance etc. 24x7 support with 4 hours of response time & 48-hour resolution time.	

14.1.3. IR Illuminators

External IR Illuminator for ANPR Camera	

Sr. No	Parameter	Specifications	Compliance (Yes/No)
1.	Wavelength	850 nm	
2.	Range	80m or better	
3.	Beam Control	10 degrees to 60 degrees (interchangeable or selectable)	
4.	Power	12-24 Volts DC	
5.	Controls	Built-in photocell (day/night auto), telemetry/dry contact input for sync with ANPR camera shutter	
6.	Housing	Aluminium	
7.	IP protection	IP 66 or better	
8.	Vandal Proof	IK 10	
9.	Temperature	minus 15 degrees to plus 50 degree or better; Humidity 95%RH or less (non-condensing)	
10.	Mounting	Adjustable bracket suitable for pole/gantry/camera housing	
11.	Quality	CE/ FCC/ RoHS.	
12.	Warranty & support	IR Illuminator Warranty Should include with 5-year comprehensive warranty with no additional cost for change, replacement of parts, labour, consumable, shipment, insurance etc. 24x7 support with 4 hours of response time & 48-hour resolution time.	

14.1.4. ANPR Camera

Outdoor Fixed ANPR Camera with IR Illuminator - 2 MP			
Sr. No	**Parameter**	**Specifications**	**Compliance (Yes/No)**
	Image sensor	1/3” Progressive Scan CMOS Sensor 2. 0 megapixel or better CMOS.	
	Max Image Resolution	1920 x 1080 (2MP)	
	Lens	C/CS with 5- 50 mm or better	
	True Day and Night	Yes	

	Wide Dynamic Range	True WDR/DWDR of 120dB or better	
	Minimum Illumination / Light Sensitivity	Colour 0. 08 Lux or better, B/W 0 Lux or better	
	IR Filter	Automatic Built in IR Cut filter	
	IR Distance	IR distance- 80m Or better; with Inbuilt or External IR	
	Shutter Speed	Configurable electronic shutter, up to 1- 1/10000s or faster for freezing number plates of moving vehicles.	
	Video Compression / Codec	H. 265 or better	
	Frame rates	50/60fps or better	
	Video Streams	Individually configurable minimum 03 H. 265 or better video streams	
	Streaming Method	Unicast, Multicast along with multi stream support	
	Local storage	SD Card Slot with 128 GB or better Support provided with 128 GB card	
	Image Settings	Brightness, Sharpness, Contrast etc.	
	Supported Protocol	HTTP, HTTPS/SSL/TLS, TCP, ICMP/RTSP, RTP, RTSPS, UDP, IGMP, RTCP, SMTP, FTP, DHCP, UPnP/ARP/DNS/ DynDNS, SMTP, Ipv4, Ipv6, EAP-TLS/EAP-MD5/SHA	
	Ethernet Port	RJ-45 (10/100Base-T) Mbps or Better	
	ONVIF	Profile S, G or Profile S, G, T	
	Operating Temp	-10 °C ~ 55 °C, Up to Humidity 90%	
	HLC, BLC	Auto" (Both the attribute must be available and shall function in Auto mode in either of the case)	
	Alaram Input / Output	Min 1/1 or better	
	Housing	Weather-proof IP66 or better, Vandal-proof IK10	
	Certifications	BIS-IS13252 And Cyber Security Certified by STQC as per IoTSCS and meet the essential requirement issued by MeitY	
	Power Requirement	DC12V/AC 24V/PoE power input/POE+	

	Mounting Accessories	For pole and surface mount with L/C Brackets	
	Audio	1 Channel Audio IN/ 1 Channel Audio Out or Built In MIC/ 1 Channel Audio Output, Support two-way audio (Optional)	
	MTBF	Min 50000 Hours or better	
	Defogger	Digital defogger/Defogger	
	Misc.	The Camera to be provided by the OEM/bidder should not be complying to GB28181, GB/T28181-2011 standards and there should be no option to activate or deactivate GB/T 28181 standards in the camera web page/settings.	
	Warranty & support	Camera Warranty Should include with 5-year comprehensive warranty with no additional cost for change, replacement of parts, labour, consumable, shipment, insurance etc. 24x7 support with 4 hours of response time & 48-hour resolution time.	

Note:

1. ANPR 2 Mega pixel camera / Sensor (True day and night): one per lane to be used to capture all vehicles including 2 wheelers. All types of number plates reflective type and standard type should be captured.
2. Colour images for day, monochrome images for night
3. Global shutter sensor or rolling shutter sensor with Image stabilization
4. Lens: True Mega pixel or better, Day & night, IR corrected, lens.
5. Flash power should be sufficient to capture vehicle images also at night which can help ANPR Camera to capture retro reflective and non-reflective number plates.
6. Cameras should be able to detect Number plates of Vehicle up to 100 Kmph @ 25/30/50/60 FPS without any distortion in image with recognition accuracy ≥ 85% in day/night conditions.

14.1.5. Field Junction Box

S. No.	Parameters	Minimum Specifications
1.	Size	Suitable size as per site requirements to house the field equipment
2.	Cabinet Material	GI with powder coated
3.	Material Thickness	Min 1.2mm

S. No.	Parameters	Minimum Specifications
4.	Protection	IP 55, Junction Box design should ensure to keep the temperature within suitable operating range for equipment's and should also avoid intentional water splash and dust intake
5.	Mounting	On Camera Pole / Ground mounted on concrete base
6.	Other Features	Rain Canopy, Cable entry with glands, proper earthing and Fans/any other accessories as required for operation of equipment's within junction box.

14.1.6. Poles for Cameras

S. No.	Parameters	Minimum Specifications
1.	Pole type	Hot Dip Galvanized after Fabrication with Silver coating of 86 micron as per IS:2629; Fabrication in accordance with IS-2713 (1980)
2.	Height	5-10 Meters (or higher), as-per-requirements for different types of cameras & Site conditions
3.	Pole Diameter	Min. 10 cm diameter pole (bidder to choose larger diameter for higher height)
4.	Cantilevers	Based on the location requirement suitable size cantilevers to be considered with the pole
5.	Mounting facilities	To mount ANPR, CCTV cameras, Switch, Junction Box etc. or any other device as decided by authority
6.	Pipes, Tubes	All wiring must be hidden, through tubes/pipes. No wires shall be visible from outside.

S. No.	Parameters	Minimum Specifications
7.	Foundation	Casting of Civil Foundation with foundation bolts, to ensure vibration free erection Please refer to earthing standards mentioned elsewhere in the document.
8.	Protection	Lightning arrester shall be provided, to protect all field equipment mounted on pole.

14.1.7. Edge Level Switch at Field Junctions

Sr. No.	Minimum Specifications
1	**Architecture**
	The should have minimum 8-port Class 4 POE and 4-port Class 6 POE and 2-port SFP+ ports, Should be DIN Mount Switch.
	The switch should support minimum 240W of POE power
	Should have 4GB RAM and 16GB Flash;Should have minimum 8 MB packet buffer
	Should have 1x RJ Console and 1x Alarm socket
2	**Layer 2/3 Feature**
	The switch should support VLAN and VLAN tagging for IEEE 802.1Q
	The switch should support STP standard IEEE 802.1D STP, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for faster convergence, and IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)
	The switch should support Bridge Protocol Data Unit (BPDU) tunneling transmits STP BPDUs transparently, allowing correct tree calculations
	The switch should support Internet Group Management Protocol (IGMP) Controls and manages the flooding of multicast packets in a Layer 2 network
	The switch should support Static routing
	Should support dual stack static IPv4 and IPv6 routing provides simple manually configured IPv4 and IPv6 routing
3	**Resiliency and Availability**

	Should support Uni-directional Link Detection (UDLD) to monitor link connectivity and shut down ports at both ends if unidirectional traffic is detected, preventing loops in STP-based networks.Should support ERPS(Ethernet Ring Protection Switching (ERPS) support for rapid protection and recovery in a ring topology).
	Should support EEE 802.3ad LACP supports up to 8 LAGs, each with up to 8 links per LAG
4	**QOS**
	Class of Service (CoS) sets the IEEE 802.1p priority tag based on IP address, IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and DiffServ
	Strict priority (SP) queuing,Traffic prioritization (IEEE 802.1p) for real-time classification
5	**Security and Management**
	Switch should support RA guard, DHCPv6 protection, dynamic IPv6 lockdown, and ND snooping
	The switch should support Strict priority (SP) queuing,Traffic prioritization (IEEE 802.1p) ,Class of Service (CoS) ,IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and DiffServ
	The Switch should support Network Time Protocol (NTP)/SNTP synchronizes timekeeping among distributed time servers and clients.
	The Switch should support IEEE 802.1AB Link Layer Discovery Protocol (LLDP) advertises and receives management information from adjacent devices on a network to facilitate easy mapping by network management applications
	The Switch should support ACLs filtering based on the IP field, source/ destination IP address/subnet, and source/ destination TCP/UDP port number on a per-VLAN or per-port basis
	The Switch should support multiple user authentication methods. Uses an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server to authenticate in accordance with industry standards
	The Switch should support Web-based authentication provides a browser-based environment, similar to IEEE 802.1X, to authenticate clients that do not support IEEE 802.1X
	The Switch should support MAC-based client authentication
	The Switch should support Identity-driven ACL to enable implementation of a highly granular and flexible access security policy and VLAN assignment specific to each authenticated network user
	The Switch should support STP BPDU port protection to block Bridge Protocol Data Units (BPDUs) on ports that do not require BPDUs and prevent forged BPDU attacks
	The Switch should support Port security to allow access only to specified MAC addresses, which can be learned or specified by the administrator
	The Switch should support Source-port filtering to allow only specified ports to communicate with each other
	The Switch should support Concurrent IEEE 802.1X, Web, and MAC authentication schemes per switch port accepts up to 32 sessions of IEEE 802.1X, Web, and MAC authentications
	The Switch should support Auto VLAN configuration for voice RADIUS VLAN uses a standard RADIUS attribute and LLDP-MED to automatically configure a VLAN for IP phones

	The Switch should support Management Interface Wizard to help secure management interfaces such as SNMP, SSH,SSL, Web.
6	**Environment/Warranty**
	The switch should have IP30 rating
	The switch support -40°C to +60°C operating temparture range
	The switch should support 5% to 95% of Humidity
	The switch should support AC or DC power supply
	Green initiative support for RoHS (EN 50581:2012) and WEEE regulations.
	The switch shall be offered with minimum five years hardware warranty with 24x7 Technical support from OEM directly

14.1.8. Online UPS for field locations

S. No.	Parameters	Minimum Specifications
1.	Capacity	Adequate capacity to cover all above IT Components at respective field locations
2.	Technology	IGBT based PWM Technology, True Online UPS, SNMP Card
3.	Input Frequency Range	Preferably 45 to 55 Hz
4.	Output Frequency Range	Preferably 45 to 55 Hz
5.	Output Voltage	Preferably 220VAC - 230VAC
6.	Voltage Regulation	Preferably +/-2% (or better) and with built in Over Voltage Cut off facility in the Device
7.	Frequency	Preferably 50 Hz +/- 0.1% (free Run Mode)
8.	Harmonic Distortion (THD)	Preferably < 3% (linear load)
9.	Output Waveform	Pure Sine wave

S. No.	Parameters	Minimum Specifications
10.	Output Power Factor	0.8 or more
11.	Battery Backup	Minimum 1 Hour
12.	Battery Type	Preferably Lead acid, Sealed Maintenance Free (SMF)
13.	General Operating Temperature	As Per local environment conditions
14.	Alarms & Indications	All necessary alarms & indications essential for performance monitoring of UPS like mains fail, low battery & fault detection
15.	Bypass	Automatic, Manual Bypass Switch
16.	Certifications	For Safety & EMC as per international standard

14.1.9. Structured Cabling Components

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

14.1.10. Electrical cabling component

Sr. No.	Parameters	Minimum Specifications
1.	Standards	All electrical components shall be design manufactured and tested in accordance with relevant Indian standards IEC's

15. Data Centre Equipment Specifications

15.1 Server

Sr. No.	Parameters	Minimum Specifications
1	Processor	Latest 6th Gen 64-bit x86 processor(s) with minimum 24 or higher Cores as per bidder design. Processor must support hyper/multi threading.
		Processor speed should be minimum 2.2 GHz
		Minimum 2 processors per each physical server.
2	RAM	Minimum 128 GB Memory in balanced configuration per physical server scalable up to 1TB. Fast fault tolerance or higher.
3	Memoery RAS	Advanced ECC to protect servers against single-bit errors as well as to protect against multi-bit memory errors within a single RAM chip as well as within a single memory module. Adaptive Double DRAM Device Correction (ADDDC), Fast Fault Tolerance.
4	Internal Storage	2 x 600 GB 12G SAS (10k rpm) or better
5	RAID Controller	Tri-mode SAS/SATA/NVMe RAID controller with RAID 1/5/6/10/50/60 support and with minimum 4GB cache. Offered controller must support mix-and-match up to 8 no's 12G SAS, 6G SATA, and 16G NVMe drives to the same controller.
6	Network interface	4 X 10G ports for providing Ethernet connectivity or equal Fiber ports as per bidder design
7	Power supply	Dual Redundant Power Supply

8	Interfaces	4 x USB 3.0, 1 x VGA, 1 x 1GbE BaseT dedicated OOB Management with perpetual system management licensing. Minimum three PCI-E 5.0 x16 or higher slots.
9	Compliance and System Security	ACPI 6.4, PCIe 5.0, USB 3.0, UEFI, OCP, FIPS 140-2, TPM 2.0, SMBIOS 3.4, IPMI 2.0, SNMPv3, TLS 1.2, ASHRAE A3/A4, CNSA, Secure Erase pf NAND data, Immutable Silicon Root of Trust. EAL4 or higher common criteria certification for the OOB management subsystem.
10	System Management	One-click secure erase, security dashboard, virtual media, multi-factor authentication, Dedicated space earmarked in the IPMI OOB system to be used as a repository for firmware, drivers and software components for rollback/patch faulty firmware. REST API.
11	OEM ranking	OEM should be ranked within top 3 as per IDC report for any one of the previous four quarter in India for server.
12	Operating System	64-bit latest version of operating system as per requirement of AI solution
13	Form Factor	Maximum 2U rack mount server with Bezel, Bezel Locking Kit, Chassis Intrusion Detection Kit, Sliding rails, and AC power cords.
14	Virtualization	Shall support Industry standard virtualization hypervisor like Hyper-V, VMWARE, HPE, Red Hat etc.
15	Warranty	Five years on-site comprehensive OEM Warranty Support with 24X7 coverage and access to OEM TAC/support. OEM shall have their own support portal to log the case online and historical data about cases must be available in the same portal.

15.2 Servers for Video analytics

Sr. No.	Parameters	Minimum Specifications
1	Processor	Latest 6th Gen 64-bit x86 processor(s) with minimum 24 or higher Cores as per bidder design. Processor must support hyper/multi threading.

		Processor speed should be minimum 2.2 GHz Minimum 2 processors per each physical server.
2	RAM	Minimum 128 GB Memory in balanced configuration per physical server scalable up to 1TB. Fast fault tolerance or higher.
3	Memoery RAS	Advanced ECC to protect servers against single-bit errors as well as to protect against multi-bit memory errors within a single RAM chip as well as within a single memory module. Adaptive Double DRAM Device Correction (ADDDC), Fast Fault Tolerance.
4	Internal Storage	2 x 600 GB 12G SAS (10k rpm) or better
5	RAID Controller	Tri-mode SAS/SATA/NVMe RAID controller with RAID 1/5/6/10/50/60 support and with minimum 4GB cache. Offered controller must support mix-and-match up to 8 no's 12G SAS, 6G SATA, and 16G NVMe drives to the same controller.
6	Network interface	4 X 10G ports for providing Ethernet connectivity or equal Fiber ports as per bidder design
7	Power supply	Dual Redundant Power Supply
8	Interfaces	4 x USB 3.0, 1 x VGA, 1 x 1GbE BaseT dedicated OOB Management with perpetual system management licensing. Minimum three PCI-E 5.0 x16 or higher slots.
9	Compliance and System Security	ACPI 6.4, PCIe 5.0, USB 3.0, UEFI, OCP, FIPS 140-2, TPM 2.0, SMBIOS 3.4, IPMI 2.0, SNMPv3, TLS 1.2, ASHRAE A3/A4, CNSA, Secure Erase pf NAND data, Immutable Silicon Root of Trust. EAL4 or higher common criteria certification for the OOB management subsystem.
10	System Management	One-click secure erase, security dashboard, virtual media, multi-factor authentication, Dedicated space earmarked in the IPMI OOB system to be used as a repository for firmware, drivers and software components for rollback/patch faulty firmware. REST API.
11	OEM ranking	OEM should be ranked within top 3 as per IDC report for any one of the previous four quarter in India for server.

12	Operating System	64-bit latest version of operating system as per requirement of AI solution
13	Form Factor	Maximum 2U rack mount server with Bezel, Bezel Locking Kit, Chassis Intrusion Detection Kit, Sliding rails, and AC power cords.
14	Virtualization	Shall support Industry standard virtualization hypervisor like Hyper-V, VMWARE, HPE, Red Hat etc.
15	GPU	Minimum 2 GPU each server, L4 or better (server grade GPU cards not workstation grade)
16	Warranty	Five years on-site comprehensive OEM Warranty Support with 24X7 coverage and access to OEM TAC/support. OEM shall have their own support portal to log the case online and historical data about cases must be available in the same portal.

15.3 Virtualization

Sr. No.	Minimum Specifications
1	The bidder shall propose direct back-to-back OEM support on 24x7x365 coverage basis for proposed solution with unlimited number of incidents.
2	The bidder shall ensure that all the proposed software components as part of the Virtualization solution shall have the ability to run on any standard commodity server infrastructure and external FC storage without having any dependence on specific make/model of infrastructure components and without dependence on storage CSI driver.
3	Offered virtualization software solution shall be qualified for both Intel as well as AMD architecture and shall have capability to provide high availability.
4	Offered virtualization solution shall be supported with all leading Guest Operating Systems.
5	Offered virtualization solution shall support migration of a running virtual machine from one host to another within the same cluster with zero downtime.

6	Offered virtualization solution shall automatically restart virtual machines on another host in the same cluster in the event of an unexpected host failure within the cluster.
7	The offered Hypervisor shall dynamically schedule the placement of virtual machines within a cluster based upon optimal workload distribution across the cluster.
8	Virtualization Management software should be available independent of failure of host/node, and OS.
9	The offered Hypervisor shall support migration the virtual disk(s) of a running of virtual machine from one storage datastore to another with zero downtime.
10	The offered Hypervisor solution shall include suitable data backup solution which shall be able to protect VM and Hosts to Target Storage provider. Offered backup engine shall be able to use at least CIFS, NFS, S3 from Storage providers as a backup target.
11	The offered hypervisor shall also have functionality to integrate with third party backup software like Veeam, Commvault, Rubrik, Zerto etc.
12	The offered backup engine shall have deep integration into the instances / VM provisioning so that all newly created instances / VMs are protected and backed up automatically.
13	The offered backup engine shall also support critical features like Scheduling of backup, backup retention counts, on-demand backup etc.
14	The offered Hypervisor shall support and integrate with storage - Object Buckets which can be used for Backup, Archives, Deployment and Virtual Images storage targets.
15	It shall be possible to browse, upload, download, or delete files from Bucket and shall support all well-known object storage from AWS, Azure, Google, Dell-EMC ECS, OpenStack Swifts buckets etc.
16	The offered Hypervisor shall also allow creation of file share based NFS and CIFS protocols which can be used for Backup, Archives, Deployment and Virtual Images storage targets. It shall be possible to browse, upload, download, or delete files from File share and shall support all various file share protocols like CIFS, NFS, Local Storage and all well-known industry leading file storage arrays.

17	The offered Hypervisor shall support running virtual machines on external storage via iSCSI, NFS, and Fibre Channel. Such storage connectivity should not be dependent only upon CSI drivers i.e. storage without having CSI driver should be supported.
18	The offered Hypervisor management engine shall have a concept of grouping of resources into a common identity, comprises of resources like Clouds, hosts, VMs, network, resource pools, data stores etc. so that required users can be assigned to it.
19	The offered hypervisor management engine shall allow users to configure their photo, username, password, email, theme, 2FA, Linux and Windows VM login credentials from the console.
20	The offered Hypervisor management engine shall support additional private cloud provider and hypervisor, preferably VMware, from the common interface without any additional coding.
21	The offered hypervisor Management engine shall allow administrator to create service plan or t-shirt size based on CPU, Memory and Storage and shall be available to users while creating / provisioning the instance / VMs
22	Services plan shall also have the option to provide custom ranges and flexibility to provisioning users for providing predefined limit for number of additional volumes, customization of Volumes, number of cores etc.
23	The offered Hypervisor shall have internal user management engine, integration with external directory-based providers – Active directory and LDAP, SAML based providers – Okta, OneLogin, Azure AD SAML etc. It shall be possible for mapping of External integration provider users with offered hypervisor roles.
24	The offered Hypervisor shall have Integration with external IPAM providers like Infoblox, phpIPAM, BlueCat, SolarWinds etc. to automate the reservation of an IP address for the virtual machine during the provisioning process.

25	The offered Hypervisor shall have Integrate with external DNS providers like Infoblox, Microsoft DNS, BlueCat, SolarWinds etc. to automate the creation of DNS records for a virtual machine during the provisioning process.
26	The offered Hypervisor shall execute Bash or PowerShell scripts during virtual machine provisioning to automate system bootstrapping operations.
27	The offered Hypervisor shall also support the execution of Bash and PowerShell scripts on provisioned and discovered virtual machines like an operational workflow.
28	The offered Hypervisor shall support both expansion and shrinking of VM cluster
29	The offered Hypervisor shall support both internal and external Credential store for securely pulling in the username and password, access and secret key along with key pair and SSH certificates.
30	The offered hypervisor software shall provide the flexibility to bring / upload OS images. While uploading the OS image, it shall be possible to define the location and provide the flexibility to use internal space within the hypervisor cluster or using appropriate available S3 bucket or file share.
31	The offered Hypervisor shall provide global search to facilitate search of Instances, Users, cloud, group, hosts and networks.
32	The offered Hypervisor shall allow creation of Wiki, which shall be RBAC-controlled, auditable Wiki that allows easy access to information, notes, configurations or any other data needed to be referenced or shared with others.
33	Consolidated dashboard for the offered Hypervisor shall highlight the overall environment status, System Status, Alarms, log history, Instance status, Instance status by configured clouds, cluster workloads etc.
34	The offered Hypervisor management engine shall provide activity report like provisioning tasks, Users related tasks etc. It shall be able to search the specific activity.
	Licensing
35	Bidder shall provide the licenses for list of servers as per their offered solution.
	Support

36	Five years OEM software support with 24X7 coverage and access to OEM TAC/support. OEM shall have their own support portal to log the case online and historical data about cases must be available in the same portal.

15.4 Storage

Sr. No.	Parameters	Minimum Specifications
1	Operating System & Clustering Support	The storage array should support industry-leading OS platforms including Windows 2016/2019/2022, VMware and Linux. Offered Storage Shall support all above operating systems in Clustering.
2	Capacity & Scalability	The Storage Array shall be offered with 2000 TB Usable Capacity using NLSAS drives and 100TB usable capacity using SSD drives. For effective power saving, Storage subsystem shall also support SFF drives with the addition of required disk enclosures. Storage shall be provided with suitable OEM bezel kit as well as bezel lock kit.
3	Front-end Ports & Back-end Ports	Offered Storage system shall be supplied with 8 * 25G IP ports and shall support 12G SAS Back-end connectivity.
4	Architecture	The storage array should support dual, redundant, hot-pluggable, active-active array controllers for high performance and reliability.
5	No Single point of Failure	Offered Storage Array shall be configurable in a No Single Point of configuration including Array Controller card, Cache memory, FAN, Power supply etc.
6	Disk Drive Support	Storage system shall support Enterprise SAS spinning drives, SSD and near line SAS / 7.2K RPM drives. The storage array offered shall also have support for FIPS 140-2 validating self-encrypted drives.
7	Cache	Offered Storage Array shall be given with Minimum of 48GB cache. Cache shall be backed up in case of power failure for indefinite time either using batteries or capacitors or any other equivalent technology. Offered Storage shall also have optional support for Flash cache using SSD / Flash drives. Offered Flash cache shall be tuned for random read operations and shall remain activated even at less than 70% of random average read workload.

8	Raid Support	Offered Storage Subsystem shall support Raid 1,10, 5 and Raid 6. All Raid Sets shall support thin provisioning. Vendor shall offer the license of thin provisioning for complete supported capacity of the array. Thin provisioning shall be supported with offered Flash Cache. Raid processing shall be offloaded to a dedicated ASIC instead of CPU. In case vendor is not supporting it then vendor shall ensure that additional 12GB cache per controller is configured to offset the raid processing workload.
9	Point in time and clone copy	Offered Storage array shall be configured with array-based Snapshot and clone functionality and shall be configured for minimum of 512 snapshot licenses. Offered Storage array shall support at-least 512 point-in-time copies (Snapshots) and 128 volume / Clone copies
10	Replication	The storage subsystem offered shall support storage-based replication to DR location. License for maximum supported capacity of the array shall be offered.
11	Virtualization and Thin provisioning	Storage offered shall be offered and configured with virtualization capability so that a given volume can be striped across all spindles of given drive type within a given disk pool. Disk pool shall support all listed raid sets of Raid 1, Raid 10, Raid 5 and Raid 6. Storage offered shall be configured with Thin Provisioning capability.
12	Data Tiering	Storage offered shall also be configured for Sub-Lun Data tiering in real time fashion across different types of drives within a given pool like SSD, SAS, NL-SAS etc. License shall be configured for maximum supported capacity of the array.
13	Global and dedicated Hot Spare	Offered Storage Array shall support Global hot Spare for offered Disk drives. At least 2 Global hot spare drives shall be configured for every 30 drives. Offered storage array shall have the support for distributed hot spare
14	Logical Volume & Performance	Storage Subsystem shall support minimum of 512 Logical Units. Storage Array shall also support creation of more than 120TB volume at controller level. Offered Storage shall have inbuilt performance management software. Configuration Dashboard shall show overall IOPS and MB/sec performance.
15	Load Balancing & Muti-path	Multi-path and load balancing software shall be provided if vendor does not support MPIO functionality of Operating system.

16	Performance	The storage offered shall have listed benchmark for performance of more than 100,000 in Raid 5 using appropriate drives at 8k block size. Vendor shall provide documentary proof for it.
17	Array Integration	Offered storage array offered shall have plug-in for VMware VCenter, Microsoft System center as well as vStorage APIs (VAAI) for array integration.
18	OEM Ranking	OEM should be ranked within top 3 as per IDC report for any one of the previous four quarter in India for storage OR OEM should be from the leaders category as per last published Gartner's magic quadrant report on "Primary storage".
19	Warranty	Five years on-site comprehensive OEM Warranty Support with 24X7 coverage and access to OEM TAC/support. OEM shall have their own support portal to log the case online and historical data about cases must be available in the same portal.

15.5 Backup Solution

Sr. No.	Minimum Specifications
1	Offered Disk to disk backup device shall be a purpose-built backup appliance and shall be certified to work with at-least 3 Backup application vendor ISV like HPE Zerto, Veeam and Commvault etc.
2	Offered device shall be offered with Minimum of 80TB of raw space scalable to more than 250TB
3	Offered device shall have separate dedicated drives for Operating System of appliance and shall not participate in data backup
4	Offered device shall also be scalable to at-least 200TB usable capacity in native mode (Without de-duplication and compression) and additional 400TB of native usable capacity using storage on the cloud like AWS, Azure or on object storage
5	Vendor shall not use any additional staging device in-between while moving the data from Disk based backup device to public cloud or object storage.
6	Offered device shall be protected with hardware raid 6 from the factory so that no raid configuration is required in field.
7	Offered device shall be protected with hardware raid 6 from the factory so that no raid configuration is required in field.

8	Offered device shall support emulation of both VTL and NAS target like NFS & CIFS.
9	Offered device shall have the ability to configure at-least combination of 64 tape Libraries & NAS targets along with 100,000 or more Cartridge slots in the single appliance.
10	Offered device shall have capability to do complete copy of data sets from on premise disk backup storage to Cloud storage instead of data tiering.
11	Offered device shall have capability to deliver selective restore from disk Library itself.
12	Offered Device shall integrate and utilize customer's current tape backup infrastructure in the following aspects:
	a) Compatibility with the existing backup server / media servers at customer.
	b) Compatibility with existing tape library and tape drives
	c) Compatibility with existing backup software
13	Offered device shall have integrated de-duplication license, low bandwidth replication license so that only unique non duplicated block transfers to remote / DR location.
14	Offered device shall have intelligence to understand both source based and target based de-duplication and shall be integrated with all well-known backup ISVs. At-least 3 ISVs shall be supported.
15	Offered device shall support receiving non duplicated data from remote locations or branch office directly from the application servers / Client servers Offered device shall support receiving non duplicated data from remote locations or branch office directly from the application servers / Client servers.
16	Ability to flexibly emulate tape drive/ tape formats LTO-Gen5, LTO-Gen6, and LTO-Gen7 etc.
17	Offered device shall have Minimum of 4 x 10/25Gbps SFP IP ports & 4 x 32Gbps ports. License and SFP for all ports shall be offered and configured
18	Offered Appliance Fiber channel ports shall support connectivity of servers either directly or via SAN switches while supporting the both source and Target based de-duplication
19	Offered disk-based backup device shall also support encryption functionality
20	Offered disk-based backup device shall also support dual authorization for preventing disruptive operations so that hackers shall not be able to execute or complete all critical operations like deletion of backup store, changing system time etc.

21	Dual authorization shall be approved by two separate accounts or entities instead of a single responsible account / entity so that all malicious actions such as ransomware attacks can be effectively prevented.
22	Dual authorization shall be independent of Backup ISV being used in the environment
23	Offered disk-based backup device shall also support Secure erase feature for protecting against unauthorized recovery of deleted data
24	Offered disk-based backup appliance shall support VLAN tagging. Offered IP ports of same type shall also support Port bonding in Adaptive Load balancing as well as in Active-backup mode.
25	Offered device shall support rated write performance of at-least 25TB per hour
26	Offered solution shall include the required backup software/engine & related license should be for 80TB front end capacity / 30 OS Instances. Required servers for running the backup software/engine shall be included in the solution.
27	Offered backup software/engine shall have following features/functionalities:
	a) The proposed backup software should be modular in architecture, allowing for components to be added and removed without requiring the backup system to be shutdown.
	b) Proposed backup software should be available on various OS platforms like Windows, Linux, IBM AIX, Solaris etc. The backup server should be compatible to run on both Windows and Linux OS platforms
	c) The proposed backup software should be able to recreate backed up data from existing volumes from metadata backups. The solution should offer recovery of specific volumes for recovery from metadata in case of a disaster recovery.
	d) Backup software should support agentless backups of applications residing in VMs like SQL, Exchange, SharePoint, Oracle, etc. with non-staged granular recovery of all these applications. It should support crash consistent VM level backup for all other workloads. Backup software should support SAP HANA backup integrated with HANA Cockpit.
	e) It should support various level of backups including full, incremental, differential, synthetic and virtual synthetic backups.
	f) Should have in-built calendar based scheduling system and also support check-point restart able backups for file systems.

	g) Should integrate with third party VTL which has data deduplication capabilities. Backup software must support Robotic/automated Tape library and the licensing of such library should be on the unlimited number of slots and not on the drive counts as additional drives are added to improve performance. Must support OST, VTL, Disk, NFS. CIFS for proposed backup disk appliance.
	h) It should also have configurable REST API support for management, administration and reporting on backup infrastructure via custom applications.
28	OEM should be ranked within top 3 as per IDC report for any one of the previous four quarter in India on Storage OR OEM should be from the leader's quadrant as per last published Gartner's primary storage MQ report.
29	Five years on-site comprehensive OEM Warranty Support with 24X7 coverage and access to OEM TAC/support. OEM shall have their own support portal to log the case online and historical data about cases must be available in the same portal.

15.5 Operator Workstation

Sl. No.	Parameter	Minimum Specification	Compliance (Yes/No)
1	Processor	Intel Core i7 or better	
2	Memory	32GB memory or higher	
3	Drive Controller	Integrated Intel Controller or similar	
4	Hard Disk Drive	512 GB SSD and 8TBx 1 no SATA HDD or higher	
5	Graphic Card	Nvidia 8GB or better	
6	Networking	1x Intel Ethernet Connection 10/100/1000 or better	
7	OS	Windows 11 Pro for Workstations (64-bit)	
8	Keyboard & Mouse	wired Keyboard & Mouse, should be of Same OEM make as workstation	
9	Monitor	21 inch FHD monitor with 1920 x 1080 resolution	

15.6 Next Generation Firewall (NGFW)

Sl. No	Item Description	Technical Specification	Technical Compliance (Yes/No)
1	**Architecture Requirement**	The proposed hardware based firewall should support minimum 19' (1 RU)	
		Proposed Firewall should not be proprietary ASIC based in nature & should be open architecture based on multi-core CPU's to protect & scale against dynamic latest security threats. Solution should propose built and provide Next Generation Firewall capabilities.	
		Proposed solution should be supplied with Primary & HA appliance which should be same model & features of primary device.	
		Appliance must have one Console port, dedicated one management Port, two USB port and redundant power supply	
		The device should have 8 x 1G Copper ports, 4 x 10G (Cu), 6 x 10G /25G SFP+ ports from day one. The device should be upgradable to 8 x 1G Cu ports, 2 x 40G and 4 x 10G in the same chassis in future.	
		Bidder should supply 4 x 10G Multi mode SFP+ and 2 x 1G SFP Multi mode module for each firewall. All SFP module should be OEM original.	
		Device should have 1 x 1 GE dedicated management interfaces, 1 x Console interface and 1 x USB interface	
		Appliance should have minimum 1.2 TB (SSD) Built in Storage from day 1.	
2	**Performance**	Appliance should support 35 Gbps or more Firewall throughput & 19 Gbps or more IPS throughput.	
		Appliance should support 18 Gbps or more Threat Protection throughput	
		Appliance should support 20 Gbps or more IPS Throughput	
		The device should have Concurrent Sessions: 7.5 Million or higher & New connection/Sec: 200,000 or higher	

		Firewall Should support at least 16 Gbps or more IPsec VPN throughput	
		Firewall shall support 4000 IPsec Site-to-Site VPN tunnels & 2000 IPsec VPN clients and support 10 SSL VPN clients for future scalability.	
		Firewall Should support at least 8 Gbps or more TLS/SSL inspection throughput	
		The Firewall shall support minimum of 745,000 SSL Inspection connections from day.	
		Firewall should support deep packet inspection and the appliance should have 5,900,000 Deep Packet Inspection connections from day one.	
3	**General Firewall Features**	Solution should provide unified threat policy like AV/AS, IPS, URL & Content filtering, Application control, Malware protection, Bandwidth management, policy & policy based routing on firewall rules to secure connectivity between Internet & internal network and security controls must be applied on inter zone .	
		Should support BGP,OSPF, RIP v1/v2 routing protocol and IPv4 & IPv6 functionality (Both phase 1 and Phase2).	
		Firewall should support manual NAT and Auto-NAT, Static NAT, Dynamic PAT, PAT etc.	
		Should have Layer 2 bridge or transparent mode, Wire mode, Sniffer mode /Tap mode.	
		Should support Zero-Touch registration & provisioning using mobile App or equivalent method.	
		solution should support policy based routing, Application based routing and also Multi Path routing.	
		The proposed system shall have the ability to detect, log and take action against network based on over 3500 application signatures .	

		Should have extensive protocol support to identify common protocols such as HTTP/S, FTP, SMTP, SMBv1/v2 and others, which do not send data in raw TCP, and decode payloads for malware inspection, even if they do not run on standard, well-known ports.	
		Firewall should support Link aggregation (static and dynamic) to provide additional level of redundancy.	
		Firewall should support static routing ,Dynamic Routing and WAN load balancing for redundant or backup Internet connections.	
		The appliance should be capable of scanning raw TCP streams on any port bi-directionally preventing attacks that they to sneak by outdated security systems that focus on securing a few well-known ports.	
		Should support deep packet SSL to decrypt HTTPS for scanning (IPS,Gateway Antivirus, Content Filtering, Application control) transparently and send to destination if no threat found.	
		The Firewall should Support for TLS 1.3 to improve overall security on the firewall. This should be implemented in Firewall Management, SSL VPN and DPI.	
		Firewall should support clientless SSL VPN technology or an easy to manage IPSec client for easy access to email, files, computers, intranet sites and applications from a variety of platforms.	
		Should support Redundant VPN gateway when primary and secondary VPN can be configured to allow seamless, automatic failover and failback of	
		Solution should have inbuilt support of DES, 3DES, AES 128/192/256 encryption MD5, SHA and Pre-shared keys & Digital certificate-based authentication connection tunnel.	

		Should support Route-based VPN that allow dynamic routing over VPN links to ensure continuous uptime in the event of a temporary VPN tunnel failure, by seamlessly re-routing between endpoints through alternate routes.	
		Solution should support Dead Peer Detection, DHCP Over VPN, IPsec NAT Traversal, Route-based VPN over OSPF, RIP, BGP.	
		Proposed solution must support application signature on following services or protocols DNS, FTP, H.323 ,SMTP,SQL, RTSP, SCCP, SMBv1/v2,SIP, NetBios, TFTP,SNMP etc.	
		Solution should support User identification and activity available through seamless AD/LDAP/Citrix/Terminal Services SSO integration combined with extensive information obtained through Deep Packet Inspection.	
		The proposed firewall should have the ZTNA capabilities and should support 10 nos of ZTNA license from day one .	
		Should have secure SD-WAN that enables organizations to build, operate and manage secure, high-performance networks across remote sites for sharing data, applications and services without adding any additional components or hardware. Vendors not having SD- WAN features integrated in their firewall should provide additional device to provide this feature support from day 1. Necessary licenses, if required, need to be provisioned from day 1.	
		Proposed solution must have Mac IP Spoof Prevention, Jumbo frames support & IP Helper for other than DHCP.	
		Firewall should have graphical view of a particular access rule, NAT and Routing rule which helps in finding realtime statistics. Displays the rules which are	

		actively used or not being used & enabled or disabled	
4	**Firewall Security Features**	Firewall should scan for threats in both inbound and outbound and intra-zone for malware in files of unlimited length and size across all ports and TCP streams by GAV & Cloud AV.	
		The proposed firewall should support Bi-directional raw TCP inspection that scans raw TCP streams on any port and bi-directionally to detect and prevent both inbound and outbound threats	
		Antivirus should provide real-time detection of viruses and malicious code at the gateway for SMTP, POP3, HTTP, FTP etc	
		Firewall must support Proxy-less and non-buffering inspection technology for DPI scanning without introducing file and stream size limitations, and can be applied on common protocols as well as raw TCP streams.	
		Solution should have single-pass Deep Packet Inspection architecture simultaneously scans for malware, intrusions and application identification and ensuring that all threat information is correlated in a single architecture .	
		Firewall must have integrated IPS shall be able to scan packet payloads for vulnerabilities and exploits, covering a broad spectrum of attacks and vulnerabilities. Should have at least 5000 IPS Signatures or 20K DPI signatures and 50 million Could AV signatures.	
		Should protect against DDoS/DoS attack using both Layer 3 SYN proxy and Layer 2 SYN blacklisting technologies. It protects against DOS/DDoS through UDP/ICMP flood protection and connection rate limiting.	

		Firewall Identifies and controls network going to or coming from specific countries to either protect against attacks from known or suspected origins of threat activity, or to investigate suspicious originating from the network. Ability to create custom country and Botnet lists to override an incorrect country or Botnet tag associated with an IP address.	
		Should have facility to block the URL's based on categories, granular control like Allow/Block, Bandwidth Management, Passphrase override, Notify. URL database should have at least 15-20 million sites and 70 + categories.	
		The Firewall solution should have detection and prevention capabilities for C&C communications and data exfiltration.	
		Shall be able to configure shaping on a per policy basis for specific application/ Specific networks and should be able to define guaranteed bandwidth and maximum bandwidth per policy.	
		Should have advanced QoS that guarantees critical communications with 802.1p, DSCP tagging, and remapping of VoIP on the network.	
		Deep packet SSL should be available on the same platform & License for DPI SSL should be along with appliance.	
		Should provide complete protection by performing full decryption and inspection of TLS/SSL and SSH encrypted connections regardless of port or protocol.	
		Firewall shall support AI-Driven Open XDR/SIEM to provide proactive threat analytics and automatic remediation for the proposed firewall.	

		OEM must have own SOC as a Service solution along with 24x7 threat monitoring, threat hunting and detection response. Customer may avail Network Detection Response solution for present Firewall as and when required in future as an addon service. Customer may purchase this solution along with required license in future.	
5	**Anti-APT / Malware Features**	Solution should support cloud based Malware analysis /APT solution for preventing zero-day threats. The APT solution should be proposed which should integrate with the proposed Firewalls from day one. Both the APT solution and Firewalls should be essentially from the same OEM.	
		The sanboxing should have memory based inspection, Multi-Stage Analysis with reputation check, static analysis and dynamic analysis.	
		The sandbox/Anti APT solution should have technology that detects and blocks malware that does not exhibit any malicious behavior and hides its weaponry via encryption.	
		Should detect and block zero-day threats and unknown malware. The solution should discover packed malware code that has been compressed to avoid detection, the technology should allow the malware to reveal itself by unpacking its compressed code in memory in a secure sandbox environment. It should see what code sequences are found within and compares it to what it has already seen. The Firewall should have the capability to block/prevent from Side Channel attacks.	
		The advanced threat protection displays a list of all the files that have been scanned and analyzed. User can filter results, search, search for specific strings to show	

		scans from the last month, last week, last 24 hours, and in the last hour.	
		The advanced threat protection functionality block file download until a verdict is returned, that ensures no packets get through until the file is completely analyzed. The file is held until the last packet is analyzed. If the file has malware, the last packet is dropped, and the file is blocked. The threat report provides information necessary to respond to a threat or infection	
		Should support both for analysis of a broad range of file types, either individually or as a group, including executable programs (PE), DLL, PDFs, MS Office documents, archives, JAR, and APK plus multiple operating systems including Windows, Android, Mac OS X and multi-browser environments etc.	
		Should have ability to prevent potentially malicious files from entering the network and those files sent to the appliance for analysis to be held at the gateway until a verdict is determined.	
		Administrator can view file-analysis status details including file submission time, source /destination IP, File size, File type, Suspicious Act etc.	
		Should support the capability of providing network-based detection of malware by checking the disposition of unknown files using SHA-256 file-hash or signature as they transit the network and capability to do dynamic analysis.	
6	**High-Availability Features**	The proposed NGFW shall have built-in high availability (HA) features without extra cost/license or hardware component.	
		The NGFW shall support stateful session synchronization in the event of a fail-over to a standby unit.	

		The NGFW must support Active-Active or Active-Passive stateful High Availability options.	
		The HA solutions should support silent firmware upgrade process that ensures minimum downtime.	
		The Firewall shall support failover in case of primary hardware failure without session loss and manual intervention to a standby unit.	
		The NGFW shall support interface link monitoring failover.	
7	**Management & Reporting Feature**	The firewall must be accessible via a web-based interface and ideally with no need for additional client software	
		Should provide centralized management and reporting solution with complete feature parity on firewall administration. The Central Management and Reporting Solution should be a dedicated OEM appliance (VM/Hardware) based.	
		Should provide provides a graphical representation of top applications , top address, top users and intrusion by sessions for granular insight into across the network.	
		The system should provide GUI panels and actionable dashboards with general information, system status, system usage, network interface status, security services information & High availability status	
		Solution should support granular network visibility of network topology along with host info.	
		Solution should have real-time visibility of infected hosts, critical attacks, encrypted information & observed threats	
		The management platform must be accessible via a web-based interface and without any additional client software	
		Firewall should support management via Cli, SSH ,GUI and support for SNMPv2/3.	

		The solution should support Centralize management & reporting platform which includes configuration, logging, monitoring, and reporting are performed by the Management Centre onprem .	
		The Centralize management & reporting platform should support multidevice firmware upgrade, certificate management, global policy template to push config across multiple firewall in single click.	
		The Centralize management & reporting platform should support account lockout security & account access control through whitelisted IPs.	
		The on prem Centralize management platform should support closed network deployment with High Availability & 2FA via mail/MS/Google authenticator.	
		The solution should store syslog in local storage or remote appliance. OEM can offer individual solution for logging and reporting based architecture to meet the requirements.	
		Reporting Solution must include predefined OnDemand, daily, weekly or monthly reports. Including at least Top events, Top sources, Top destinations, Top services etc.	
		Should have options to generate reports in terms of which are the frequent attacks as well as top sources and destination for attacks in different formats such as PDF/TEXT/ CSV/XML.	
		The solution should have configurable options to send the alert emails based on event type & reports as a mail to the designated email address	
		Reporting platform support Real-time risk monitoring and analysis of all network and user that passes through the firewall ecosystem.	

		The Firewall solution should support Cloud-based configuration backup	
		The solution should support IPFIX or NetFlow protocols for real-time and historical monitoring and reporting	
		The solution should support Application Visualization and Intelligence - should show historic and real-time reports of what applications are being used, and by which users. Reports should be completely customizable using intuitive filtering and drill-down capabilities.	
8	**Support Warranty and License Requirements**	All Required features of new firewall, management, reporting software should be done by single OEM.	
		The NGFW should be proposed with subscription licenses for IPS, Anti Virus, Anti Spyware, Anti Botnet , Zero day Protection, URL Filtering and Management with reporting.	
		License for Management, Reporting, any other license required to meet the above features should be provided from day one for min. period 5 (five) years.	
		5 years comprehensive warranty and support for hardware, software updates and patches shall be offered directly from the OEM	
		OEM should have TAC and R&D center in INDIA. Proposed solution should support 24x7 remote technical support by OEM through chat/email / remote access.	
		The NGFW firewall should include cyber warranty that offers limited compensation for covered losses that lead to business interruption from Non-volumetric DDOS attack and Unauthorized remote access types of events. OEM must offer the cyber warranty alongwith firewall from day one.	
9	**3rd Party Test Certification**	Proposed Firewall manufacturer should be placed in Gartner Magic Quadrant of Enterprise/Network firewall for last three years.	

		The Firewall, Antivirus & Advanced Threat Defense module should have ICSA or other equivalent Certification.	
		Offered product should more than 97% of block rate in 2019 SVM NGFW report of NSS and above 93% security effectiveness. Also, should feature in the top quadrant of the Security Value Map (SVM) of NSS Labs report 2019 for Next Generation Firewall (NGFW). Report to be submitted by the bidder.	
		Firewall solution should be certified under Common Criteria program (global or the Indian Common Criteria Certification Scheme (IC3S) has been set up by the Ministry of Electronics and Information Technology (MeitY)) program for Protection Profile).	
		Offered model should have also FCC, CE, VCCI certifications.	
		Manufacturer's warranty should be mentioned minimum 05 (five) years warranty including all services like GAV, IPS, Antispyware or antimalware, CFS, Application control, BoT protection , ATP, Patch & Firmware upgrade and management and reporting.	
10	**OEM Authorization**	Original Manufacturer Authorization Certificate to be submitted along with the bid	

15.7 Web Access Firewall

Sl. No.	Specifications
1	The solution should have a purpose built standalone dedicated appliance-based solution (not white labelled). It should NOT be part of Router, ADC, Firewall / UTM Device. The OEM should be different from proposed Firewall solution.

2	The solution should have a dedicated out-of-band management interface for management of the appliance. Management interface(s) shall be separate from traffic interfaces and must not switch traffic.
3	The solution should have Rack Mountable
4	The solution should have enough CPU capacity and Memory so as to efficiently meet all the capability parameters as well as functionalities laid down in the technical specifications.
5	The solution should have Redundant Power Supply. The primary as well as redundant power supply shall be hot swappable and no downtime / reboot shall be required for addition / removal of power supply module.
6	The solution should have designed to run both IPv4 & IPv6 simultaneously (Dual Stack) from day one.
7	The solution should provide automatic threat updates to the signature database, geo IP feed, tor nodes, malicious IP feeds, etc. to ensure complete protection against the latest application threats.
8	The solution should provide notifications through Email, Syslog, SNMP Trap, Notification via HTTP(S) push etc.
9	The solution should support clustered deployment of multiple mitigation appliances sharing the same policy. The solution should support High Availability with VRRP (or equivalent) with Active-Active or Active-Passive deployment options
10	The solution should support offline or inline reverse proxy (one-arm or n-arm), IP transparency, Direct Server Return deployment options

11	The solution should have 80% content Make-in-India and should be tested by Govt. of India agencies like STQC or CERT-In empaneled agency. The OEM of The solution should be ISO-9001, ISO-27001 certified and should have a R&D and Development Centre in India
12	The solution shall conform to UL 60950 or IEC 60950 or CSA 60950 or EN 60950 or equivalent Indian Standards like IS-13252 (Part 1):2010 for Safety requirements of Information Technology Equipment.
13	The solution shall conform to EN 55022 Class A/B or CISPR22 Class A/B or CE Class A/B or FCC Class A/B or equivalent Indian Standards like IS 6873 (Part 7):2012 for EMC (Electro Magnetic Compatibility) requirements.
14	The OEM of the solution should own 100% IPR on the technology along with copyright. The solution should not be white labelled.
Requirement Sizing Specs	
1	The solution should have dedicated at least 01 management port and 01 port for high availability
2	The solution should have 8 x 1G ports.
3	The solution should have minimum 20 Million concurrent L4 TCP connections.
4	The solution should have minimum 4 Gbps Layer-7 throughput
5	The solution should have minimum 450K L4 TCP connections / second and 750K HTTP requests / second
6	The solution should have hardware based SSL acceleration with minimum 20K RSA 2K and 15K ECC transactions per second with bulk encryption / decryption of 4 Gbps. The solution should support SSLv2, SSLv3, TLSv1.0, TLSv1.1, TLSv1.2 & TLSv1.3
Management & Reporting Specs	

1	The solution should have manageable (both GUI and CLI) using console port, SSH and Web based management i.e. HTTPS etc for configuration and management purpose.
2	The solution shall provide real-time and historical statistics on dropped and passed traffic in packets and bytes, top URL, methods, country, etc.
3	The solution should have the ability to take manual or scheduled backup of solution configuration and policies.
4	The solution should be able to provide overall status of the solution health (CPU, Memory etc), network traffic and ongoing attacks
5	The solution should generate periodic reports and should be able to send it via email or downloadable from web based management
6	The solution should be able to integrate with
	- AAA/TACACS server for user authentication
	- NTP/SNTP server
	- SIEM via API or syslog (in CEF format)
	- NMS solutions via SNMP
	- 3rd Party solution via API (REST or XML)
7	The solution should provide role based access to users / group of users with different permissions and capabilities
Feature Specs	
1	The solution shall support IPv4 to IPv6 address translation and vice-versa.
2	The solution should support line speed throughput and sub-millisecond latency so as not to impact Web application performance.
3	The solution should prevent the following attacks (but not limited to) in network, HTTP request / response and Web sockets for Web Applications and Web Services (JSON, XML, etc.) :
	- OWASP Top 10 Web Application Attacks
	- OWASP Top 10 API attacks

	- SQL Injection
	- Cross Site Scripting (XSS)
	- Broken Authentication
	- Session Management
	- Brute force
	- Access to predictable resource locations
	- Unauthorized navigation
	- Web server reconnaissance
	- HTTP request format and limitation violations (size, unknown method, etc.)
	- HTTP protocol validation
	- Web service layer correlated attack validation
	- HTTP protocol attack signatures
	- Web service layer customized protection
	- Cookie signing validation
	- Anti site scrapping
	- Bot protection and mitigation
	- Web profile protection
	- Web worm protection
	- Web application attack signatures
	- Web application layer customized protection
	- OCSP protocol validation
	- Account Takeover Detection
	- MITB and MIM attack protection
	- L7 Behavioural DoS Protection"
4	The solution should have DLP features to identify and block sensitive information such as credit card numbers, Aadhar Numbers, etc.
5	The solution should support positive and negative security model with built-in database of signatures of known attacks and application platforms.
6	The solution should be able to execute the following actions upon detecting an attack or any other unauthorized activity:
	- Ability to drop requests and responses
	- Block the TCP session
	- Block the application user

	- Block the IP address.
	- Temporarily blacklist IP address
	- Send custom response with custom error code
	- Send empty response
	- Send Captcha
7	The solution should support different policies for different applications based on host name or per application path or source country / IP list. Each policy should be customizable to run in one of bypass (no logging), record (log incident but don't act) and mitigate (log and act) modes
12	The solution should provide auto profiling of web application to automatically learn the Web application structure and elements and periodic changes to protected applications
13	The solution should have 0-day protection. It should use behavioral learning to detect and mitigate traffic / payload anomalies.
14	The solution should have anti-automation protection which can block the automated / bot attacks that use hacking tools, scripts, frame work etc.
15	The solution must support integration with third party DAST tool to perform virtual patching for its protected web applications. The solution must support all the common web application vulnerability assessment tolls (Web application scanners) including Acunetix, Qualys, Rapid 7, IBM AppScan etc. to virtually patch web application vulnerabilities. In addition, the solution should provide built-in DAST tool from same OEM for faster application structure profiling and security. The built-in DAST should support active as well as passive scanning with support for login and token authentication. The built-in DAST tool should also support scheduled scanning, pausing existing scan and pre-mature scan termination

16	The solution should have ability to create custom logging rules to allow / mask sensitive information from being logged by the Web Application Firewall
17	The solution should offer header, cookie, content and hidden form fields (Static/Dynamic) obfuscation or encryption to protection against manipulation
19	The solution should have Layer 7 DDoS protection
20	The solution should support both URL rewriting and content rewriting for http header and body.
21	The solution must support user tracking using various authentication via form based, certificate-based, Basic Auth, JWT, Key Auth, etc. authentication schemes
22	The solution should support anti-bot SDK for mobile application for protecting mobile apps and Web APIs. The anti-bot mobile SDK should be available for Android and iOS and should be from same OEM as WAF
23	The solution should have built-in AV scanner and sandboxing capability. In additional it should also support integration with 3rd party sandboxing solution via API or ICAP
24	The solution shall support scripting language for events based rule creation to make traffic management and security decisions using scripting language
25	The solution should have deception capability to implant decoys (fake links and forms) in any application without any changes to application or client.
26	The solution should provide SSL certificate management with support for uploading custom certificates or generating certificates with Lets Encrypt

27	Thr proposed solution should user defined scripts to define custom logic to block HTTP request that break business logic
28	The proposed solution should have the ability of caching, compression of web content and SSL acceleration.
29	The proposed solution should provide load balancing and origin server monitoring. It should support various load balancing algorithms (round robin, least connection, least bandwidth, hashing, SNMP metrics) and advanced content based routing for application delivery (for e.g., requested contents such as URL, HTTP Headers and Parameters)
30	The proposed solution should integrate with managed Bot Protection Service for advanced BOT detection and mitigation. The Bot Protection Service should be from same the OEM as WAF and should provide marking requests as "good", "suspicious" or "bot" based on Bot Protection Service analysis
31	The proposed solution should support API discovery, auto-documentation generation and import / export in Swagger (Open API) format.
32	The proposed solution should support Proof-of-Work and Proof-of-Space challenge when sending CAPTCHA challenge to make them unbeatable by advanced bots.
33	The proposed solution should have built-in Bot detection logic without having to rely upon any cloud based 3rd party APIs.

15.8 L2 switch

Sr. No.	Minimum Specifications
1	Switch should have 24 x 10/100/1000 Base-T ports with additional 4 x 1/10G SFP+ ports
2	Should have 4GB RAM and 16GB Flash and 8 MB Packet buffer

3	Minimum 128 Gbps switching capacity
4	The switch should have dedicated Console Port
5	Should have minimum 8000 MAC address entries and minimum 500 active VLANs.
6	IPv6 ready from day 1 and support REST API
7	Should support UDLD or equivalent.
8	Should support Uni-directional Link Detection (UDLD) to monitor link connectivity and shut down ports at both ends if unidirectional traffic is detected, preventing loops in STP-based networks
9	Should support EEE 802.3ad LACP supports up to 8 LAGs, each with up to 8 links per LAG
10	The switch should have minimum 512 Ipv4 Unicast Routes and 512 Ipv6 Unicast Routes ,512 Igmp Groups
11	Switch should support Static routing
12	Switch should support RA guard, DHCPv6 protection, dynamic IPv6 lockdown, and ND snooping
13	IPv6 ACL/QoS supports ACL and QoS for IPv6 network traffic
14	The switch should support Strict priority (SP) queuing,Traffic prioritization (IEEE 802.1p) ,Class of Service (CoS) ,IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and DiffServ
15	The Switch should support Network Time Protocol (NTP)/SNTP synchronizes timekeeping among distributed time servers and clients.
16	The Switch should support IEEE 802.1AB Link Layer Discovery Protocol (LLDP) advertises and receives management information from adjacent devices on a network to facilitate easy mapping by network management applications
17	The Switch should support ACLs filtering based on the IP field, source/ destination IP address/subnet, and source/ destination TCP/UDP port number on a per-VLAN or per-port basis
18	The Switch should support multiple user authentication methods. Uses an IEEE 802.1X supplicant on the client in conjunction with a RADIUS server to authenticate in accordance with industry standards
19	The Switch should support Web-based authentication provides a browser-based environment, similar to IEEE 802.1X, to authenticate clients that do not support IEEE 802.1X
20	The Switch should support MAC-based client authentication
21	The Switch should support Identity-driven ACL to enable implementation of a highly granular and flexible access security policy and VLAN assignment specific to each authenticated network user
22	The Switch should support STP BPDU port protection to block Bridge Protocol Data Units (BPDUs) on ports that do not require BPDUs and prevent forged BPDU attacks
23	The Switch should support STP root guard to protects the root bridge from malicious attacks or configuration mistakes
24	The Switch should support Port security to allow access only to specified MAC addresses, which can be learned or specified by the administrator

25	The Switch should support Source-port filtering to allow only specified ports to communicate with each other
26	The Switch should support Concurrent IEEE 802.1X, Web, and MAC authentication schemes per switch port accepts up to 32 sessions of IEEE 802.1X, Web, and MAC authentications
27	The Switch should support Auto VLAN configuration for voice RADIUS VLAN uses a standard RADIUS attribute and LLDP-MED to automatically configure a VLAN for IP phones
28	The Switch should support Management Interface Wizard to help secure management interfaces such as SNMP, SSH,SSL, Web.
29	EN 60950-1/IEC 60950-1 EN 60825/equivalent or higher CAN/CSA C22.2 No. 60950, 2nd Edition UL 60950-1, 2nd Edition
30	The switch shall be offered with minimum five years hardware warranty with 24x7 Technical support from OEM directly

15.9 L3 Switch

Sr. No.	Minimum Specifications
1	**Physical Characteristics and Port Requirements**
1.1	The switch should be 1U 19" Rack Mountable
1.2	The switch should have dual, redundant, field-replaceable, hot-swappable power supplies and field-replaceable, hot-swappable fans with front-to-back airflow
1.3	The switch should have 24 ports of 1/10GbE/25GbE (SFP+/SFP28) and 4 ports of 10G SFP+. Cables/Transceivers shall be populated as per the design
1.4	The switch should have 4 ports of 40GbE/100GbE (QSFP+/QSFP28). Cables/Transceivers shall be populated as per the design
1.5	The switch should have RJ-45 serial or USB-C console port, RJ-45 Ethernet Management port and USB Interface
1.6	The switch should be based on programmable ASICs purpose-built to allow for a tighter integration of switch hardware and software to optimize performance and capacity
1.7	Switch should have integrated trusted platform module (TPM) or equivalent for platform integrity to ensure the boot process is from trusted source
2	**Performance Requirements**
2.1	The switch should have multi-core CPU/processor
2.2	The proposed switch should have minimum 16GB DRAM, 32GB Flash Memory and 32MB Packet buffer memory
2.3	The proposed switch should have minimum 2 Tbps switching capacity
2.4	The proposed switch should support virtualization/distributed and redundant architecture by deploying two switches with each switch maintaining independent control and synchronized during upgrades or failover and also supports Multi-Chassis Link aggregation (MC-LAG) for uplink/downlink connectivity. Should also supports upgrades during live operation.
2.5	The switch ports should support Jumbo frames with maximum frame size of 9K bytes

2.6	The switch should have minimum 200K MAC Address Table size
2.7	The switch should support minimum 200K IPv4 routes,200K IPv6 Routes and 6K IPv4/IPv6 Multicast Routes
2.8	The switch should support minimum 32K IPv4 ACLs and 16K IPv6 ACLs
3	**Operating System Capabilities**
3.1	The switch should have modular operating system with micro-services or equivalent architecture providing superior fault tolerance and high availability
3.2	The switch operating system should be database-driven where software processes communicate with the database rather than each other, ensuring near real-time state and resiliency
3.3	The switch operating system should provide easy access to all network configuration state information
3.4	The switch OS should support programmability through REST APIs, Python scripting or equivalent
4	**Layer-2, QoS and Security Features**
4.1	The switch should support Spanning Tree Protocol (STP/RSTP/MSTP) and Ethernet Ring Protection Switching (ERPS) for rapid protection and recovery
4.2	The switch should support Link Aggregation Control Protocol (LACP)
4.3	The switch should support IEEE 802.1Q VLANs (4000 VLANs)
4.4	The switch should support Private VLAN for traffic isolation for users on the same VLAN
4.5	The switch should provide storm protection to limit unknown broadcast, multicast, or unicast storms with user-defined thresholds
4.6	The switch should support Datacenter Bridging (DCB) capability supporting Priority Flow Control (PFC), Enhanced Transmission Service (ETS) and DCB Exchange Protocol (DCBX)
4.7	The switch should support Strict priority (SP) queuing, Explicit Congestion Notification (ECN) or equivalent for congestion avoidance and Access control lists (ACLs) for both IPv4 and IPv6 traffic
4.8	The switch should support Internet Group Management Protocol (IGMPv1, v2, and v3) and Multicast Listener Discovery (MLDv1 and v2)
4.9	The switch should support Secure port access like 802.1x, Mac-auth, Port-Access Policy, Static Port Filtering
5	**Layer-3 Routing and Services Features**
5.1	The switch should support IPv4 and IPv6 Static Routing, RIPng
5.2	The switch should support Open shortest path first (OSPF) for IPv4 and IPv6
5.3	The switch should support Border Gateway Protocol 4 (BGP) for IPv4 and IPv6
5.4	The switch should support Policy Based Routing (PBR)
5.5	The switch should support Multicast Routing using PIM-SM,SSM and Multicast Service Delivery Protocol (MSDP)
5.6	The switch should support dynamic VXLAN with BGP-EVPN
5.7	The switch should support DHCP Server providing DHCP services (for IPv4 and IPv6)

5.8	The switch should support Equal-Cost Multipath (32 way), Generic Routing Encapsulation (GRE),MPLS
6	**Management Features**
6.1	The switch should support SNMP and Remote monitoring (RMON)
6.2	The switch should support sFlow or equivalent for traffic analysis
6.3	The switch should provide advanced telemetry and automation features for monitoring, troubleshooting and improving network operations
6.4	The switch should support RADIUS and TACACS+ for securing administrative access
6.5	The switch should have Command Line Interface (CLI) with a hierarchical structure and SSH, Secure FTP/TFTP support
6.6	The switch should support Precision Time Protocol (PTP)
6.7	The switch should support Port mirroring
7	**Certifications and Industry Recognition**
7.1	The Switch series/Switch OS should be Common Criteria Certified (EAL or NDPP)
7.2	The switch should have RoHS compliance
7.3	The switch should have safety/emissions certifications including UL/CUL 62368, EN 55024/55032, VCCI Class A, IEC 62368-1.
8	**Support and Warranty**
8.1	The switch shall be offered with minimum five years hardware warranty with 24x7 Technical support from OEM directly
8.2	All the features mentioned in the specifications shall be enabled/activated. Any licenses required shall be included from Day 1

15.10 SAN Switch

Sr. No.	Minimum Specifications
1	Proposed SAN switch shall be configured with 48 x 32G FC Ports. Minimum 5-mtrs OM4 Duplex LC-LC OFC patch cords need to be quoted for all active ports.
2	Required scalability shall not be achieved by cascading the number of switches and shall be offered within the common chassis only.
3	Proposed switch Should deliver 32 Gbit/Sec Non-blocking architecture with 1:1 performance for up to 48 ports in an energy-efficient fashion.
4	Proposed switch Should protect existing device investments with autosensing 8, 16, and 32 Gbit/sec capabilities.
5	The proposed switch should be rack mountable. Rack-mount kit to be included.

6	The proposed switch shall provide an aggregate bandwidth of 1.5Tbps end to end.
7	The proposed switch should have support for web-based management and should also support CLI.
8	Proposed switches shall provide enterprise-class availability features such as redundant and hot pluggable components like power supply and FAN.
9	OEM should be ranked within top 3 as per IDC report for any one of the previous four quarter in India on Storage OR OEM should be from the leader's quadrant as per last published Gartner's primary storage MQ report.
10	Five years on-site comprehensive OEM Warranty Support with 24X7 coverage and access to OEM TAC/support. OEM shall have their own support portal to log the case online and historical data about cases must be available in the same portal.

15.11 LPU

Sl. No.	Technical Specifications		
1	System	Processor	Intel® 9th Generation Core™ i7-9700 with Min 8 Cores/8 Threads or Higher as per the ITMS OEM Requirements.
		Graphics	Intel® HD Graphics (OpenGL up to 5.0, DirectX 11, Open CL 2.1)
		Memory	Should Support Up to 64GB DDR4
			LPU to be Populated with Min. 16 GB RAM from Day 1.
2	I/O Interface	Ethernet	4x Gigabit Ethernet ports by Intel
		USB	4x USB 3.1 Gen1 ports
			2x USB2.0 ports
		Video Port	1x VGA connector
			1x HDMI/DP connector (Auto Detection)
		Serial Port	4 x RS-232/422/485 (DB-9)
			2x RS-232 ports
		DIO	8 Bit DIO (DB-9)
3	Storage	SATA SSD	2 x 2.5" SATA 3.0 Drive Bay RAID Support
			LPU to be Populated with Min. 1 TB SSD from Day 1.

		m.2 Slot	1 x M.2 2280 M key (SATA)
5	Audio		1 x Line-out
			1 x Mic-in
6	Power	Type	Wide Range 9~36VDc
		Connector	3-pole terminal nlock
			3-pin power extension switch connector
7	Environmental	Operating Temperature	10°C to 60°C fanless operation
		Construction	Metal + Aluminium
		Humidity	5%~90% , non-condensing
		Vibration	IEC68-2-64
		Shock	Half sine wave 3G, 11ms, 3 shock per axis
		Certificate	CE, FCC Class A, RoHS, UKCA, BIS

15.11 Public Address System

OEM Criteria:

· The OEM of PA should be ISO 27001 Certified

· The OEM of PA system should have supplied to minimum 5 Smart/Safe cities/ITMS projects in India

· MAC address of the equipment shall be on the name of proposed OEM. Requisite documents should be submitted along with the bid. OEM should also be able to produce all supporting documents to the purchaser and can also display the same online

Sl. No.	Parameter	Compliance (Yes/No)
1	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 50 Watts RMS, Class D.	
3	Native IP connectivity, no convertors to be used	
4	0 to 55 C operating temperature rating for Amplifier	
5	Protocols: IPv6, IPv4, TCP, UDP, HTTP (RFC 2617, RFC 3310),	
	RTP (RFC 3550), RTCP, DHCP, SDP (RFC 2327),	
	SIP (RFC 3261), SNMPv2, STUN, TFTP, URI (RFC 2396),	
	DTMF Decoding (RFC 2876, RFC 2833),	

	SIP User Agent (UDP RFC 3261),	
	SIP Refer Method (RFC 3515)	
6	ONVIF Profile S for unidirectional audio	
7	2Inputs and 1 Output relay contacts inbuilt Amplifier	
8	Short-circuit and over-range protection	
9	Power supply: 20 –26 VDC 2) (max. 2.6 A at 4 Ω/50 W or max. 1.3 A at 8 Ω/25 W, max. 3 A at the 70 V/100 V loudspeaker output) or PoE	
10	Speaker: Minimum 2 Speakers 20 W capacity	
11	Frequency Response of Speaker 350 -10,000Hz	
12	Central Software based server application capable of working on virtual environment/cloud with redundancy	
13	Software based on Linux (Debian 9, 64 bit) for virtualised IT platforms	
14	Integration with VMS and Command and control centre or any other component if required	
15	PA Master Controller to have facility for multiple mic inputs, direct dialling buttons, LCD screen	
16	Software Client for making Calls to PA and ECB	
17	Automatic Volume Control, Call recording	
18	Transmission bandwidth16000 KHz for master control desk	
19	Operating temperature for control desk 0 to +60C	
20	Web hook commands via HTTP/HTTPS	
21	ISO 27001:2013 Information security management system certified OEM	
22	Certification: UL Certification for IP Amplifier	
23	MAC id of the products should be in the name of the Quoted OEM	

15.8 Fire Protection and Safety Measures for ICCC and Data Center (DC)

A robust fire protection strategy is essential for safeguarding critical assets in both Control Rooms and Data Centers. This document outlines a structured approach that combines advanced fire detection, suppression, infrastructure resilience, and emergency preparedness, while incorporating additional measures such as rodent repellent systems and enhanced power backup.

Sl.	Parameters	Specifications	

No.			Compliance (Yes/No)
1	Fire Alarm and Detection Systems		
	Control Room: Conventional Fire Alarm System	Control Room: Conventional Fire Alarm System	
		System Configuration: A conventional fire alarm system segmented into multiple zones with detectors and call points.	
	Alert Mechanisms:	Intelligent hooter cum strobe units that deliver both auditory and visual alerts.	
		An in-built Auto Dialer with GSM connectivity to ensure immediate notification of fire incidents, even if primary communication channels fail.	
1.1	Data Center: Ultra-Early Detection System		
	VESDA (Very Early Smoke Detection Apparatus):	Designed for ultra-early fire detection by continuously sampling air for microscopic smoke particles.	
		The system must be rated to meet the rigorous standards expected of industry-leading manufacturers, ensuring reliable performance and early warning without directly naming specific brands.	
2	Fire Suppression Systems		
2.1	Control Room: Portable Fire Extinguishers	Recommended Types and Rationale: CO_2 Extinguishers (2kg & 4.5kg): Ideal for electrical fires, leaving no residue.	
		ABC Dry Powder Extinguishers (4kg & 6kg): Provide broad coverage for Class A (solid combustibles), Class B (flammable liquids), and Class C (electrical) fires.	
		Foam-Based Extinguishers (9L): Effective against Class A and B fires, especially where flammable liquids are present.	
	Maintenance Methodology:	Conduct monthly inspections to verify pressure levels, seals, and overall condition.	
		Ensure annual servicing by certified technicians, including refilling and pressure testing.	
2.2	Data Center: Gas-Based Fire Suppression System		

	System Specifications:	Employ FM200 or Novec as the clean agent to suppress fire effectively without harming sensitive IT equipment.	
		The suppression system should be rated to the standards synonymous with top industry manufacturers, ensuring robust performance and reliability.	
	Operation:	These agents work by displacing oxygen or interrupting the combustion process, providing rapid fire suppression with no residue or need for extensive post-fire clean-up.	
3	Infrastructure & Safety Enhancements		
3.1	Fire-Resistant Infrastructure and Electrical Safety	Structural Integrity: Construct fire-rated walls, ceilings, and doors (minimum 2-hour rating) to contain fire spread.	
		Utilize fire-retardant cable trays and conduits to minimize the risk of fire propagation via electrical wiring.	
	Electrical Protection:	Install surge protection devices and automatic circuit breakers to safeguard against electrical overload.	
		Implement regular thermographic scanning to detect overheating components.	
	Power Backup:	Ensure that the DG (Diesel Generator) set is equipped with an AMF (Automatic Mains Failure) or similar panel for seamless switching during power outages.	
	Rodent Protection:	Incorporate a rodent repellent system to protect critical cabling and electrical installations from damage and potential fire risks caused by rodent activity.	
4	Emergency Signage and Lighting		
	Visibility Enhancements:	Install backlit passive signage to clearly mark the locations of fire extinguishers and emergency exits, ensuring they are visible under all conditions.	
		Provide lighting with battery backup to maintain clear pathways and operational exit signs during power failures.	

		ACTIVE LED Stretch Displays installed for aesthetic reasons on both side walls of main control room to act as Emergency Signage in case of emergencies.	
5	Environmental & Facility Management for Data Centres		
5.1	Precision Air Conditioning with Redundancy		
	Cooling Requirements:	Mandate precision air conditioning with an N+1 redundancy configuration to maintain optimal temperature and humidity control, thereby protecting IT equipment from overheating.	
	Leak Detection:	Equip the facility with water leak detection sensors near precision AC units to prevent water damage and reduce the risk of short circuits.	
	Flooring and Cable Management:	Use sealed raised flooring with fire-resistant properties to house critical cabling, with cable entry points properly sealed to restrict fire and smoke spread.	
6	Emergency Preparedness and Maintenance		
6.1	Training and Drills	Conduct quarterly fire drills to ensure that all personnel are familiar with evacuation routes and emergency procedures.	
		Provide regular training on the proper use of fire extinguishers and emergency response protocols.	
6.2	Periodic Testing and Compliance Audits	Perform monthly inspections of fire extinguishers and suppression systems.	
		Schedule annual servicing and pressure testing for all fire suppression and detection equipment.	
		Arrange for annual third-party fire safety audits to verify compliance with national and local fire codes.	
7	Security Integration and Access Control		
	Access Management:	Implement biometric access control systems to restrict entry and reduce potential risks from unauthorized personnel.	

15.9 Dual mode Drone (Tethered and Untethered)			
Sl. No.	**Parameters**	**Specifications**	**Compliance (Yes/ No)**

1.	UAV Operating Mechanism	Tethered & Untethered Mode	
2.	Weight (All up Weight)	<= 8 Kg (Tethered mode, excluding Tether cable) <= 6 Kg (in Untethered Mode)	
3.	Endurance	· 6 hours minimum with payload on Tethered Mode · 60 Mins of Endurance in Untethered Mode (Separate Standard Battery) upto 1000m Above mean sea level (AMSL) & 500m Above Ground level (AGL)	
4.	Tethering Range (Control, Operating and Video Transmission)	· 100m variable as per Tethered Cable length · Auto-winching / Auto-sensing · Video transmission tether cable or wireless	
5.	Operating Altitude	100m (Tethered Cable Length) AGL	
6.	Launch Altitude	Upto 4000 m AMSL or more	
7.	Operational Temperature Range	,-10ºC to 50º)	
8.	IP Rating	IP54	
9.	Wind Resistance	36 Km/h or more in both head wind and cross wind conditions	
10.	Take off Mode and Landing Mode	Vertical Takeoff and Vertical Landing (VTOL)	
11	Flight Modes	(a) Fully Autonomous mode & stabilized (b) Remotely Piloted mode (c) Semi – autonomous mode (d) Should be controllable in real time from the GCS upto recovery	
12	Failsafe Features (Automatic Return to home capability)	(a) Automatic return to home on communication failure. (b) Auto land on Tethered power interruption / low battery without pilot intervention. (c) Return to home on tether cable breakage	
13	Navigation	GPS/ IRNSS/ GLONASS. Minimum two On-board GPS/ Navigation System	
14	Battery Charger	Suitable battery chargers to charge Aerial System battery from 220V AC mains and from 12V / 24V DC Source with two spare batteries for each unit	
15	Day Camera	Optical Zoom - Minimum 20X Digital Zoom - Minimum 4X Resolution - Minimum 1920 x 1080 pixels	

		Control & Ranges; · 360° Pan and 90° tilt control (in-flight) with scan range of 2 to 3 km from VTOL · Human Detection upto 1 km · Vehicle Detection upto 3 Km	
16	Night Thermal Camera	Digital Zoom -Minimum 4X Resolution -Minimum 640 x 480 pixels	
		Control & Ranges; · 360° Pan and 90° tilt control with scan range of 1 to 1.5 km from VTOL · Human Detection upto 0.7 kms · Vehicle Detection upto 1.2 Kms	
17	Data Transmission	To provide data link either via tether cable or wireless	
18	Minimum Transmitted Video Resolution at 100m altitude	· Transmit minimum 1920 x 1080 pixels resolution for day camera, minimum 640 x 480 pixels resolution for night camera, stabilized, clear and continuous video from 100m altitude to GCS. · Transmit Control Commands from GCS to Tethered Drone · Transmit telemetry data from Tethered Drone to GCS. · Transmit high resolution, stabilized, clear and continuous video from Tethered Drone to GCS. · Configurable RF link	
19	Communication Failure	Return to home failsafe feature on Communication Failure	
20	Encryption	Minimum 128 Bit AES encryption.	
21	Computer Hardware & Software	· Minimum 10'' ruggedized (MIL-STD-810G and IP55 or better) Laptop with minimum 1TB internal storage and processor speed of minimum 3.2 GHz (Certification from OEM of computer hardware for MIL-STD-810G & IP-55 or better) · Compatible Software Solutions working on Standard Operating System.	
22	Command Link	Configurable RF link with secured 128 Bit encryption.	
23	220V AC mains and from 12V/ 24V DC Source	Generator for 220V AC supply. GCS should be capable of running on 220V AC mains and from 12V/ 24V DC Source.	
24	Maps	· Map along with Aerial System location, camera view, waypoints indicated on Military Map.	

		· Capability to work with Google maps also and /or other available open-source maps.	
		· Capability to upload grid reference in at least one of the commonly used digital map formats (TIFF/ DTED2/ SHP/DEM).	
		· Capability to show aerial system and delivery location in both Indian Grid Reference System and coordinates.	
		· Capability to show and give coordinates of cursor on map, GIS and image/ video output	
		· Open Software Architecture with capability to upload Maps in any Format.	
25	Video	· Real time HD video from payload along with essential coordinates should be displayed.	
		· Video should be recorded at GCS.	
		· Real Time video from the Tethered Drone with on-screen display of following parameters: - - Aerial System co-ordinates, Altitude, Camera Tilt and Pan Angle, - Bearing, Capability to take photographs with on-screen display parameters at any time during flight, Display grid reference and coordinates of cursor on map and video/ image	
26	User Interface	Easy to control the flight and altitude with marking of the important locations.	
27	Pre-Flight Checks	Capability to automatically perform pre-flight check of the complete system before every flight for confirming the suitability of flight worthiness	
28	User Control	· One-Click Take-off/Land.	
		· Set altitude of the Tethered Drone.	
		· RPV Mode which allows Tethered Drone to be flown in semi-autonomous mode.	
		· Fully autonomous mode for flying without RPV mode with manual override capability.	
29	Joystick Controls	· Full Camera Controls: -	
		- Pan- 360^{o}	
		- Tilt- 90^{o}	
		- Zoom In/Out	
		· RPV mode & Altitude Control.	
		· Switch button to toggle between Video recording and photography.	

30	GUI Display Parameters	· Geographic Map along with location of the Tethered Drone.	
		· Real Time video from the Tethered Drone with on-screen display of important parameters like co-ordinates and altitude.	
		· HD Live streaming of video should always be displayed during the flight.	
		· Artificial Horizon indicating.	
		· Cross wind speed.	
		· No on-board recording of any event.	
		· Indication of GCI antenna bearing with reference to Home position.	
		· Interfacing of digital / Scanned maps on GCS.	
31	Moving Target Indicator	Ability to auto detect and highlight multiple movements (vehicles, human movement, large animal movement) in live video display to decrease operator fatigue	
32	GCS Antenna	GCS Antenna should be capable of automatically tracking the Tethered Drone during flight to maintain optimum communication link	
33	Other	USB 3.0 /HDMI 2.1 Port for data and video transfer	
34	Life of equipment	Minimum Reliable Flying time of 1000 hours	
35	ISO/ ISI Certification	Required for Tethered Drone and Ground Control Station.	

15.10 Social Media Monitoring System			
Sl. No.	Parameter	Description	Compliance (Yes/No)
1	Perception Management	The agency shall help authority to develop methods for perception management on social media platforms to bolster the positive image and strategic goals of the authority. The agency should implement SOPs for perception management for building trust, transparency, engagement and responsiveness. This includes analysis to gauge public sentiment, address grievances, counter misinformation, showcase achievements, engage communities, and shape a positive citizen-focused city narrative.	

2	Responsive Handling of Citizen Concerns through Social Media Monitoring:	Addressing inquiries and issues raised by citizens through diligent monitoring of social media channels.	
3	Sentiment Analysis	The agency shall conduct in-depth sentiment analysis to gauge the prevailing sentiments and opinions expressed in discussions related to the authority in the region/state across various social media platforms available in India.	
4	Fake News Mitigation	The agency shall actively counter the propagation of misinformation and fake news on social media platforms to safeguard the authority's reputation. The agency is to take proactive measures to detect and counteract the spread of false information pertaining to the event through continuous monitoring of social media content.	
5	Crisis Handling	The agency shall prepare and execute crisis communication strategies on social media, managing potential PR crisis effectively and safeguarding the department's reputation.	
6	Trend Recognition	By monitoring social media trends, the agency shall identify emerging topics within the Department's digital discourse, enabling proactive engagement and response.	
7	Local Event Promotion	Leveraging social media, the agency shall promote local events, campaigns, and initiatives to boost citizen engagement and participation. (Cost of advertisements/ campaigns charged by social media platforms if applicable is outside the scope.)	
8	Performance Analytics	Regular reports furnished by the agency shall feature comprehensive social media analytics, insights, and actionable suggestions, evaluating the impact of their efforts.	
9	Multilingual Proficiency	Operating across social media, the agency shall manage content in diverse languages (English and Hindi) spoken, ensuring inclusive engagement. Proper understanding of local languages and should overcome the limitations of NLP.	

10	Emergency Alerts and Updates	Collaborating with relevant authorities, the agency shall use social media platforms to swiftly disseminate emergency alerts, updates, and safety information.	
11	Minimum Qualification of Agency	A qualified market research agency registered in India for at least 5 years should be hired for the purpose of Social Media Research and Insights for the objectives highlighted. Authorization from the agency to be submitted from the agency.	
12	Data Usage and Collection	The service provider will collect and use social media data solely for the purpose of monitoring, analysis, and reporting as agreed upon by the department. The use of unauthorized data scraping or any actions that violate the terms of service of social media platforms is prohibited.	
13	Compliance with Laws	The service provider must comply with all applicable laws, regulations, and guidelines related to data privacy, user consent, and social media usage.	
14	Ethical Use	The service provider must adhere to ethical standards while conducting social media monitoring, avoiding activities that could harm individuals, groups, or organizations.	
15	Avoidance of Data Scraping	The service provider must not engage in any form of automated data scraping or crawling that violates platform terms or applicable laws.	
16	Platform Terms of Use	The service provider is responsible for understanding and complying with the terms of use of each social media platform they monitor.	
17	Reporting and Transparency	The service provider must provide monthly reports on their monitoring activities, methods used, and data handling practices.	
18	Social Media Listening Tool	The agency shall use compliant social media analysis platforms (Hootsuite, InferStrat, Digimind, Sprinklr, Meltwater, or Brandwatch) for the duration of the contract to perform social media monitoring and perception management services.	

		The agency shall ensure that its named staff for this project are proficient in the designated tools to effectively use them for monitoring, analysis, and reporting.	
		The client reserves the right to audit and verify the agency's use of the designated tools to ensure compliance with the contract's terms and conditions.	
19	Expertise Requirement	The agency shall ensure that a team of qualified and experienced professionals with expertise in social media analysis, data cleaning, and data enrichment is available for executing the contracted services. The team shall further include subject matter specialists who possess domain knowledge relevant to the client's industry or field, enhancing the accuracy and relevance of the analysis.	
20	Human-Centric Analysis	The agency shall perform in-depth human-centric analysis of social media data to extract meaningful insights that automated tools might overlook.	
21	Data Cleaning and Enrichment	The agency shall employ data cleaning techniques to eliminate irrelevant, duplicate, or misleading data, and enhance data quality through enrichment.	
22	Expert Validation and Manual Verification	All findings and insights derived from the data shall be validated by qualified experts within the agency's team to ensure accuracy and reliability. The agency shall verify critical information and sensitive data points to minimize the risk of misinformation or misinterpretation.	
23	Data Depth Enhancement	The service provider shall add depth to the data by supplementing quantitative analysis with qualitative observations and interpretations. The agency shall employ a balanced approach by using tools to assist experts, enhancing efficiency without compromising the depth of analysis.	
24	Client Collaboration	The service provider shall collaborate closely with the client to understand their goals, preferences, and objectives, ensuring the analysis aligns with client expectations.	

15.11 Cloud Eligibility Parameters			
Sl. No.	Basic Requirement	Eligibility Criteria	Document to be submitted
1	Legal Entity	The CSP should be a Legal Entity registered under the Companies Act, 2013 or the Companies Act, 1956 OR a Limited Liability Partnership (LLP) registered under the LLP Act, 2008 or Indian Partnership Act 1932.	Copy of Certificate of Incorporation/Registration/Partnership deed
2	MeitY Empanelment	The CSP should be MeitY empaneled (as on bid submission date) OR Indian Government / PSU Cloud Service Provider. The proposed Data Centre should be within India. The proposed Data Centre should be successfully STQC audited. The CSP should be the single point of responsibility by owning and providing Cloud services.	Valid copies of proof attested by authorized Bid signatory
3	Compliance	The CSP is compliant with IT Act 2000 (including 43A) and amendments	Letter from authorized signatory on the letter head of bidder mentioning the compliance.
4	Turnover	The CSP should have a combined total turnover of at least 150 Crore in the last three audited financial years from cloud services (FY 2020-2021, 2021-2022 and 2022-2023).	Certificate from the Statutory Auditor/Chartered Accountant
5	Net worth	The CSP should have positive net worth as per last audited financial report.	Certificate from the Statutory Auditor/Chartered Accountant
6	Blacklisting	The CSP should not be debarred/ blacklisted by any Government/PSU in India as on the date of submission of the Bid.	Letter signed by the Authorized in format given in the RFP.

7	Data Centre Facility	The Data Centre should be at least Tier III standard (certified under TIA 942 or Uptime Institute certifications) and implement tool-based processes based on ITIL standards.	Valid copy of the certificate
8	Data Center Certification	Certification: ISO 27001 – Data Centre and the cloud services should be certified for the latest version of the standards. ISO/IEC 27017:2015-Code of practice for information security controls based on ISO/IEC 27002 for cloud services and Information technology. ISO 27018 – Code of practice for protection of personally identifiable information (PII) in public clouds. ISO-22301 for Business Continuity Management. ISO/IEC 20000-9-Guidance on the application of ISO/IEC 20000-1 to cloud services. PCI DSS – compliant infrastructure for storing, processing, and transmitting credit card information in the cloud.	Valid copy of the certificate
9	DC – DR Configuration	The CSP must be operating in multiple Data Centres in India. DC-DR should not be in the same data center.	Letter from Authorized signatory on the letter head of the bidder..
10	DR Site	Proposed DR site should be decided based on the risk assessment to confirm that the DR location does not share the same risks of the department primary Data Centre. Note:- The secondary Data Center shall be located in a different seismic zone / at least 100 Kms away from the primary Data Centre.	Letter from Authorized signatory on the letter head of the bidder.

11	Experience	The CSP should have successfully implemented / commissioned at least Ten (10) projects of DC/DR with Cloud services provided on MEITY (Ministry of Electronics and Information technology) empaneled cloud for any central/state Govt/PSU or government body/ institution in India during last five financial years (2019-20,2020-21,2021-22,2022-23, 2023-24,) and till the date of Bid submission.)	Work order/contract + completion certificate from client/undertaking of work in progress from bidder
12	Advance Security	The CSP should have accreditations relevant to security, availability, confidentiality, processing integrity, and/or privacy Trust Services principles. SOC 1, SOC 2, SOC 3	Valid copy of the certificate
13	Tax Payment	The CSP must have a valid GST Registration in India and PAN	Valid copy of the certificate
14	Capability	The CSP should provide the department the flexibility to create resources like Virtual instance, storage and other services of custom configuration and should not restrict to specific configuration.	Letter from Authorized signatory on the letter head of the bidder.
15	Public Pricing	The proposed cloud should have public price in INR on the Public calculator for the price validation and verification	Public Links and Letter from Authorized signatory on the letter head of the bidder.
16	GPU	The CSP must have GPU based machines as one of the publicly listed service	Public Links and Letter from Authorized signatory on the letter head of the bidder.

17	Cloud AI/ML	The CSP should have native Unified End-to-End AI/ML Platform as Managed Service : • Managed services for Model training • Build, orchestrate, and automate reproducible ML workflows, easing the transition from experimentation to production • Centralized repository for managing, versioning, and tracking trained ML models • Flexible model serving options (online or batch prediction) at scale with optimized infrastructure • Manage and deploy multiple models or model versions behind a single API endpoint for simplified model serving	Public Links and Letter from Authorized signatory on the letter head of the bidder.
	Cloud Security Posture Management	Centralized Security solution providing a single, consolidated view of the organization security posture covering the following features: • Proactive and Reactive • Vulnerability Scanning • Threat Detection • Compliance Monitoring • Risk Prioritization • Incident Response • Discovery and Inventory	Public Links and Letter from Authorized signatory on the letter head of the bidder.
19	Cloud Native Database	The proposed Cloud should have Native Managed database services for MS-SQL EE and Std. , PostgreSQL and My-SQL enterprise Editions	Public Links and Letter from Authorized signatory on the letter head of the bidder.
20	Cloud Native CDN	The proposed Cloud should have the CSP Native CDN service with Compliances mentioned for Cloud Native CDN	Public Links and Letter from Authorized signatory on the letter head of the bidder.

15.12 Cloud Technical Parameters			
Sl. No.	Name of Service	Specification	Compliance (Yes/No)

1	Security Monitoring and Posture Management	The CSP should have a native service for a comprehensive view of the high-priority security alerts and compliance status across multiple accounts.	
		Native service to provide a single place that aggregates, organizes, and prioritizes the security alerts, or findings, from multiple services and sources.	
		The findings should be visually summarized on integrated dashboards with actionable graphs and tables.	
		CSP should have native capability to continuously monitor the environment using automated compliance checks based on the best practices and industry standards.	
2	Identity and Access Management	The CSP should have native capabilities to securely control access to services and resources for the users.	
		CSP should have native abilities to create and manage users.	
		CSP should have native capabilities to create roles and groups.	
		Native support to enforce permissions-based access to the resources.	
		Native support to manage federated users and their permissions.	
3	Threat Detection	The CSP should offer a native fully managed threat detection service.	
		Capabilities to continuously monitor for malicious or unauthorized behaviour.	
		Capabilities to analyse billions of events across multiple accounts using machine learning to detect anomalies.	
		The threat detection service should be able to generate actionable alerts.	
		The threat detection service should support integration with existing event management and workflow systems.	
4	Security Assessment Services	The CSP should offer a native service for automated security assessment.	
		Native service to help improve the security and compliance of applications deployed on the cloud.	
		Native service to automatically assess applications for exposure, vulnerabilities and deviations from best practices.	

		Service should be able to produce a detailed list of security findings prioritized by level of severity.	
		Should be able to check for unintended network accessibility and vulnerabilities of the VMs.	
5		Should offer pre-defined rules packages mapped to common security best practices and vulnerability definitions Rules should be regularly update by the CSP.	
6	SSL Certificate	The CSP should have a native service to manage and deploy Secure Sockets Layer /Transport Layer Security (SSL/TLS) certificates.	
7	Cloud HSM	The CSP should offer a native, fully managed, cloud-based hardware security module to easily generate and use our own encryption keys on the Cloud.	
		The native hardware security module should be FIPS 140-2 Level 3 compliant.	
		The native hardware security module should support our own encryption keys.	
		The native hardware security module should support deployment in cluster mode for high availability.	
		The native security module should have ability to provide high availability and load balancing.	
		Should be able to provide availability of HSM within 1 hour, in case of any failure of HSM unitC29:C30.	
		The native hardware security module should have support to integrate with the applications using industry-standard APIs.	
8	Firewall Management	The CSP should offer a native security service to centrally configure and manage firewall rules.	
		The native security service should be able to configure firewall rules across multiple accounts and applications.	
		The native security service should provide a mechanism to easily roll out firewall rules.	
		The native security service should be able to support new applications and resources into compliance with a common set of security rules from day one.	
		The native security service should provide a single place to build firewall rules, create security policies, and enforce them in a consistent, hierarchical manner.	

9	Encryption Key Management	The CSP should offer a native, fully managed service to create and manage encryption keys.	
		The native, fully managed key management service should be able to control encryption across a wide range of cloud services and applications.	
		The native, fully managed key management service should be FIPS 140-2 complaint.	
		The native fully managed key management service should be able to provide the logs of all key usage to help meet our regulatory and compliance.	
10	Password Management	The CSP should have a native, fully managed service to centrally manage secrets needed to access the applications, services, and IT resources.	
		The native, fully managed secret management service should be able to easily rotate, manage and retrieve database credentials, API keys, and other secrets throughout their lifecycle.	
		The native, fully managed secret management service should be able to support API based retrieval of secrets.	
		The native, fully managed secret management service should be able to control access to secrets using fine-grained permissions.	
		The native, fully managed secret management service should be able to audit secret rotation centrally for resources in the cloud, third-party services and on-premises.	
11	DDoS Protection	The CSP should have a native managed service to protect against Distributed Denial of Service (DDoS) attacks.	
		The native managed DDoS protection service should provide always-on detection and automatic inline mitigations that minimize application downtime and latency.	
12	Single Sign-On	The CSP should have native support for Single Sign-On (SSO).	
		The native SSO service should be able to centrally manage SSO access to multiple accounts and business applications.	

		The native SSO service should be highly available.	
		The native SSO service should support built-in SAML integrations to many business applications.	
		The native SSO service should be able to extend SSO access to any of the SAML-enabled applications.	
		The native SSO service should be able to use existing corporate credentials to access all the assigned accounts and applications from one place.	
13	Web Application Firewall	The CSP should have a native web application firewall.	
		The native web application firewall should be able to protect the web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources.	
		The native web application firewall should be able to give us control over which traffic to allow or block the web application by defining customizable web security rules.	
		The native web application firewall should support creation of new custom rules and block common attack patterns, such as SQL injection or cross-site scripting, OWASP's Top 10 Web Application Vulnerabilities and rules that are designed for our specific application.	
		The native web application firewall should be able to deploy new rules immediately.	
		The native web application firewall should support API based operations to automate the creation, deployment, and maintenance of web security rules.	
14	Multi-factor authentication	The CSP should offer rule based multi-factor authentication for the cloud portal.	
15	Automated Vulnerability Management	The CSP should offer automated vulnerability management service that continually scans virtual machines and container workloads for software vulnerabilities and unintended network exposure.	

		The CSP native Vulnerability Management Service should automatically detect all newly launched Virtual Machines, and container images pushed to container registry and immediately scans them for software vulnerabilities	
		The CSP native Vulnerability Management Service should perform automated discovery and continual scanning that delivers near real-time vulnerability findings	
16	Hot Tier Storage/ Blob / Object / File Storage	Highly Available and durable storage to be used by applications for frequent use and access of E&P Data sets. This storage should support an availability of >= 99.9%	
17	Block storage	SSD based storage with minimum 6 IOPS per GB which will be used as OS disk. Disk should support native encryption	
18	General Compliance	Secured, authenticated and authorized Service APIs to Provision/Scale/Manage the resources	
		Public Documentation of every API along with examples available in popular programming languages including CLI, Java, Python, Node.js etc.	
		Metering and Monitoring of Service usage in terms of compute, bandwidth, storage, performance metrics	
		Security by Design: Encryption of data at Rest and while Transit enabled by default without any manual configuration required. The TLS certificates and Encryptions keys should be secured by Key Management Solution backed by HSM.	
		Native Integration with CSP Identity and Access Management (IDAM) solution to allow granular access control.	
		Automated Backup of data with IDAM based Access Control, encryption and monitoring for access/download.	
		Automated/Push button scaling with published APIs for scaling so that developers can create custom logic to scale the application as per business requirements.	
		Automated setup of Multiple node cluster to sync data across data centers with option for Synchronous/Asynchronous replication.	
		Automatic Failover without manual intervention.	

		Self-Service capability for Restoration of cluster from backup.	
		Self-heal capability to detect health of underlying hardware and restore services on a different physical host without any manual intervention.	
		Integrated Logging and Monitoring with option to create alerts based on performance anomaly based on Machine Learning.	
		Service version Upgrade with customer having control over the Upgrade window.	
		Automated Operating System Patching with customer having control over the Patching window.	
		CSP should offer the facility to support Active-Active architecture having multiple availability zones with built in fault tolerance to avoid any failure at the underlying hardware infrastructure.	

16. Variable Message Display

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

16.1. Functional Requirements

a) The system should be capable to display warnings, traffic advice, route guidance, situational awareness information and emergency messages to motorists from the CCCs/ICCC in real time by using local PC/Laptops.
b) The VMD should display text and graphic messages using Light Emitting Diode (LED) arrays.
c) The System should be able to display failure status of any LED at CCCs/ICCC.
d) The System should support Display characters in true type fonts and adjustable based on the operating system requirement.
e) The VMD workstation at the CCCs/ICCC should communicate with the VMD controller through the network. It should send out command data to the variable message display controller and to confirm normal operation of the signboard. In return, the VMD workstation should receive status data from the VMD controller.

f) VMD controllers should continuously monitor the operation of the VMD via the provided communication network.
g) Operating status of the variable message display should be checked periodically from the CCCs/ICCC
h) It shall be capable of setting an individual VMD or group of VMD's to display either one of the pre-set messages or symbols entered into the computer via the control computer keyboard or by another means.
i) It shall be capable of being programmed to display an individual message to a VMD or a group of VMD's at a pre-set date and time.
j) A sequence of a minimum of 10 messages/pictures/pre-decided sign or group of signs shall be possible to assign for individual VMD or group of VMD's.
k) It shall also store information about the time log of message displayed on each VMD. The information stored shall contain the identification number of the VMD, content of the message, date and time at which displayed message/picture starts and ends.
l) The central control computer shall perform regular tests (pre-set basis) for each individual VMD. Data communication shall be provided with sufficient security check to avoid unauthorized access.
m) It shall have the capability to display live streaming/program/event, etc.

Variable Message Displays (VMD) Application

a) Central Control Software allows controlling multiple VMD from one console.
b) Capable of programming to display all types of Message/ advertisement having alphanumeric character in English, Hindi and combination of text with pictograms signs. The system should have feature to manage video / still content for VMD. The system should have capability to divide VMD screen into multi-parts to display diverse form of information like video, text, still images, advertisements, weather info, city info etc. The system should also provide airtime management and billing system for paid content management.
c) Capable of controlling and displaying messages on VMD boards as individual/group.
d) Capable of controlling and displaying multiple font types with flexible size and picture sizes suitable as per the size of the VMD.
e) Capable of controlling brightness & contrast through software.
f) Capable to continuously monitor the operation of the Variable Message Display board, implemented control commands and communicate information to the CCCs/ICCC via communication network.
g) Real-time log facility – log file documenting the actual sequence of display to be available at central control system.
h) Multilevel event log with time & date stamp.
i) Access to system only after the authentication and acceptance of authentication based on hardware dongle with its log.
j) Location of each VMD shall be plotted on GIS Map with their functioning status which can be automatically updated.
k) Report generation facility for individual/group/all VMDs with date and time which includes summary of messages, dynamic changes, fault/repair report and system accessed logs, link breakage logs, down time reports or any other customized report.
l) Configurable scheduler on date/day of week basis for transmitting pre-programmed message to any VMD unit.

m) Various users should access the system using single sign on and should be role based. Different roles which could be defined could be Administrator, Supervisor, Officer, Operator, etc.
n) Apart from role-based access, the system should also be able to define access based on location.
o) Rights to different modules / Sub-Modules / Functionalities should be role based and proper log report should be maintained by the system for such access.
p) Components of the architecture should provide redundancy and ensure that there are no single points of failure in the key project components. To take care of remote failure, the systems need to be configured to mask and recover with minimum outage.
q) The architecture should adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft, natural disasters etc. provisions for security of field equipment as well as protection of the software system from hackers and other threats shall be a part of the proposed system.
r) Ease of configuration, ongoing health monitoring, and failure detection are vital to the goals of scalability, availability, and security and should be able to match the growth of the environment.
s) System shall use open standards and protocols to the extent possible.
t) Facility to export reports to excel and PDF formats.

Remote Monitoring

a) All VMD shall be connected/configured to ICCC for remote monitoring through network for two way communication between VMD and control Room to check system failure, power failure & link breakage.
b) Remote Diagnostics to allow identifying failure up to the level of failed individual LED.

16.2. Technical Specifications of VMDs

a. **Size:** Minimum 4.0m length X 3.0m height X 0.2m depth. (4000mm x 3000mm X 200mm approx.)
b. **Colour LED:** Full Colour, class designation C2 as per IRC/EN 12966 standard
c. **Luminance Class/Ratio**: L3 as per IRC/EN 12966 standards.
d. Luminance Control & auto Diming:
- Should be automatically provide different luminance levels but shall also be controllable from the traffic center using software.
- Should have auto dimming capability to adjust to ambient light level (sensor based automatic control)
- Photoelectric sensor shall be positioned at the Display front and Display rear to measure ambient light. Capable of being continually exposed to direct sunlight without impairment of performance.

e. **Contrast Ratio:** R3 as per IRC/EN 12966 standard
f. **Beam Width:** B6+ as per IRC/EN12966 standards.
g. **Pixel Pitch:** 6MM or better
h. Picture Display:
- At least 300mm as per IRC /EN 12966 standards
- Full Matrix: Number of lines & characters adjustable, active area: 3.88m X 2.8m at least

- Synchronized Dot to Dot display.
- Capable of displaying real time message generated by CCCs/ICCC.
- Special frontal design to avoid reflection.
- Display shall be UV resistant.

i. **Viewing Angle**: B6+ as per IRC/EN12966 standard- Viewing angle shall ensure message readability for motorists in all lanes of the approach road.

j. **Viewing Distance**: Suitable for readability from 150 Mtr. or more at the character size of 240mm, from moving vehicles.

k. Self-Test

- VMD shall have self-test diagnostic feature to test for correct operation.
- Display driver boards shall test the status of all display cells in the Display board even when diodes are not illuminated.
- All periodic self-test results shall be relayed to the CCCs/ICCC in real time to update the status of the VMD.

l. Alarms

- Door Open sensor to Inform Control room during unauthorized access.
- LED Pixel failure detection alarm

m. Flicker: Refresh Frequency should not be less 90 Hz. No visible flicker to naked eye.

n. Multiple Data Communication interface/Port: RJ45 Ethernet, RS232, RS 485, FC port and any other suitable

o. Communication (connectivity): Wired & GPRS based wireless technology with 4G/5G.

p. Ambient Operating Temperature: The system should be capable of working in ambient temperature as per Puri weather conditions.

q. Humidity (RH): As Per local environment conditions

r. Protection against Pollution/dust/water: Complete VMD should be of IP 65 protection level from front and IP54 from side and rear. As per EN60529 or equivalent Standard.

s. Power:

- Preferably 170-250V AC (more than 90% power factor) or DC as per equipment requirement.
- Protection for overvoltage/ fluctuation/drop of the nominal voltage (50%) shall be incorporated.
- The enclosure shall contain at least two 15 Amp VAC (industrial grade) outlet socket for maintenance purpose.

t. **Power Back-up & its enclosure:** Should have UPS provisioning as per SLA requirements. The
enclosure of UPS and battery should be pole mountable with IP 65 protected housing and lockable.

u. Material for VMD frame: Preferably at least 2mm aluminium or non-corrosive, water resistant or better. Frame of the VMD should be black & Powder coated**.**

v. Mounting, Installation and finishes:

- Mounting structure shall use minimum 6Mtrs. High Cylindrical GI Pole (Class B) or suitable structure with 5.5 mtr. Minimum vertical clearance under the VMD from the Road surface.
- The mounting shall be capable of withstanding roadside vibrations at site of installation
- It shall be provided with suitable walkway for maintenance access.
- The sides interior and rear of enclosures shall be provided in maintenance free natural aluminium finish. All enclosure shall be flat and wipe clean.

- Rugged locking mechanism should be provided for the onsite enclosures and cabinets.
- For Structural safety, the successful bidder has to provide structural safety certificate from qualified structural engineers approved/ certified by Govt. Agency.

w. Wind Load: WL9 as per EN12966 to withstand high wind speeds and its own load**.**

x. Cabling, connections and Labelling:

- All cable conductors shall be of ISI marked for quality and safety. It shall be of copper insulated, securely fastened, grouped, wherever possible, using tie warps approximately every 10-20 Cms or cable trays.
- All connections shall be vibration-proof quick release connections except for power cables terminating in terminal blocks, which shall be screwed down.
- All terminal blocks shall be made from self-extinguishing materials. Terminations shall be
  logically grouped by function and terminals carrying power shall be segregated from control signal terminals.
- Lightening arrester shall be installed for safety on each VMD.

y. **Local Storage in VMD:** Embedded VMD controller should be capable to store at least 100 messages and symbols/pictograms to allow display to run in isolated mode on a predefined structures/timing, in case of connectivity failure.

Physical/Civil requirement

The IA shall be responsible for carrying out all the civil work required for setting VMD infrastructure including, but not limited to:

- Survey, location finalization in coordination/ approval from Authority
- The IA shall consider for ateral clearance as well as a vertical clearance height as per Public Works Departments/ road repair division following IRC NHAI (National Highway Authority of of India) guidelines.
- Preparation of concrete foundation for VMD Gantry/Pole.
- Hard/soft soil deep digging and backfilling after cabling.
- Erect Gantry/Pole of required size and specifications) with spans, at various locations single lane road, double lane road) for installing VMDs.
- Chambers with metal cover at every junction box, gantry/pole and at road crossings.
- Coordination with relevant authorities for permission to erect gantry/poles and other infrastructure. No commercial/legal fees (except the RoW charges) shall be applicable to Authority for obtaining the necessary permissions.
- To ensure all the components installed in the outdoor locations are vandal proof.
- In case the equipment/sensors get damaged for reasons whatsoever, it shall repair/replace the same in the specified time as per SLAs at no extra cost to the Authority.

Electrical requirements

- IA shall provision for electricity connection to the VMDs through an aggregation point. Since this component has dependency on approval from local authorities, it is recommended that IA plans this requirement well in advance & submits the application to the concerned electricity distribution agency with requisite fees, as applicable.
- IA shall carry out the electrical work required for powering all the components of VMD system

- Electrical installation and wiring shall conform to the electrical codes of India.
- The electricity meters, if any, should be placed inside a power cabinet.

17. Data Center (DC) on premise & Disaster Recovery Center on cloud with 20% capacity for critical application of DC

17.1. Overview

The physical DC and DR on Cloud Infrastructure/ services are planned by the Authority and shall support multiple stakeholders in their effort to deliver the services as part of the Project.
The Data Centre on Cloud shall meet certain key functional requirements and it should cover at the minimum, but not limited to, the following infrastructure components:

- Compute Infrastructure
- Data Storage Infrastructure
- Data Networking
- Cyber Security
- Applications proposed under the scope of IA.

17.2. Functional Requirements

The Authority has identified Data Center and Disaster Recovery Center as one of the important core IT components of the solution. While subscribing to Cloud to suite the functional, scalability and performance requirements, various prevalent deployment models (IaaS, PaaS, SaaS) may be proposed and adopted by IA to design and deploy the use cases.

These different cloud models may be used in combination in a manner that is similar to that used in a traditional IT environment, with underlying infrastructure supporting platforms and services.

- IaaS model: The IA may choose this model to utilize only the virtual machines, storage services (IaaS) from the CSP and deploy/manage their own application or database software.
- PaaS model: The IA may opt for taking platform services (e.g., database, containers, developer tools, AI/ML capabilities) where the application/database software including the underlying Virtual Machines is managed by the CSP.
- SaaS model: Where available, the IA may take the entire software as a service (referred as SaaS) without having to invest on the application development, middleware licenses and underlying infrastructure.

The mix of the above models for an application typically depends on the application (e.g., granularity of control) and business (e.g., need for ease of management) requirements. The IA shall optimize the above service model as per the project requirement and propose the solution meeting the SLA requirement mentioned in Volume III of the RFP.

The IA is required to provide a robust, fault tolerant infrastructure with enterprise grade SLAs with an assured uptime as per SLA defined in the Vol-3 of the RFP. The IA shall not delete any data at the end of the O&M period (for a minimum of 30 days beyond the expiry of the O&M period) without the express approval of Authority.

The Solution/Services proposed by the IA is broadly categorized into the following components:

- Cloud Services
- IT Infrastructure implementation services.
- Operations and Management

The IA shall ensure the following requirements are met:

#	Parameters	Functional Requirement	Bidders Response (on how Functionality shall be met)
1.	Availability	DC and DR shall be operational 24 x 7 x 365 with no single point of failure (NSPoF) at any of the following component level: • Power • Cooling • Fire protection • Data Network • IT infrastructure • Physical security	
2.	Certifications	• DR on cloud shall comply with the following standards: • Tier III or above by UPTIME/TIA-942 • ISO27001, ISO 27017, ISO 27018, ISO 20000-9, ISO/IEC20000-1. • The CSP should be MeitY empanelled /MeitY funded under GoI Cloud (MeghRaj) Initiative	
3	Audit Rights with provisioned cloud services	Management console to the Authority. The IA shall allow review of the provisioned resources (e.g., cloud services, network & security controls, utilizations etc.) and view the configuration of each; Logs of all user activity within an account and any other logs (e.g., n/w traffic, account activity, resource inventory, configuration history, and configuration change) that are captured for audit purpose. The CSP must provide access to the cloud	

#	Parameters	Functional Requirement	Bidders Response (on how Functionality shall be met)
4	Data Storage	The envisaged storage solution shall store video feeds for 30 days. After 30 days, the video feeds would be overwritten unless it is flagged or marked by the Police / Stakeholder Department for investigation or any other purpose. The video feeds of all relevant cameras capturing the incident or flagged in question would be stored until the Police deem it good for deletion. The system shall record the native frame rate and resolution supplied by the camera or as configured by the operator from the System Administration Server. The system shall allow for the frame rate, bit rate and resolution of each camera to be configured independently for recording. The system shall allow the user to configure groups of cameras with the same frame rate, bit rate and resolution for efficient set-up of multiple cameras simultaneously Storage data should be accessible 24 x 7. Storage system should be highly available to meet the demands of the stakeholders	
5	Cloud Services	IA shall provide details of all the IT services procured from the CSP along with: • Availability parameters • SLA parameters • Cyber Security Controls	
6.	DR Location	As per MeitY guidelines	
7.	DR Services	DR Management services shall provide facilities to measure the RTO and RPO parameters regularly. Procured list of services by IA shall meet all the functional requirements for the IT infrastructure given in the RFP	
		DR Management services shall enable Authority to carry out automated DR switchover both in cases of emergencies and during planned DR drills.	
		DR Management services shall enable Authority to carry out phased restoration to switchback services to normal operations in DC.	

17.3. Responsibility Matrix - CSP and IA

An indicative list of the responsibilities between CSP and IA is as below:

#	Description	Cloud Service Provider	Implementation Agency
1	ISO 27001 Compliance & Certification - CSP Managed Infrastructure	Yes	No
2	ISO 27017 Compliance & Certification	Yes	No
3	ISO 27018 Compliance & Certification	Yes	No
4	ISO 2000 Compliance & Certification	Yes	No
5	DR Physical Security & Environmental Controls - Supply Chain Security - Personnel Security - Network Security: Firewall and Other Boundary Devices - Network & Security Continuous Monitoring - Asset Management, Maintenance, and Refresh - Configuration and Change Management - Vulnerability Management - Information Security Incident Response & Management - Resource / Capacity Planning - Business Continuity and Resiliency - Media Protection - Decommissioning / Secure Equipment Disposal	Yes	No
6	Hypervisor Security and Patch Management	Yes	No
7	Conduct a well architected framework review of deployed infrastructure and workloads. Submit the report to Authority once an year	Yes	No
8	Conduct a security review of all the deployed infrastructure and submit reports to Authority once an year	Yes	No
9	Virtual Infrastructure (e.g. Compute, Storage) provisioned in Cloud under the responsibility of the IA - Network & Data Security - Continuous Monitoring - Incident Management - Content Lifecycle Management - Capacity Planning - Backups & Archival - Business Continuity - Provisioning & De-Provisioning of Cloud Services - Termination / Deletion	Provides Self-Service Capabilities	Implementation / Configuration / Monitoring Responsibility
10	Guest Operating System (Security, Patch Management)	Provides	Implementation

#	Description	Cloud Service Provider	Implementation Agency
		Self-Service Capabilities	/ Configuration / Monitoring Responsibility
11	N O C / SO C for the Virtual Private Cloud (VPC) Environment Provisioned in Cloud by the MSP using the audit trail, configuration logs, access logs, network traffic logs.	Provides Self-Service Capabilities	Implementation / Configuration / Monitoring Responsibility
12	Cloud Services - Load Balancers - Virtual Isolated Network - VPN Gateway - Firewall	Provides Self-Service Capabilities	Implementation / Configuration / Monitoring Responsibility
13	Service to monitor, store, and analyse log files from various cloud services provisioned in the Cloud	Provides Self-Service Capabilities	Implementation / Configuration / Monitoring Responsibility
14	Auto Scaling Capability	Provides Self-Service Capabilities	Implementation / Configuration / Monitoring Responsibility
15	Service to record API calls - identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements.	Provides Self - Service Capabilities	Implementation / Configuration / Monitoring Responsibility
16	Service to capture resource (cloud services) inventory, configuration history, and configuration change notifications to enable security and governance	Provides Self - Service Capabilities	Implementation / Configuration / Monitoring Responsibility
17	Notification of security and privacy events affecting Cloud services	Provides Self-Service Capabilities	Monitoring / Necessary Action Responsibility
18	Up-to-the-minute information on service availability and notification of interruptions to each individual service and a full status history of each individual service health.	Publishes Information	Monitoring / Necessary Action Responsibility
19	Alerts and remediation guidance when underlying cloud services are experiencing events that may impact the provisioned services. View into the performance and availability of the cloud services underlying the provisioned resources.	Publishes Alerts & Guidance	Monitoring / Necessary Action Responsibility
20	Services to optimize costs & identify security gaps,	Provides Self-Service	Monitoring / Necessary Action Responsibility

#	Description	Cloud Service Provider	Implementation Agency
		Capabilities	
21	DDoS Protection Service	Yes	No
22	Web Application Firewall (WAF) Service	Provides Self-Service Capabilities	Implementation / Configuration / Monitoring Responsibility
23	Identity & Access Management Service	Provides Self-Service Capabilities	Implementation / Configuration / Monitoring Responsibility
24	Multi-factor Authentication Service	Provides Self-Service Capabilities	Implementation / Configuration / Monitoring Responsibility
25	Key Management & Encryption Service (Data at rest and Data in Transit)	Provides Self-Service Capabilities	Implementation / Configuration / Monitoring Responsibility
26	Uptime S LAs for-Cloud Services	Yes	No
27	Transition Out / Exit Management - Services to export Virtual Machine Images - Services to export customer content / Data	Provides Self-Service Capabilities	Implementation / Exit Management Responsibilities

17.4. Security Compliances

While selecting the CSP, the IA shall ensure compliance to following security controls for cloud services:

- The CSP shall comply with any security requirements applicable to CSPs published (or to be published) by MeitY or any standards body setup / recognized by Government of India from time to time and notified to the CSP by MeitY as a mandatory standard (Refer MeitY published guidelines/reference document)
- The CSP shall meet the security requirements indicated in the IT Act 2000, the terms and conditions of the Provisional Empanelment of the Cloud Service Providers and shall comply with the audit criteria defined by STQC directorate.
- Incident Management shall be taken care of by IA
- Periodic secure code review shall be performed for cloud applications and compliance to secure software development lifecycle.
- Data encryption at rest / transit depending on sensitivity of data shall be implemented using Authority's managed keys, which are not stored on the cloud. Data communications should be encrypted in transit and no access over public network should be allowed
- CSP shall take appropriate measures such as ISO 27001, ISO 27017, ISO 27018, SOC1, SOC2, certifications for their cloud services to secure Authority's content against accidental or

unlawful loss, access, or disclosure.

- E-Discovery shall be included in SLA with IA, a process of locating, preserving, collecting, processing, reviewing, and producing Electronically Stored Information (ESI) in the context of or criminal cases/proceedings or investigation. Logging and reporting (e.g., audit trails of all access and the ability to report on key requirements/indicators) must be ensured.
- The Law Enforcement Agency as mandated under any law in force may seek access to information stored on cloud as provided by the CSP. The onus shall be on the IA to perform all due diligence before releasing any such information to law enforcement agency.
- CSP must ensure location of all data to be stored in India only. The CSP must explicitly detail the access to data being stored and guarantee that there shall be no access to the data or its derivatives to any other commercial entity or any access to foreign entities.
- The CSP's services offerings shall comply with the audit, access and reporting requirements defined under the terms and conditions of the Provisional Empanelment of the CSPs (or STQC /MEITY guidelines).
- SLA with CSP/IA shall cover performance management & dispute resolution escalation. Additionally, refer Guidelines on SLA issued by MeitY which lists out the critical SLAs for cloud services.
- Identification and problem resolution (e.g., helpline, call center, or ticketing system) mechanism must be defined and approved
- Change-management process (e.g., changes such as updates or new services) must be defined with sufficient staging and testing.
- Appropriate segregation of security rules defined as part of firewall should be implemented and there should be provision to have different security rules and zones for different applications & its tiers
- Digital Certificate shall be implemented for secure access.
- The CSP should adhere to the model framework for cyber security (K- 15016/61/2016-SC - 1, Government of India, and Ministry of Urban Development) and also section 9 of this RFP.
- Web servers must be configured as per the CIS hardening guidelines and baseline security requirements, logging and monitoring should be enabled. Application access between hosted applications shall be segregated, internal infrastructure and external traffic, Role based access must be defined, hardening of database instances as per the CIS baselines configuration guidelines in the cloud setup must be ensured, Logging and monitoring must be enabled.
- The proposed CSP architecture may have multiple Data Centres grouped through a low-latency network to support redundancy, higher degree of High-Availability and Fault Tolerance.
- The IA shall provide required DR planning. The following are the key DR requirements for the envisaged solution:
    - The solution should be designed for an Active-Passive DC/DR architecture. In case of Active-Passive architecture, then DR should be provisioned with 100% capacity as provisioned in the DC. System Architecture to be designed to achieve (i) Zero min RPO and 30 minutes RTO for critical applications and (ii) 15 min RPO and 30 minutes RTO for non- critical application.
    - The IA shall be responsible for provisioning of replication bandwidth between DC & D R.

- The IA shall offer services from DR at the time of outages in the DC.
- All servers should be replicated, and automation must be part of the software functionality to failover/failback to the DR-DC adhering to the specified RPO and RTO.
- Failover scenario: The proposed solution should allow pre-built recovery plans for various servers which includes target server configuration, IP configurations, network configuration etc. Test DR Failover scenario should not affect the primary server at all.
- Failback Scenario: The proposed solution should ensure failback to original DC and should take care of replication of only incremental change (changed data after failover) from DR to DC.
- DR drills needs to be performed monthly to check for disaster preparedness and a report to be submitted to Authority. The IA shall also provide a plan for handling the DR scenario including the roles and responsibilities for each stakeholder.
- The IA shall undertake to treat information passed on to them as classified in a secure way. Such Information shall not be communicated / published / advertised by the CSP to any person/organization without the express permission of the Authority.
- IA shall inform all security breach incidents to Authority in real time.

17.5. Enterprise Management System (EMS)

To ensure that ICT systems are delivered at the performance level envisaged, it is important that an effective monitoring and management system be put in place. It is thus proposed that a proven Enterprise Management System (EMS) should be proposed for efficient management of the system, reporting, SLA monitoring and resolution of issues. Various key components of the EMS to be implemented by IA as part of the scope of work of this RFP are:

1. SLA and Contract Management System
2. Network Monitoring System
3. Server & Storage Monitoring System

Make in India & IPR: As per the DPIIT guidelines the prefences to Make in India products.

The proposed solution should be CERT-In certified as per OWASP top -10 vulnerability guidelines by any cert-in empanelled Govt. organization.

OEM proposed EMS software application shall have ISO 9001, ISO 14001, ISO 45001, ISO 27017, ISO 27034-1 and ISO 27001.

The OEM for EMS shall be appraised at a minimum of CMMI Level 3 for Development, demonstrating defined, standardized and documented engineering processes to ensure consistent quality, predictable delivery timelines and effective project risk management

Basic Requirements

- Solution should be inclusive with software, OS and patches, etc.
- Solution should provide for scalability of the whole system without major architectural changes.
- Should be SNMP v1, v2, v3 and MIB-II compliant.
- Filtering of events should be made, with advance sort option based on components, type of message, time etc.
- Should support Web / Administration Interface.
- Solution should be distributed, scalable and open to third party integration.
- Should provide fault and performance management for multi-vendor TCP/IP networks.

SLA & Contract management System

The SLA & Contract Management solution should enable the OCAC to capture all the System based SLAs defined and then calculate monthly (or for any duration) penalty automatically. Measuring service performance requires incorporation of a wide variety of data sources. The SLA solution should support the collection data from various sources in order to calculate Uptime / Performance / Security SLAs. Various features required in this component to EMS are:

- It should be a centralized monitoring solution for all IT assets (including servers, network equipment etc.)
- The solution should have integrated dashboard providing view of non-performing components / issues with related to service on any active components
- The solution should follow governance, compliance and content validations to improve standardization of service level contracts
- Application should be pre-configured so as to allow the users to generate timely reports on the SLAs on various parameters.
- The solution should support Service Level Agreements & Lifecycle Management including Version Control, Status Control, Effectively and audit Trail to ensure accountability for the project.
- The solution should have the ability to define and calculate key performance indicators from an End-to-End Business Service delivery perspective.

Reporting

- Ability to generate reports on penalty and credit due, to check on non-compliance of SLAs
- Monetary penalties to be levied for non-compliance of SLA, thus the system must provide Service Level Performance Report over time, contract, service and more.
- The solution should provide historical and concurrent service level reports for the projects to ensure accountability of the service provider's performance

- Automatic Report creation, execution and Scheduling, must support variety of export formats including Microsoft Word, Adobe PDF, Excel etc.
- Support real-time reports (like at-a-glance status) as well as historical analysis reports (like Trend, TopN, Capacity planning reports etc.)
- Resource utilization exceeding or below customer-defined limits
- Resource utilization exceeding or below predefined threshold limits
- A List of SLAs that needs to be measured centrally by SLA contract management system. These SLAs must be represented using appropriate customizable reports to ensure overall service delivery.

Network Monitoring System

Solution should provide fault & performance management of the server-side infrastructure and should monitor IP\SNMP enabled devices like Routers, Switches, CCTV etc. Proposed Network Management shall also help monitor key KPI metrics like availability, in order to measure SLA's. Following are key functionalities that are required which will assist administrators to monitor network faults & performance degradations in order to reduce downtimes, increase availability restore network services.

- The proposed solution must automatically discover manageable elements connected to the infrastructure and map the connectivity between them. Solution should provide centralized monitoring console displaying network topology map.
- Proposed solution should provide customizable reporting interface to create custom reports for collected data.
- System shall be able to provide network bandwidth utilization and availability report for required period.
- The system must use advanced root-cause analysis techniques for comprehensive analysis of infrastructure faults, security threats/attacks detections, etc.
- The system should be able to send an alert to administrator every time there is change in configuration.

Server and Storage Management

- The proposed tool should integrate with network performance management system and support operating system monitoring for various platforms supplied as part of this Project.
- The proposed tool must provide information about availability and performance for target server and storage nodes.
- The proposed tool should be able to monitor various operating system parameters such as processors, memory, files, processes, file systems, etc. where applicable.

- The proposed system shall through alerts in case of RAM over utilization, Over CPU utilization for physical as well as virtual serves/VMs installed.

18. Functional Requirements for ICCC

The Integrated Command & Control Centre (ICCC) to be developed at **Jagannath Ballabh Parking Complex (JBPC)** shall function as the centralized platform for real-time monitoring, incident management, analytics-driven decision support, and multi-agency coordination for the city of Puri. The ICCC shall support both routine surveillance operations and high-intensity event operations during festivals such as Jagannath Rath Yatra, Snana Purnima, New Year celebrations, and other large gatherings.

The ICCC shall meet, at minimum, the following functional requirements:

1. Real-Time Video Surveillance & Monitoring

- Centralized live monitoring of all CCTV cameras including PTZ, Bullet, Dome, ANPR, Event Cameras and temporary/event deployments.
- High-resolution real-time video streaming with configurable frame rates, quality profiles, and multi-camera display layouts.
- PTZ control with presets, auto-patrol, tracking, zooming and operator overrides.
- Ability to quickly switch between important zones such as Grand Road, Temple periphery, parking locations, railway station, entry/exit corridors and coastal monitoring points.
- Device health status, connectivity status, and uptime monitoring dashboards integrated into the ICCC.

2. Crowd Management and AI-Based Analytics

- Automated crowd density estimation and congestion alerts for all high footfall routes including Temple approaches, Yatra corridor, Beach Road, markets, and parking locations.
- Detection of abnormal crowd behaviour including reverse movement, sudden accumulation, stagnation or panic patterns.
- Heatmaps and movement flow analysis for proactive crowd control.
- User-configurable thresholds for crowd alerts, integrated with response workflows.
- Dashboard visualization of crowd distribution across multiple zones.

3. Incident Detection, Classification & Automated Alerting

The ICCC must support the following intelligent incident detection capabilities:

1. Intrusion and perimeter breach alerts
2. Abandoned or removed object detection
3. Loitering, suspicious activities or prolonged presence
4. Fire and smoke detection

5. Violence-prone behaviours or anomaly patterns
6. Automated prioritization of alerts based on severity and operational rules
7. Audio-visual annunciation of alerts on operator consoles and video walls
8. Incident lifecycle management: acknowledgement → escalation → assignment → closure → audit trail

4. Traffic Monitoring & Vehicle Intelligence (ANPR / RLVD / SVD)

1. Real-time ingestion of ANPR camera streams with accurate license plate detection.
2. Hotlist/blacklist matching for vehicles under surveillance.
3. Monitoring of vehicle movement at all city entry/exit points, major corridors, and enforcement zones.
4. Integration with modules for red-light violation detection and speed violation detection wherever deployed.
5. Storage of vehicle metadata for investigative and enforcement purposes.

5. Multi-Agency Operations & Role-Based Dashboards

The ICCC shall support coordinated operations across:

- Police Department
- District Administration
- Temple Administration (SJTA)
- OBCC
- Railways
- Municipality

Functional Requirements:

1. Role-based access control with differentiated permissions for viewing, control, and analytics.
2. Separate dashboards for sensitive temple-zone video feeds to comply with operational restrictions.
3. Agency-wise routing of alerts based on type of incident (law and order, fire, medical, mobility, sanitation, etc.).
4. Joint dashboard view for inter-departmental collaboration.
5. Integration of viewing centers (e.g., Singhdwar Police Station) with live and recorded feeds.

6. Event Mode Operations (Rath Yatra & Other Large Gatherings)

The ICCC shall have the capability to switch into an enhanced "Event Mode" enabling intensified monitoring and response operations.

Functional Requirements:

1. Seamless integration of temporary/event cameras, portable towers, mobile surveillance units and wireless backhaul links.
2. Ability to ingest drone video streams (as permitted by authorities).
3. Event-specific dashboards showing crowd surges, queue lengths, emergency corridors and hotspot analytics.

4. Configurable SOPs for event-specific alerting and responses.
5. Command hierarchy workflows with operator → supervisor → nodal officer → event commander escalation.
6. Ability to broadcast public announcements through PAS/VMD in case of critical alerts.

7. Video Management System (VMS) Capabilities

The ICCC shall host a unified VMS with the following minimum functionalities:

1. Live viewing, playback, bookmarking, forensic search and evidence generation.
2. Multi-site, multi-server architecture supporting large camera counts.
3. High-availability and failover mechanisms ensuring uninterrupted recording and playback.
4. Map-based navigation allowing operators to select cameras visually.
5. Synchronized playback from multiple cameras for incident reconstruction.
6. Full administrative controls for camera configuration, permissions, storage management and codec parameters.

8. Integration Layer Requirements

The ICCC shall integrate with all relevant systems deployed under the surveillance project, including:

1. Temple Administration's existing ICCC or monitoring systems
2. Police surveillance and incident response systems
3. PAS/VMD systems for coordinated announcements
4. ANPR, Speed Violation and Red-Light Violation systems
5. Video summarization and GPU-based analytics platforms
6. Drone video ingestion framework
7. Body-worn camera feeds
8. Contact center, CRM or ticketing modules used by authorities

All integrations shall follow open API standards and modular plug-in architecture.

9. Data Storage, Retrieval & Archival

1. Centralized storage capable of handling large-scale video retention as per project requirements.
2. High-speed retrieval engine allowing operators to access any recorded footage quickly.
3. Compliance with investigation workflows including secure evidence extraction.
4. Tiered storage models (cloud DR) with redundancy and high availability.
5. Metadata indexing for accelerated search and analytics usage.

10. Performance, Availability & Scalability Requirements

1. ICCC systems shall operate on high-availability architecture ensuring continuity during failures.
2. Redundant compute, storage, networking and application layers must be provisioned.
3. System must scale to incorporate additional locations under Phase-2 and future expansion needs.

4. Power backup with uninterrupted supply for ICCC (UPS, DG set) and redundant cooling/HVAC.
5. Secure configuration ensuring cyber-hardening, audit logging and proactive threat monitoring.

11. Emergency Response Enablement

1. Real-time incident routing to Police, Fire Services, Hospital and Disaster Response teams.
2. SOP-driven workflows ensuring structured response actions.
3. Emergency corridor monitoring and clearance guidance.
4. Display of incident mosaics on video walls for command-level decision-making.
5. Integrated communication infrastructure for field coordination.

12. Documentation, Reporting & Audit Trail

1. Daily operations logbook covering alerts, incidents, camera uptime, network status and operator actions.
2. Automated performance and availability reports for all components.
3. Audit trail of all user activities, evidence retrievals and configuration changes.
4. System health dashboards and warning indicators for proactive maintenance.
5. Secure archival of all logs, reports and backups as per policy.

IA has to provision the viewing capability for the cameras to be procured under the scope of this project with the existing installed cameras and other cameras as required in ICCC project i.e. Implementation of Integrated Command & Control Center. The VMS licenses for the same will be procured by IA. Authority and police department would like to monitor all the cameras (existing and to be procured) from the CCC.

19. Surveillance & Crowd Management System Build Infrastructure

19.1. Proposed ICCC

1. Proposed ICCC shall be constructed in 3rd Floor of JBPC Parking area, third floor (Entertainment Zone) in 4200 sqfts area. Proposed Layout included in this RFP.
2. The viewing centres at SJTC would have access of simultaneous viewing capacity of 48 Nos of CCTV Surveillance Cameras installed under their local jurisdiction. The Viewing Centres will have only viewing rights and data storage would be at Cloud Data Centre only.
3. The IA shall establish Surveillance & Crowd Management System at viewing centers, the indicative key components for the same shall be as follows:

    - VMS Software application with simultaneous viewing capability for monitoring any 48 cameras at each viewing center
    - Operator workstations
    - Furniture and fixtures
    - Active Networking Components
    - Passive Networking Components

- Electrical Cabling and Necessary LED Illumination Devices
- Workstations
- UPS

4. The following required IT and Non-IT Infrastructure for establishment of Viewing Centre shall be provided by IA, but not limited to:

   a. All Electricity Equipment's' including luminance devices
   b. All networking devices including switches, routers, cabling, Internet / WI-FI etc.
   c. Online UPS
   d. Fixtures and Furniture
   e. IP Phones / Telecommunication Infrastructure
   f. Workstations
   g. Software application licenses
   h. Cyber Security systems
   i. Video Wall Solutions
   j. Cooling infrastructure

19.2. Technical Specification for Videowall LED Display for ICCC

Sr. No.	Parameters	Minimum Specifications
1	Technology	HD LCD Display, Direct LED Backlight
2	Screen Size	55" diagonal or better for viewing centers
3	Resolution	Full high definition (Min 1920 x 1080) 16:9 Widescreen
4	Contrast ratio	5000:1
5	Brightness	500 nits
6	Viewing angle	178 degree/178 degree (H/V)
7	Response time	8ms
8	Control	- RS232 control - On Screen Display (OSD)
9	Operations	24x7
10	LED Backlight Lifetime	Minimum backlight lifetime of 100,000 hours

11	Additional Specifications	CE, CB, BIS, RoHS, ISO 27000, ISO 9000

19.3. Technical Specification for Video Wall Controller

Sr. No.	Parameters	Minimum Specifications
1	Display controller	Controller to control Video wall in a matrix (4x2 output) as per requirement along with software
2	Processor	Latest Generation 64-bit x86 Quad Core processor (3.4 Ghz) or Better
3	RAM	16 GB DDR3 ECC RAM
4	HDD	2x 480 GB/better or 7200 RPM HDD (Configured in RAID 0)
5	RAID	Should support RAID 0 and 1
6	Networking	Dual-port Gigabit Ethernet Controller with RJ-45 ports
7	Accessories	104 key Keyboard and Optical USB mouse
8	OS	Supports 64-bit Operating Systems Windows 10
9	Chassis	19” Rack mount
10	Power Supply	(1+1) Redundant hot swappable
11	Redundancy Support	Power Supply, HDD, LAN port & Controller
12	Scalability	Display multiple source windows in any size, anywhere on the Wall
13	Control Functions	Brightness/ Contrast/ Saturation/ Hue/ Filtering/ Crop/ Rotate
14	Video Wall, Controller, Cube & wall management	Video Wall, Controller, Cube & Wall management software should preferably be from same OEM for ensuring smooth operations and seamless integration and feature enablement and enhancement.

19.4. Video Wall Management Software

Sr. No.	Parameters	Minimum Specifications
1	Display & Scaling	Display multiple sources anywhere on display up to any size
2	Input Management	All input sources can be displayed on the video wall in freely resizable and movable windows
3	Scenarios management	Save and Load desktop layouts from Local or remote machines
4	Layout Management	Support all Layout from Input Sources, Internet Explorer, Desktop and Remote Desktop Application
5	Multi View Option	Multiple view of portions or regions of Desktop, Multiple Application Can view from single desktop
6	Other Features	• SMTP support • Remote Control over LAN • Alarm Management • Remote Management • Multi concurrent client • KVM Support

20. Annexure 1: List of Locations

20.1. Permanent and Temporary Parking Details

S. No.	Name of the Location	Type of the Location	Number of Roads	Number of Lanes
1	Talabania Parking	Temporary Parking	2	2
2	Samanga Village	Temporary Parking	2	2
3	JBPC	Permanent Parking	3	3
4	Old JBPC	Permanent Parking	2	2

S. No.	Name of the Location	Type of the Location	Number of Roads	Number of Lanes
5	Lokanath Parking	Temporary Parking	2	2
6	Gadadhar High School	Temporary Parking	2	2
7	Jatrika	Permanent Parking	2	2
8	Nalifield	Permanent Parking	2	2
9	Bhudan Parking	Permanent Parking	2	2
10	Helipad Parking	Permanent Parking	2	2
11	Horticulture Parking	Temporary Parking	2	2
12	Hygienic Fish Market	Temporary Parking	2	2
13	Sterling Parking	Temporary Parking	2	2
14	Sonar Bangla	Temporary Parking	2	2
15	Blue Lilly	Temporary Parking	2	2
16	Saha College	Temporary Parking	2	2
17	Matiotta Parking	Temporary Parking	2	2
18	Digabareni Parking	Permanent Parking	2	2
19	Market Chhaka Parking	Permanent Parking	2	2
20	Jail Road Parking	Permanent Parking	2	2

20.2. Locations to be Covered in Phase - 1

S. No	Name of the Location	Type of the Location	Phase (1/2)	Number of Roads	Number of Lanes	Proposed Solution
Bhubaneshwar to Puri Road - Uttra Crossing to Malatipatapur						
1	Uttara Crossing	Entry/Exit	Phase 1	2	4	ANPR and Surveillance
2	Gudiapokhari	Entry/Exit	Phase 1	1	1	ANPR and Surveillance
3	Biragobindapur Chhaka	Entry/Exit	Phase 1	1	1	ANPR and Surveillance
4	Samjajpur By-Pass Chhaka	Entry/Exit	Phase 1	2	2	ANPR and Surveillance
5	Tulasi Chaura By-pass	Entry/Exit	Phase 1	1	1	ANPR and Surveillance
6	Malatipatapur	Square	Phase 1	4	8	ITMS
Konark to Puri Road - Tosali Chhaka to Konark						
7	Tosali Chhaka	Tri Junction	Phase 1	3	6	ANPR and Surveillance
8	Balighai Chhaka	Tri Junction	Phase 1	3	6	ANPR and Surveillance
Satapada to Puri Road - Mangalaghata Chhaka to Satapada						
9	Mangalaghata	Square	Phase 1	4	8	ITMS
Grand Road						
10	Jagabalia Lodge	Approach road to GR	Phase 1	1	1	Surveillance
11	Kakudi Khai Chhaka	Approach road to GR	Phase 1	2	2	Surveillance
12	Dhana Kothi Sahi Lane	Approach road to GR	Phase 1	1	1	Surveillance

S. No	Name of the Location	Type of the Location	Phase (1/2)	Number of Roads	Number of Lanes	Proposed Solution
13	Gandua Chaura Chhaka	Approach road to GR	Phase 1	2	2	Surveillance
14	Baseli Thakurani Lane	Approach road to GR	Phase 1	1	1	Surveillance
15	Baijayantri Lane	Approach road to GR	Phase 1	1	1	Surveillance
16	Odia Matha Lane	Approach road to GR	Phase 1	1	1	Surveillance
17	Gadanti Chhaka	Approach road to GR	Phase 1	2	2	Surveillance
18	Uttaraparswa Matha side Lane	Approach road to GR	Phase 1	1	1	Surveillance
19	Dolabedi Kona	Approach road to GR	Phase 1	3	3	Surveillance
20	Sanachhatra Matha	Approach road to GR	Phase 1	1	1	Surveillance
21	Shree Marga Entry Point	Approach road to GR	Phase 1	1	1	Surveillance
22	Shree Marga crossing to SKCH Lane	Approach road to GR	Phase 1	2	2	Surveillance
23	Shree Marga crossing to Shani Temple Lane	Approach road to GR	Phase 1	2	2	Surveillance
24	In front of Sugriba Temple	Approach road to GR	Phase 1	1	1	Surveillance
25	Shree Marga End Point	Approach road to GR	Phase 1	1	1	Surveillance
26	Grand Center	Approach road to GR	Phase 1	2	2	Surveillance
27	Raja Nahar Lane	Approach road to GR	Phase 1	1	1	Surveillance
28	Shyama Kunja Lane	Approach road to GR	Phase 1	1	1	Surveillance
29	Dudhwuala Dharmasala	Approach road to GR	Phase 1	1	1	Surveillance

S. No	Name of the Location	Type of the Location	Phase (1/2)	Number of Roads	Number of Lanes	Proposed Solution
30	Surya Complex	Surveillance Point	Phase 1	0	0	Surveillance
31	Shani Temple Lane	Approach road to GR	Phase 1	1	1	Surveillance
32	Marichikote Lane	Approach road to GR	Phase 1	1	1	Surveillance
33	Smart Bazar	Approach road to GR	Phase 1	1	1	Surveillance
34	Anapurna Theater	Approach road to GR	Phase 1	1	1	Surveillance
35	Goenka Dharmasala	Surveillance Point	Phase 1	0	0	Surveillance
36	Town PS Chhaka	Approach road to GR	Phase 1	1	1	Surveillance
37	Jagannath Ballava Entry Gate	Approach road to GR	Phase 1	1	1	Surveillance
38	Fish Market Lane	Approach road to GR	Phase 1	1	1	Surveillance
39	Balabhadra Lane	Approach road to GR	Phase 1	1	1	Surveillance
40	Chudapati Lane	Approach road to GR	Phase 1	1	1	Surveillance
41	Narendra Kona Lane	Approach road to GR	Phase 1	2	2	Surveillance
42	Hotel Paradise	Surveillance Point	Phase 1	0	0	Surveillance
43	T.P. Hotel	Surveillance Point	Phase 1	0	0	Surveillance
44	Nayak Plaza side Lane	Approach road to GR	Phase 1	1	1	Surveillance
45	Akhaya Patra Foundation side Lane	Approach road to GR	Phase 1	1	1	Surveillance
46	Mausima Temple side Lane	Approach road to GR	Phase 1	1	1	Surveillance

S. No	Name of the Location	Type of the Location	Phase (1/2)	Number of Roads	Number of Lanes	Proposed Solution
47	M Bazar side Lane	Approach road to GR	Phase 1	1	1	Surveillance
48	Kachera Matha Lane	Approach road to GR	Phase 1	1	1	Surveillance
49	Majana Jaga Lane	Approach road to GR	Phase 1	1	1	Surveillance
50	Ray Bahadur Lane	Approach road to GR	Phase 1	1	1	Surveillance
51	ICICI Bank	Surveillance Point	Phase 1	0	0	Surveillance
52	Salabega Matha	Surveillance Point	Phase 1	0	0	Surveillance
53	Blood Bank Entry gate	Approach road to GR	Phase 1	1	1	Surveillance
54	Petrol Pump side Lane	Approach road to GR	Phase 1	1	1	Surveillance
55	Vishal Megamart Lane	Approach road to GR	Phase 1	1	1	Surveillance
56	Medical Chhaka	Square	Phase 1	2	4	Surveillance
57	Upara amiashai Lane	Approach road to GR	Phase 1	1	1	Surveillance
58	Tala Malisahi Lane	Approach road to GR	Phase 1	1	1	Surveillance
59	Mali Jaga Lane	Approach road to GR	Phase 1	1	1	Surveillance
60	Jail Road Parking	Approach road to GR	Phase 1	1	1	Surveillance
61	V. Mart	Surveillance Point	Phase 1	0	0	Surveillance
62	Alok Sweets	Surveillance Point	Phase 1	0	0	Surveillance
63	Red Cross Road	Approach road to GR	Phase 1	2	2	Surveillance

S. No	Name of the Location	Type of the Location	Phase (1/2)	Number of Roads	Number of Lanes	Proposed Solution
64	Egg Center Lane	Approach road to GR	Phase 1	1	1	Surveillance
65	Kumuti Sahi Lane	Approach road to GR	Phase 1	1	1	Surveillance
66	Sudarsan Nagar Lane	Approach road to GR	Phase 1	1	1	Surveillance
67	Sankeswari Lane	Approach road to GR	Phase 1	1	1	Surveillance
68	Sangram Club Lane	Approach road to GR	Phase 1	1	1	Surveillance
69	Gajapati Nagar Lane	Approach road to GR	Phase 1	1	1	Surveillance
70	Khadi Matha Nuasahi Lane	Approach road to GR	Phase 1	1	1	Surveillance
71	Abhaya Mahaveer Temple side Ln	Approach road to GR	Phase 1	1	1	Surveillance
72	Baulamath Lane	Approach road to GR	Phase 1	1	1	Surveillance
73	Next Lane to Baula Matha	Approach road to GR	Phase 1	1	1	Surveillance
74	Abakash Lane	Approach road to GR	Phase 1	1	1	Surveillance
75	Friend's Club Lane	Approach road to GR	Phase 1	1	1	Surveillance
76	Aai Tota Lane	Approach road to GR	Phase 1	1	1	Surveillance
77	Pejanala Lane	Approach road to GR	Phase 1	1	1	Surveillance
78	Bus Stand Entry	Approach road to GR	Phase 1	1	2	Surveillance
Atharnala to Jatiababaji Chhaka						
79	Atharanala	Tri Junction	Phase 1	3	3	ANPR and Surveillance

S. No	Name of the Location	Type of the Location	Phase (1/2)	Number of Roads	Number of Lanes	Proposed Solution
80	Kumbharapada PS Chhaka	Tri Junction	Phase 1	3	3	ANPR and Surveillance
81	Jatiababaaji Chhaka (Entry towards Narendra Pond)	Square	Phase 1	4	4	Surveillance
Balighat to Atharanala Chhaka via Matiapada						
82	Balighata Chhaka	Tri Junction	Phase 1	3	3	Surveillance
83	Siddha Mahaveer Lvl Crossing	Railway Crossing	Phase 1	3	3	Surveillance
84	Indradyumna Crossing	Tri Junction	Phase 1	3	3	Surveillance
85	Matiapada Chhaka	Square	Phase 1	4	4	Surveillance
86	Akhandalamani Chhaka	Tri Junction	Phase 1	3	3	Surveillance
Helipad Chhaka to Matiapada Chhaka						
87	Railway Station Gate I (RPF Office)	Lane	Phase 1	2	2	Surveillance
88	Railway Station Gate II (Main Gate under construction)	Lane	Phase 1	2	2	Surveillance
89	Railway Station Gate III (Main Gate under construction)	Lane	Phase 1	2	2	Surveillance
90	Railway Station Gate IV (RMS Office side)	Lane	Phase 1	2	2	Surveillance
91	Bus Stand Exit Point	Lane	Phase 1	1	1	Surveillance
Malatipatpur to Sterling Road Chhak						
92	Cutting point of Malatipatpur	Surveillance Point	Phase 1	2	2	Surveillance
93	Batagaon	Square	Phase 1	4	4	ITMS

S. No	Name of the Location	Type of the Location	Phase (1/2)	Number of Roads	Number of Lanes	Proposed Solution
94	Sterling Resort Chhaka	Tri Junction	Phase 1	3	6	ANPR and Surveillance
95	Sterling Resort Bridge	Surveillance Point	Phase 1	2	2	Surveillance
Critical Locations for Surveillance						
96	Beleswar Temple	Surveillance Point	Phase 1	2	2	Surveillance
97	Narayani Temple	Surveillance Point	Phase 1	2	2	Surveillance
98	Bailharchandi Temple	Surveillance Point	Phase 1	2	2	Surveillance
Parking						
1	Talabania Parking	Temporary Parking	Phase 1	2	2	Parking
2	Samanga Village	Temporary Parking	Phase 1	2	2	Parking
3	JBPC	Permanent Parking	Phase 1	3	4	Parking
4	Old JBPC	Permanent Parking	Phase 1	2	2	Parking
5	Lokanath Parking	Temporary Parking	Phase 1	2	2	Parking
6	Gadadhar High School	Temporary Parking	Phase 1	2	2	Parking
7	Jatrika	Permanent Parking	Phase 1	2	2	Parking
8	Nalifield	Temporary Parking	Phase 1	2	2	Parking
9	Bhudan Parking	Temporary Parking	Phase 1	2	2	Parking
10	Helipad Parking	Temporary Parking	Phase 1	2	2	Parking

S. No	Name of the Location	Type of the Location	Phase (1/2)	Number of Roads	Number of Lanes	Proposed Solution
11	Horticulture Parking	Temporary Parking	Phase 1	2	2	Parking
12	Hygienic Fish Market	Temporary Parking	Phase 1	2	2	Parking
13	Sterling Parking	Temporary Parking	Phase 1	2	2	Parking
14	Sonar Bangla	Temporary Parking	Phase 1	2	2	Parking
15	Blue Lilly	Temporary Parking	Phase 1	2	2	Parking
16	Saha College	Temporary Parking	Phase 1	2	2	Parking
17	Matiotta Parking	Temporary Parking	Phase 1	2	2	Parking
18	Digabareni Parking	Permanent Parking	Phase 1	2	2	Parking
19	Market Chhaka Parking	Permanent Parking	Phase 1	2	2	Parking
20	Jail Road Parking	Permanent Parking	Phase 1	2	2	Parking

20.3. Locations to be Covered in Phase - 2

S. No	Name of the Location	Type of the Location	Phase (1/2)	Number of Roads	Number of Lanes	Proposed Solution
Bhubaneshwar to Puri Road - Uttra Crossing to Malatipatapur						
1	Pipili Toll Gate	Entry/Exit	Phase 2	2	4	ANPR and Surveillance

S. No	Name of the Location	Type of the Location	Phase (1/2)	Number of Roads	Number of Lanes	Proposed Solution
2	Baghuabanka Chhaka (Netaji Club)	Entry/Exit	Phase 2	2	4	ANPR and Surveillance
3	Mangalpur	Entry/Exit	Phase 2	1	1	ANPR and Surveillance
4	Satasankha Bazar	Entry/Exit	Phase 2	2	2	ANPR and Surveillance
5	Pattnaikia Bazar	Entry/Exit	Phase 2	2	4	ANPR and Surveillance
6	U.G.S. College, Sakhigopal	Entry/Exit	Phase 2	1	2	ANPR and Surveillance
Konark to Puri Road - Tosali Chhaka to Konark						
7	Ramchandi Chhaka	Entry/Exit	Phase 2	2	4	ANPR and Surveillance
8	Chandrabagha Chhaka	Entry/Exit	Phase 2	2	4	ANPR and Surveillance
9	Labanya Lodge Chhaka	Tri Junction	Phase 2	3	6	ANPR and Surveillance
10	Konark Chhaka	Square	Phase 2	4	8	ITMS
11	Konark PS Crossing	Entry/Exit	Phase 2	2	4	ANPR and Surveillance
12	Junei Bazar	Entry/Exit	Phase 2	2	4	ANPR and Surveillance
Konark to Puri Road - Balighai Chhaka to Nimapada Chhaka						

S. No	Name of the Location	Type of the Location	Phase (1/2)	Number of Roads	Number of Lanes	Proposed Solution
13	Chhaitana Bazar	Tri Junction	Phase 2	3	6	ANPR and Surveillance
14	Nagapur Bazar	Entry/Exit	Phase 2	2	4	ANPR and Surveillance
Satapada to Puri Road - Mangalaghata Chhaka to Satapada						
15	Girala Chhaka	Tri Junction	Phase 2	3	6	ANPR and Surveillance
16	Brahmagiri Chhaka	Entry/Exit	Phase 2	2	4	ANPR and Surveillance
17	Satapada (Chilika lake)	Entry/Exit	Phase 2	2	4	ANPR and Surveillance
Around the Grand Road						
18	Narayani Chhaka	Square	Phase 2	4	4	ANPR and Surveillance
19	Janhi Mundia Chhaka	Square	Phase 2	4	4	ANPR and Surveillance
20	Mochi Sahi Chhaka	Tri Junction	Phase 2	3	3	ANPR and Surveillance
21	Narisewa Sadan	Tri Junction	Phase 2	3	3	Surveillance
22	Town Hall Chhaka	Tri Junction	Phase 2	3	3	Surveillance
23	Court Chhaka	Square	Phase 2	4	4	Surveillance

S. No	Name of the Location	Type of the Location	Phase (1/2)	Number of Roads	Number of Lanes	Proposed Solution
24	Jenari Gachha Chhaka	Tri Junction	Phase 2	3	3	Surveillance
25	Govt Girl's High School Chhaka	Square	Phase 2	4	4	ANPR and Surveillance
26	Labania Khia Chhaka	Square	Phase 2	4	4	ANPR and Surveillance
27	Jaduani Library Chhaka	Tri Junction	Phase 2	3	3	Surveillance
28	Book's Corner Chhaka	Square	Phase 2	4	4	Surveillance
29	Boarding Chhaka	Square	Phase 2	4	4	Surveillance
30	Dargi Pokhari Chhaka	Tri Junction	Phase 2	3	3	Surveillance
31	Jhadeswari Chhaka	Square	Phase 2	4	8	Surveillance
32	Gopalswamy Chhaka	Square	Phase 2	4	4	Surveillance
33	Sankaracharya Math Chhaka	Square	Phase 2	4	4	Surveillance
34	Jambeswar Chhaka	Square	Phase 2	4	4	Surveillance
35	Berahi Lane	Lane	Phase 2	2	2	Surveillance
36	Dhanakothisahi Lane	Lane	Phase 2	2	2	Surveillance

S. No	Name of the Location	Type of the Location	Phase (1/2)	Number of Roads	Number of Lanes	Proposed Solution
37	Manikaricha Sahi Chhaka	Tri Junction	Phase 2	3	3	Surveillance
38	Telephone Exchange	Square	Phase 2	4	4	Surveillance
39	Balipanda PS Chhaka	Lane	Phase 2	2	2	Surveillance
40	Harchandi Sahi Lane	Lane	Phase 2	2	2	Surveillance
41	Solakhia Baragacha	Tri Junction	Phase 2	3	3	Surveillance
42	Trisakti Club Chhaka	Lane	Phase 2	2	2	Surveillance
43	Kadamgargh Chhaka	Tri Junction	Phase 2	3	3	Surveillance
44	Sudarsan Guest House	Tri Junction	Phase 2	3	3	Surveillance
45	Dakhinakali Temple Lane	Lane	Phase 2	2	2	Surveillance
46	Barabati Kalyan Mandap	Tri Junction	Phase 2	3	3	Surveillance
47	Brushab Chhaka	Tri Junction	Phase 2	3	3	Surveillance
48	Chhapan Chhaka	Tri Junction	Phase 2	3	3	Surveillance
49	Sankareswar Temple Chhaka	Square	Phase 2	4	4	Surveillance

S. No	Name of the Location	Type of the Location	Phase (1/2)	Number of Roads	Number of Lanes	Proposed Solution
50	Pandey Jaga	Tri Junction	Phase 2	3	3	Surveillance
51	Markanda Pond Chhaka	Square	Phase 2	4	4	Surveillance
52	Youngstar Club Chhaka	Tri Junction	Phase 2	3	3	Surveillance
53	Chudanga Sahi Banamber Chhaka	Square	Phase 2	4	4	Surveillance
54	Jagannath Ballav Entry Pt. Chhaka	Tri Junction	Phase 2	3	3	Surveillance
55	Bisesswari Temple Chhaka	Square	Phase 2	4	4	Surveillance
56	Women's College Chhaka	Tri Junction	Phase 2	3	3	Surveillance
57	Narendra Kona	Lane	Phase 2	2	4	Surveillance
Malatipatapur to Harekrushnapur via Grid Station						
58	ROB Start Point	Lane	Phase 2	1	2	Surveillance
59	ROB End Point	Lane	Phase 2	1	2	Surveillance
60	Baidas Nagar Chhaka	Tri Junction	Phase 2	3	6	ANPR and Surveillance
61	Grid Station	Tri Junction	Phase 2	3	3	ANPR and Surveillance

S. No	Name of the Location	Type of the Location	Phase (1/2)	Number of Roads	Number of Lanes	Proposed Solution
62	Biraharekrushnapur RL Crossing	Railway Crossing	Phase 2	1	2	Surveillance
Grid Station to Penthakata Chhaka						
63	Bhudan Chhaka	Tri Junction	Phase 2	3	3	Surveillance
64	Talabania parking diversion point (Indoor Stadium)	Tri Junction	Phase 2	3	3	Surveillance
65	Central School Chhaka	Tri Junction	Phase 2	3	3	Surveillance
66	Helipad Chhaka	Square	Phase 2	4	4	Surveillance
67	Penthakata Chhaka	Tri Junction	Phase 2	3	3	Surveillance
Helipad Chhaka to Matiapada Chhaka						
68	Mangala Temple	Tri Junction	Phase 2	3	3	Surveillance
69	Sadar Block Office	Square	Phase 2	4	4	Surveillance
70	Odisha Bakery	Tri Junction	Phase 2	3	3	Surveillance
71	Water Works Road	Tri Junction	Phase 2	3	3	Surveillance
72	Srikhsetra Colony	Square	Phase 2	4	4	Surveillance

S. No	Name of the Location	Type of the Location	Phase (1/2)	Number of Roads	Number of Lanes	Proposed Solution
73	Ram Mandir Chhaka	Tri Junction	Phase 2	3	3	Surveillance
74	Ghoda Bazar Chhaka	Tri Junction	Phase 2	3	3	Surveillance
75	Garuda Chhaka	Tri Junction	Phase 2	3	3	Surveillance
76	Ashram Chhaka	Square	Phase 2	4	4	Surveillance
77	Nrusingha Temple backside	Lane	Phase 2	1	1	Surveillance
Sea Beach Road						
78	Rock Bay Hotel	Tri Junction	Phase 2	3	3	Surveillance
79	Sunara Gouranga	Tri Junction	Phase 2	3	3	Surveillance
80	Bedi Hanuman Chhak	Tri Junction	Phase 2	3	3	Surveillance
81	Gandhar Hotel	Surveillance Point	Phase 2	2	2	Surveillance
82	Sales Tax Office	Surveillance Point	Phase 2	2	2	Surveillance
83	Raja Restaurant	Tri Junction	Phase 2	3	3	Surveillance
84	Vigilance office	Tri Junction	Phase 2	3	3	Surveillance

S. No	Name of the Location	Type of the Location	Phase (1/2)	Number of Roads	Number of Lanes	Proposed Solution
85	Holiday Resort Lane	Surveillance Point	Phase 2	2	2	Surveillance
86	BNR Chhaka	Tri Junction	Phase 2	3	3	Surveillance
87	Youth Hostel Chhaka	Tri Junction	Phase 2	3	3	Surveillance
88	Kanika Kothi	Surveillance Point	Phase 2	2	2	Surveillance
89	Grand Chilli	Surveillance Point	Phase 2	2	2	Surveillance
90	Mother Public School	Tri Junction	Phase 2	3	3	Surveillance
91	Niladri Beach	Surveillance Point	Phase 2	2	2	Surveillance
92	Mayfair Hotel	Square	Phase 2	4	4	Surveillance
93	Jamidar Palace	Tri Junction	Phase 2	3	3	Surveillance
94	Urban Haat entry point	Surveillance Point	Phase 2	2	2	Surveillance
95	Subash Bose Chhaka	Square	Phase 2	4	4	ITMS
96	Blue Flag Beach	Surveillance Point	Phase 2	2	2	Surveillance
97	Collector Office	Surveillance Point	Phase 2	2	2	Surveillance

S. No	Name of the Location	Type of the Location	Phase (1/2)	Number of Roads	Number of Lanes	Proposed Solution
98	Governor House	Tri Junction	Phase 2	3	3	Surveillance
99	Acharyaharhar Chhaka	Square	Phase 2	4	4	Surveillance
100	Digabareni Chhaka	Square	Phase 2	4	4	Surveillance
101	Shakuntala Hotel side lane	Tri Junction	Phase 2	3	3	Surveillance
102	Puri Hotel Side Lane	Tri Junction	Phase 2	3	3	Surveillance
103	Victoria Hotel Side Lane	Tri Junction	Phase 2	3	3	Surveillance
104	State Emporium side lane	Tri Junction	Phase 2	3	3	Surveillance
105	Bali Nolia Sahi Lane	Tri Junction	Phase 2	3	3	Surveillance
106	Sea View Hotel side lane	Tri Junction	Phase 2	3	3	Surveillance
107	Renuka Lane	Tri Junction	Phase 2	3	3	Surveillance
108	Sonali Hotel Side Lane	Tri Junction	Phase 2	3	3	Surveillance
109	Chaitanya Chhaka	Tri Junction	Phase 2	3	3	Surveillance
110	Swargadwar Front side	Surveillance Point	Phase 2	2	2	Surveillance

S. No	Name of the Location	Type of the Location	Phase (1/2)	Number of Roads	Number of Lanes	Proposed Solution
111	New Seahawk	Surveillance Point	Phase 2	2	2	Surveillance
112	Suv Palace Chhaka	Tri Junction	Phase 2	3	3	Surveillance
113	Light House Chhaka	Tri Junction	Phase 2	3	3	Surveillance
114	Gochikar Guest House	Surveillance Point	Phase 2	2	2	Surveillance
115	Camelia Hotel	Surveillance Point	Phase 2	2	2	Surveillance
116	Asian INN Hotel	Surveillance Point	Phase 2	2	2	Surveillance
117	Tara Palace Hotel	Surveillance Point	Phase 2	2	2	Surveillance
118	Lazmi Resort Hotel	Surveillance Point	Phase 2	2	2	Surveillance
119	Patrika Hotel	Surveillance Point	Phase 2	2	2	Surveillance
120	Shri Hari Hotel	Surveillance Point	Phase 2	2	2	Surveillance
121	Lucky India Hotel	Surveillance Point	Phase 2	2	2	Surveillance
122	Regenta Central	Surveillance Point	Phase 2	2	2	Surveillance
123	Fortune hotel	Surveillance Point	Phase 2	2	2	Surveillance

S. No	Name of the Location	Type of the Location	Phase (1/2)	Number of Roads	Number of Lanes	Proposed Solution
124	Kathia Bada	Surveillance Point	Phase 2	2	2	Surveillance
125	Hans Coco Palm Chhaka	Tri Junction	Phase 2	3	3	Surveillance
126	Swosti Premium Front Chhaka	Surveillance Point	Phase 2	2	2	Surveillance
127	Swosti Premium Back side lane entry point	Surveillance Point	Phase 2	2	2	Surveillance
Parallel Road to Sea Beach Road						
128	Matamatha Road Chhaka	Tri Junction	Phase 2	3	3	Surveillance
129	Prachi Chhaka	Tri Junction	Phase 2	3	3	Surveillance
130	Bidhaba Ashram Chhaka	Square	Phase 2	4	4	Surveillance
131	Kakatura Restaurant Chhaka	Square	Phase 2	4	4	Surveillance
132	Swargadwar Chhaka	Square	Phase 2	4	4	Surveillance
133	Bharatiya Sebasram Chhaka	Tri Junction	Phase 2	3	3	Surveillance
134	Gochhikari Chhaka	Square	Phase 2	4	4	Surveillance
135	Homeo Research Center	Surveillance Point	Phase 2	2	2	Surveillance

S. No	Name of the Location	Type of the Location	Phase (1/2)	Number of Roads	Number of Lanes	Proposed Solution
136	D.K. Hotel Side Lane	Surveillance Point	Phase 2	2	2	Surveillance
New Jagannath Sadak						
137	Bira Narasinghpur Chhaka	Square	Phase 2	4	4	Surveillance
138	Bhailpur Chhaka	Square	Phase 2	4	4	Surveillance
139	Sukala	Surveillance Point	Phase 2	2	2	Surveillance
140	Bijipur	Tri Junction	Phase 2	3	3	Surveillance
141	Chupuringi	Tri Junction	Phase 2	3	3	Surveillance
Sea Beach Surveillance						
142	Sea Beach	Sea Beach Lane and Beach Area	Phase 2	1	1	Surveillance
Speed Detection System						
143	Between Mangalaghat and Sterling	Speed Detection System	Phase 2	2	4	Speed Violation Detection
144	Between Sterling and Light House	Speed Detection System	Phase 2	2	4	Speed Violation Detection
145	Between Batagaon to Malatipatapur	Speed Detection System	Phase 2	2	4	Speed Violation Detection

S. No	Name of the Location	Type of the Location	Phase (1/2)	Number of Roads	Number of Lanes	Proposed Solution
146	VIP Road, Infront of SP Office	Speed Detection System	Phase 2	2	4	Speed Violation Detection
Critical Locations for Surveillance						
147	Pir Jahania Beach	Surveillance Point	Phase 2	2	2	Surveillance
148	Back Side Eco Resort	Tri Junction	Phase 2	3	3	Surveillance
149	Baidas Nagar Chhaka	Tri Junction	Phase 2	3	3	Surveillance
150	Backside of Bankimuhan Neeladree Beach	Surveillance Point	Phase 2	2	2	Surveillance
151	Mangla River Bridge Near Sterling Hotel	Surveillance Point	Phase 2	2	2	Surveillance
152	IDCO Road	Tri Junction	Phase 2	3	3	Surveillance
153	Bailharchandi Temple	Surveillance Point	Phase 2	2	2	Surveillance
154	SIDI Chhak	Tri Junction	Phase 2	3	3	Surveillance
155	Gadamurgasira Bridge	Tri Junction	Phase 2	3	3	Surveillance
156	Suando Bridge	Tri Junction	Phase 2	3	3	Surveillance
157	Haripur Bridge	Surveillance Point	Phase 2	2	2	Surveillance

S. No	Name of the Location	Type of the Location	Phase (1/2)	Number of Roads	Number of Lanes	Proposed Solution
158	Kanti Bazar	Surveillance Point	Phase 2	2	2	Surveillance
159	Jankiagadasahi Chhak	Square	Phase 2	4	4	Surveillance

20.4. Format for BoQ

20.4.1. Abstract for BOQ

Price bid for RFP for Selection of Implementation Agency for Integrated City Surveillance System at Puri, Odisha for Home Department, Government of Odisha			
Name of the Bidder			
Financial Bid Sheet			
S.No.	**Sub-Head**	**Section/Discipline**	**Amount in Rs.**
CAPEX Cost			
1	Schedule A	Surveillance System	₹ 0.00
2	Schedule B	Parking Surveillance System	₹ 0.00
3	Schedule C	Automatic Number Plate Recognition System (ANPR)	₹ 0.00
4	Schedule D	Red Light Violation Detection (RLVD)	₹ 0.00
5	Schedule E	Speed Violation Detection (SVD) System	₹ 0.00
6	Schedule F	Integrated Command and Control Center (ICCC)	₹ 0.00
7	Schedule G	Variable Message Display (VMD)	₹ 0.00
8	Schedule H	Data Center	₹ 0.00
Sub Total CAPEX			**₹ 0.00**
OPEX Cost			
9	Schedule I	Network Connectivity	₹ 0.00
10	Schedule K	Manpower Costing	₹ 0.00
11	Schedule L	Capacity Building	₹ 0.00
12	Schedule M	Disaster recovery (Cloud Based Hosting)	₹ 0.00
13	Schedule N	Operations & Maintenance of IT/Non-IT Infrastructure for 5 years	₹ 0.00

Sub Total OPEX	**₹ 0.00**
Total for CAPEX and OPEX in figures	**₹ 0.00**
Total for CAPEX and OPEX in words	

Note:
- Quoted Rates shall be inclusive of all the Applicable Taxes Excluding GST.
- GST shall be paid over and above
- Nil Value Quote against any of the line items shall lead to disqualification of the bidder.

20.4.2. Detailed BOQ Sheets

20.4.2.1. Schedule A - Surveillance System

S.No.	Particular	Unit of Measurement	Qty	Rate per unit (INR)	Amount (INR)
1	IP Fixed Bullet Camera (4MP) Camera with in-built IR illuminator and associated accessories & systems including all cables/wires with SD card 128 GB and surge protector device	Number	639		-
2	Wide Angle Camera includes with SD card 128 GB and surge protector device	Number	247		-
3	IP PTZ (4 MP) Camera along with associated accessories & systems including all cables/wires with SD card 128 GB and surge protector device	Number	65		-
4	IP Fixed Box ANPR (4MP) Camera along with associated accessories & systems including all cables/wires with SD card 128 GB and surge protector device	Number	4		-
5	IR Illuminators	Number	251		-
6	Supply, Installation Testing & Commissioning of the Outdoor Utility Cabinet (Pole Mounted Junction Boxes)	Number	240		-
7	Providing & erecting 6 m high (clear height) galvanised octagonal pole with lightning	Number	162		-

S.No.	Particular	Unit of Measurement	Qty	Rate per unit (INR)	Amount (INR)
	arrester with Stickers and signages on poles.				
8	Providing & erecting 6 m high (clear height) galvanised octagonal pole with lightning arrester with Stickers and signages on poles with vertical GI cantilever arm of length 1.5 Meter	Number	400		-
9	Industrial Switch - Ports as per solution requirement	Number	240		-
10	Networking Cost (Passive Components like Patch Panel, LIU, OFC, Cat6 Cable, Power Cable, Patch Cords, Pipes, Installation & Labour Charges, etc.	Lumpsum	1		-
11	Supplying, erecting, testing and commissioning of single-phase input & 1 phase output 1KVA capacity online pure sine wave UPS along with battery (Minimum 1 hr back up time)	Number	240		-
12	Public Address System (Speaker)	Number	126		-
13	Public Address System (Amplifier)	Number	62		-
14	Dual mode Drone (Tethered and Untethered)	Number	05		-
15	Last mile Complete cabling and civil works as required including but not limited to: HDPE Pipe at road crossing, island, median etc.; DWC pipe, Armoured cables; Power cable Core, jointing, terminating, glanding, trenching, excavation, ducting, compacting, backfilling with RI	Number	240		-
16	Providing earthing as per specifications	Number	240		-
Total Quote for Schedule A - Surveillance System in Figures					**-**
Total Quote for Schedule A - Surveillance System in Words					

20.4.2.2. Schedule B - Parking Surveillance System

S.No.	Particular	Unit of Measurement	Qty	Rate per unit (INR)	Amount (INR)
1	IP Fixed Bullet Camera (4MP) Camera with in-built IR illuminator and associated accessories & systems including all cables/wires with SD card 128 GB and surge protector device	Number	26		-
2	IP PTZ (4 MP) Camera along with associated accessories & systems including all cables/wires with SD card 128 GB and surge protector device	Number	2		-
3	IP Fixed Box ANPR (4MP) Camera along with associated accessories & systems including all cables/wires with SD card 128 GB and surge protector device	Number	14		-
4	IR Illuminators	Number	14		-
5	Supply, Installation Testing & Commissioning of the Outdoor Utility Cabinet (Pole Mounted Junction Boxes)	Number	13		-
6	Providing & erecting 6 m high (clear height) galvanised octagonal pole with lightning arrester with Stickers and signages on poles with vertical GI cantilever arm of length 1.5 Meter	Number	13		-
7	Industrial Switch - Ports as per solution requirement	Number	13		-
8	Networking Cost (Passive Components like Patch Panel, LIU, OFC, Cat6 Cable, Power Cable, Patch Cords, Pipes, Installation & Labour Charges, etc.	Lumpsum	13		-

S.No.	Particular	Unit of Measurement	Qty	Rate per unit (INR)	Amount (INR)
9	Supplying, erecting, testing and commissioning of single-phase input & single-phase output 2KVA capacity online pure sine wave UPS along with battery (Minimum 1hr back up time)	Number	13		-
10	Last mile Complete cabling and civil works as required including but not limited to: HDPE Pipe at road crossing, island, median etc.; DWC pipe, Armoured cables; Power cable Core, jointing, terminating, glanding, trenching, excavation, ducting, compacting, backfilling with RI	Lumpsum	13		-
11	Providing earthing as per specifications	Number	13		-
Total Quote for Schedule B - Parking Surveillance System in Figures					**-**
Total Quote for Schedule B - Parking Surveillance System in Words					

20.4.2.3. Schedule C - Automatic Number Plate Recognition System (ANPR)

S.No.	Particular	Unit of Measurement	Qty	Rate per unit (INR)	Amount (INR)
1	IP PTZ (4 MP) Camera along with associated accessories & systems including all cables/wires with SD card 128 GB and surge protector device	Number	5		-
2	IP Fixed Box ANPR (4MP) Camera along with associated accessories & systems including all cables/wires with SD card 128 GB and surge protector device	Number	133		-
3	IR Illuminators	Number	133		-
4	IP Fixed Bullet Camera (4MP) Camera with in-built IR illuminator and associated accessories & systems including	Number	90		-

S.No.	Particular	Unit of Measurement	Qty	Rate per unit (INR)	Amount (INR)
	all cables/wires with SD card 128 GB and surge protector device				
5	Supply, Installation Testing & Commissioning of the Floor mount Outdoor Utility Cabinet / Junction Box (80:20 pole mounted: ground mounted)	Number	33		-
6	Supply, installation, testing & commissioning of 7 m high (clear height) galvanised octagonal pole along with Cantilever, circular type 7m length with Stickers and signages on poles	Number	80		-
7	Industrial Switch - Ports as per solution requirements	Number	33		-
8	Local Processing Units with ANPR at edge, including all passive components & accessories.	Number	33		-
9	Networking Cost (Passive Components like Patch Panel, LIU, OFC, Cat6 Cable, Power Cable, Patch Cords, Pipes, Installation & Labour Charges, etc.	Lumpsum	1		-
10	Supplying, erecting, testing and commissioning of single-phase input & single-phase output 2KVA capacity online pure sine wave UPS along with battery (Minimum 1hr back up time)	Number	33		-
11	Last mile Complete cabling and civil works as required including but not limited to: HDPE Pipe at road crossing, island, median etc.; DWC pipe, Armoured cables; Power cable Core, jointing, terminating, glanding, trenching, excavation, ducting, compacting, backfilling with RI	Lumpsum	80		-

S.No.	Particular	Unit of Measurement	Qty	Rate per unit (INR)	Amount (INR)
12	Providing earthing as per specifications	Number	80		-
Total Quote for Schedule - C ANPR System in Figures					**-**
Total Quote for Schedule - C ANPR System in Words					

20.4.2.4. Schedule D- Red Light Violation Detection (RLVD) System

S.No.	Particular	Unit of Measurement	Qty	Rate per unit (INR)	Amount (INR)
1	RLVD with Speed Violation detection (SVD) software & License per lane with No helmet, triple riding and wrong way & Local Processing Unit	Lanes	5		-
2	Traffic Light Aspects-RED	Number	60		-
3	Traffic Light Aspects-GREEN	Number	180		-
4	Traffic Light Aspects-AMBER	Number	60		-
5	Countdown Timer Dual Colour	Number	20		-
6	Pedestrian lamp heads-Stop Man	Number	20		-
7	Pedestrian lamp heads-Walk Man	Number	20		-
8	Supply, Installation Testing & Commissioning of the Floor mount Outdoor Utility Cabinet / Junction Box (80:20 pole mounted: ground mounted)	Number	5		-
9	Public Address System (Speaker)	Number	20		-
10	Public Address System (Amplifier)	Number	5		-
11	Public Address System (Transceiver)	Number	5		-
12	Industrial Switch - Ports as per solution requirement	Number	5		-
13	Junction Level Painting - Poles, Crossing, Stop Line etc.	Number	5		-

S.No.	Particular	Unit of Measurement	Qty	Rate per unit (INR)	Amount (INR)
14	Supplying, erecting, testing and commissioning of single-phase input & 1 phase output 2KVA capacity online pure sine wave UPS along with battery (Minimum 1 hr back up time)	Number	5		-
15	Last mile Complete cabling and civil works as required including but not limited to: HDPE Pipe at road crossing, island, median etc.; DWC pipe, Armoured cables; Power cable Core, jointing, terminating, glanding, trenching, excavation, ducting, compacting, backfilling with RI	Number	20		-
Total Quote for Schedule D- RLVD System in Figures					**-**
Total Quote for Schedule D- RLVD System in Words					

20.4.2.5. Schedule - E Speed Violation Detection (SVD) System

S.No.	Particular	Unit of Measurement	Qty	Rate per unit (INR)	Amount (INR)
1	Speed Violation Detection Cameras along with associated accessories & systems including all cables/wires with SD card 128 GB and surge protector device	Number	8		-
2	IP Fixed Box ANPR (4MP) Camera along with associated accessories & systems including all cables/wires with SD card 128 GB and surge protector device	Number	16		-
3	IR Illuminators	Number	24		-
4	IP Fixed Bullet Camera (4MP) Camera with in-built IR illuminator and associated accessories & systems including all cables/wires with	Number	8		-

S.No.	Particular	Unit of Measurement	Qty	Rate per unit (INR)	Amount (INR)
	SD card 128 GB and surge protector device				
5	Supply, Installation Testing & Commissioning of the Floor mount Outdoor Utility Cabinet / Junction Box (80:20 pole mounted: ground mounted)	Number	4		-
6	Supply, installation, testing & commissioning of 7 m high (clear height) galvanised octagonal pole along with Cantilever, circular type 7m length with Stickers and signage on poles	Number	8		-
7	Industrial Switch - Ports as per solution requirement	Number	4		-
8	Local Processing Unit	Number	4		-
9	Networking Cost (Passive Components like Patch Panel, LIU, OFC, Cat6 Cable, Power Cable, Patch Cords, Pipes, Installation & Labour Charges, etc.	Lumpsum	1		-
10	Supplying, erecting, testing and commissioning of single-phase input & single-phase output 2KVA capacity online pure sine wave UPS along with battery (Minimum 1hr back up time)	Number	4		-
11	Last mile Complete cabling and civil works as required including but not limited to: HDPE Pipe at road crossing, island, median etc.; DWC pipe, Armoured cables; Power cable Core, jointing, terminating, glanding, trenching, excavation, ducting, compacting, backfilling with RI	Lumpsum	8		-
12	Providing earthing as per specifications	Number	8		-
13	220/240 VAC Power Surge Protector	Number	378		

S.No.	Particular	Unit of Measurement	Qty	Rate per unit (INR)	Amount (INR)
14	3c x 10 Sqmm Power Armoured Au. cable	Nos	36100		
15	3c x 2.5 Sqmm Power Armoured Au. cable	Rate in Meter	31330		
16	2c x 1.5 Sqmm Power Armoured Au. cable	Rate in Meter	8820		
17	Fibre Optics Cable 12 core for last mile connectivity	Rate in Meter	54150		
18	UTP Cat -6 Armoured Cable	Rate in Meter	91000		
19	HDPE duct 50 mm	Rate in Meter	90250		
20	HDD Trenching	Rate in Meter	90250		
21	Electric meter connections for Field locations	Rate in Meter	362		
Total Quote for Schedule E - SVD System in Figures					-
Total Quote for Schedule E - SVD System in Words					

20.4.2.6. Schedule F- Integrated Command and Control Center (ICCC)

S.No.	Particular	Unit of Measurement	Qty	Rate per unit (INR)	Amount (INR)
1	LCD video wall, 55-inch direct-lit LCD panels, 4x2 matrix, 24×7 rated, narrow-bezel, with mounting structures, wall controller/processor, signal transport, all cabling/terminations, calibration, integration, testing & commissioning including Video wall controller with wall management software	Number	1		-
2	Audio Mixer and speaker system	Number	1		-
3	Operator Workstations (City Management Room)- 3Monitors	Number	4		-
4	IP Phones	Number	4		-
5	Multi-Function Laser Printer (City Operations Room)	Number	1		-
6	65"/70" LED display to present critical information Display	Number	1		-
7	IBMS	Number	1		-

S.No.	Particular	Unit of Measurement	Qty	Rate per unit (INR)	Amount (INR)
8	Air Conditioner 2 Ton Split Type (5 Star Rating)	Number	14		-
9	Air Conditioner 1.5 Ton Split Type	Number	4		-
10	UPS with Battery backup of 1 hour	Number	2		-
11	Access Control System	Number	1		-
12	Electrical and power cabling	Lot	1		-
13	Electrical Cabling & Necessary Illumination Devices	Lot	1		-
14	LAN and CAT-6 cabling	Lot	1		-
15	PAS in house mic along with associated accessories & systems including all cables/wires required for end-to-end installation	Number	1		-
16	Fire & Smoke Detection System	Lot	1		-
17	Fixed Dome Cameras	Number	12		-
18	Operator Table for workstations for ICCC	Number	4		-
19	Operator Table for workstations for Call Center	Number	8		-
20	Operator Table for workstations for Helpdesk	Number	6		-
21	Ergonomic Chairs (for operators, meeting rooms, office staff etc.)	Number	62		-
22	Revolving Chair	Number	5		-
23	Sofa Set 5-Seater with Glass Table	Number	1		-
24	Meeting Table for Situation Room	Number	1		-
25	Executive Table for Officer Room	Number	2		-
26	Furniture for Reception & Waiting Area	Number	1		-
27	DG Set (IT Load Only)	Number	1		-
28	IP PBX System	Number	1		-
29	ISDN PRI Licenses	Number	2		-
30	Contact Center Agent License	Number	1		-
31	Contact Center Supervisor License	Number	1		-
32	Headsets	Number	8		-

S.No.	Particular	Unit of Measurement	Qty	Rate per unit (INR)	Amount (INR)
33	Civil Work (Raised Floor, False Ceiling, Ducting, Access Doors, Painting, Partitioning etc.) total 4200 Sq. Feet as per the proposed layout	Lot	1		-
Total Quote for Schedule F: ICCC in Figures					**-**
Total Quote for Schedule F: ICCC in Words					

20.4.2.7. Schedule G - Variable Message Display (VMD)

S.No.	Particular	Unit of Measurement	Qty	Rate per unit (INR)	Amount (INR)
1	Supply, installation, commissioning of VMD board including VMD controller as per specifications	Number	7		-
2	Mounting structure for VMD as per site requirements and IRC guideline	Number	7		-
3	Supplying, erecting, testing and commissioning of single-phase input & single-phase output 3KVA capacity online pure sine wave UPS along with battery (Minimum 1hr back up time)	Number	7		
4	Supply, Installation Testing & Commissioning of the Floor mount Outdoor Utility Cabinet / Junction Box with chemical earthing	Number	7		
Total Quote for Schedule G - VMD in Figures					**-**
Total Quote for Schedule G - VMD in Words					

20.4.2.8. Schedule H - Data Center

S.No.	Particular	Unit of Measurement	Qty	Rate per unit (INR)	Amount (INR)
Servers with required Operating System (OS), Databases (DB) & Virtualization Software Licenses as per the proposed Solution					

S.No.	Particular	Unit of Measurement	Qty	Rate per unit (INR)	Amount (INR)
1	Server for ICCC Application, Public Address System, VMS & Recording, ANPR , Speed Violation Detection, Redlight Violations Detection, E-challan, EMS Server, Database Server, Variable Message Display application, IBMS software, any other server as per solution requirement. HA applicable for critical applications (VMS & ICCC)	Number	8		-
2	Video analytics server with GPUs	Number	6		
Sub Total					**-**
Software Components for Data Centre					
1	ICCC Application in N+1 (HA) and integration with VMS, VA, PAS, VMD and existing GIS engine/maps and 5 user client licenses	Number	1		-
2	Public Address System (PAS) Application	Number	1		-
3	Video Management System (VMS) (Software +Licenses) in N+1 (HA) with 10 client user licenses	Number	1476		-
4	Enterprise Management System for SLA Management	Number	1		-
5	Anti-virus Software	Number	100		-
6	ANPR (Software + Licence)	Number	1		-
7	RLVD (Software + License)	Number	1		-
8	Speed Violation Detection	Number	1		-
9	IBMS software	Number	1		-
10	Variable Message Display Software	Number	7		-
11	Video analytics for Yatra Route and City - parking	License per use case	400		-

S.No.	Particular	Unit of Measurement	Qty	Rate per unit (INR)	Amount (INR)
	violation (50) and parking management (full/empty data), Crowd detection & estimation (300), movement analysis, Fallen person detection(50), maximum 2 use case per camera				
12	Video analytics for Temple area - Entry/exit, Queue management (20), Crowd detection and estimation(50), fallen person detection(5), Fire (10), Object left detection(10), entry/exit - Face recognition (20) maximum 2 use case per camera	License per use case	115		-
13	Video Summarization Software with GPU capability for 25 camera licenses	Set	1		-
14	Social Media Monitoring System	Number	1		
15	Contact Center Application /CRM	Number	4		
16	Mobile Applications	Lumpsum	1		
17	Operating System (OS), Databases (DB), Virtualization Software Licenses as per the proposed Solution and any other as per the proposed solution				
Sub Total					-
Integration with ICCC					
1	Integration of PAS	Number	1		-
2	Integration of Surveillance	Number	1		-
3	Integration of ANPR	Number	1		-
4	Integration of Video Summarization Software	Number	1		-

S.No.	Particular	Unit of Measurement	Qty	Rate per unit (INR)	Amount (INR)
5	Integration of RLVD	Number	1		-
6	Integration SVD	Number	1		-
7	Integration with Variable Message Display	Number	1		-
8	Integration of Body Worn Camera	Number	1		-
9	Integration with Drone	Number	1		-
Sub Total					**-**
Storage					
1	Storage (in TB)	1	2000 TB		-
2	Back UP Solution with Software	1	Lumpsum		-
Sub Total					**-**
Network & Security					
2	L3 Core Switch	Number	2		-
3	L2 Switch	Number	4		-
5	SAN Switch	Number	2		-
Sub Total					**-**
Non-IT					
1	Racks 42U	Number	5		-
2	Precision AC for data center	Number	9		-
3	DG Set (IT Load Only) with 100 capacity KVA	Number	2		-
4	UPS 100KVA with 30 mins backup with failover	Number	2		-
5	DC Build as per specification including Fire Detection and Suppression System ,Precision Air Conditioning, Access Control System etc.	Lumpsum	1		-
Sub Total					**-**

S.No.	Particular	Unit of Measurement	Qty	Rate per unit (INR)	Amount (INR)
Cyber Security Components					
1	Firewall in HA	Set	1		-
2	Web Access Firewall in HA	Set	1		
Sub Total					-
Total Quote for Schedule H - Data Center in Figures					-
Total Quote for Schedule H - Data Center in Words					

20.4.2.9. Schedule I - Network Connectivity

S.No.	Particular	Unit of Measurement	Qty	Rate per unit (INR)	Amount (INR)
1	One time cost for Point to Point connectivity from Surveillance Fixed Cameras, PTZ, VMD & PAS to Data Center, min 25 Mbps per location (Bidder may consider additional if required as per their design)	Locations	240		-
2	One time cost for Point to Point connectivity from ANPR System to Data Center, min 20 Mbps per location (Bidder may consider additional if required as per their design)	Locations	33		-
3	One time cost for Point to Point connectivity from RLVD System to Data Center, min 20 Mbps per location (Bidder may consider additional if required as per their design)	Locations	5		-
4	One time cost for Point to Point connectivity from Speed Violation Detection system to Data Center, min 20 Mbps per location (Bidder may consider additional if required as per their design)	Locations	4		-
5	One time cost for min. 5 Gbps redundant link connectivity for Aggregation Bandwidth at Data	Lumpsum	1		-

S.No.	Particular	Unit of Measurement	Qty	Rate per unit (INR)	Amount (INR)
	Center/ICCC. (Bidder may consider additional if required as per their design)				
6	One time cost for Min. 1 Gbps bandwidth for DR Connectivity (Bidder may consider additional if required as per their design)	Lumpsum	1		-
7	One time cost for Bandwidth for DC- DR Connectivity (Bidder may consider additional if required as per their design)	Lumpsum	1		-
8	Recurring expenses for 5 years for Point to Point connectivity from Surveillance Fixed Cameras, PTZ, VMD & PAS to Data Center, min 25 Mbps per location (Bidder may consider additional if required as per their design)	Locations	240		
9	Recurring expenses for 5 years for Point to Point connectivity from ANPR System to Data Center, min 20 Mbps per location (Bidder may consider additional if required as per their design)	Locations	33		
10	Recurring expenses for 5 years for Point to Point connectivity from RLVD System to Data Center, min 20 Mbps per location (Bidder may consider additional if required as per their design)	Locations	5		
11	Recurring expenses for 5 years for Point to Point connectivity from Speed Violation Detection system to Data Center, min 20 Mbps per location (Bidder may consider additional if required as per their design)	Locations	4		
12	Recurring expenses for 5 years for min. 5 Gbps redundant link connectivity for Aggregation Bandwidth at Data Center/ICCC.	Lumpsum	1		

S.No.	Particular	Unit of Measurement	Qty	Rate per unit (INR)	Amount (INR)
	(Bidder may consider additional if required as per their design)				
13	Recurring expenses for 5 years for Min. 1 Gbps bandwidth for DR Connectivity (Bidder may consider additional if required as per their design)	Lumpsum	1		
14	Recurring expenses for 5 years for Bandwidth for DC- DR Connectivity (Bidder may consider additional if required as per their design)	Lumpsum	1		
Total Quote for Schedule I - Network Connectivity in Figures					-
Total Quote for Schedule I - Network Connectivity in Words					

20.4.2.10. Schedule K - Manpower Costing

S.No.	Particular	Qty	Unit of Measurement	Total Required Man month	Rate per Month per Resource (INR)	Total Cost for manpower for entire project duration (INR)
1	Project Manager	1	Manmonth	60		-
2	Solution Architect	1	Manmonth	12		-
3	Security Infrastructure Specialist	1	Manmonth	60		-
4	Technical Expert – GIS	1	Manmonth	6		-
5	Data Management Expert/Analyst	1	Manmonth	12		-
6	Business Analyst / Use-case/SoP expert	1	Manmonth	12		-
7	Network Architect	1	Manmonth	12		-

S.No.	Particular	Qty	Unit of Measurement	Total Required Man month	Rate per Month per Resource (INR)	Total Cost for manpower for entire project duration (INR)
8	Server Storage/Database Expert	1	Manmonth	12		-
9	Operators	15	Manmonth	60		-
10	Security Guard	6	Manmonth	60		-
Total Quote for Schedule K - Manpower Costing in Figures						**-**
Total Quote for Schedule K - Manpower Costing in Words						

20.4.2.11. Schedule L - Capacity Building

S.No.	Particular	Unit of Measurement	Qty	Rate per unit (INR)	Amount (INR)
1	Functional Training	Number	4		-
2	Administrative Training	Number	2		-
Total Quote for Schedule L - Capacity Building in Figures					**-**
Total Quote for Schedule L - Capacity Building in Words					

20.4.2.12. Schedule M - Disaster Recovery (Cloud Based Hosting)

S.No.	Particular	Unit of Measurement	Qty	Cost for Year 1	Cost for Year 2	Cost for Year 3	Cost for Year 4	Cost for Year 5	Total Cost
1	DR (Cloud Based Hosting)	Yearly	5						-
Total Quote for Schedule M - Disaster Recovery in Figures									**-**

S.No.	Particular	Unit of Measurement	Qty	Cost for Year 1	Cost for Year 2	Cost for Year 3	Cost for Year 4	Cost for Year 5	Total Cost
Total Quote for Schedule M - Disaster Recovery in Words									

20.4.2.13. Schedule N - Operations & Maintenance of IT / Non-IT Infrastructure

S.No.	Particular	Unit of Measurement	Qty	Cost for Year 1	Cost for Year 2	Cost for Year 3	Cost for Year 4	Cost for Year 5	Total Cost
1	Comprehensive Operations & Maintenance of IT / Non-IT Infrastructure for 5 years	Yearly	5						-
Total Quote for Schedule N - O&M of IT / Non-IT Infra in Figures									**-**
Total Quote for Schedule N - O&M of IT / Non-IT Infra in Words									

*The quantity mentioned above are only indicative and the bidder may propose additional item to meet the solution requirements.

* The qty. of Server mentioned as 14 nos. is minimum, however the bidder may provision actual numbers considering the virtualisation and other requirement.

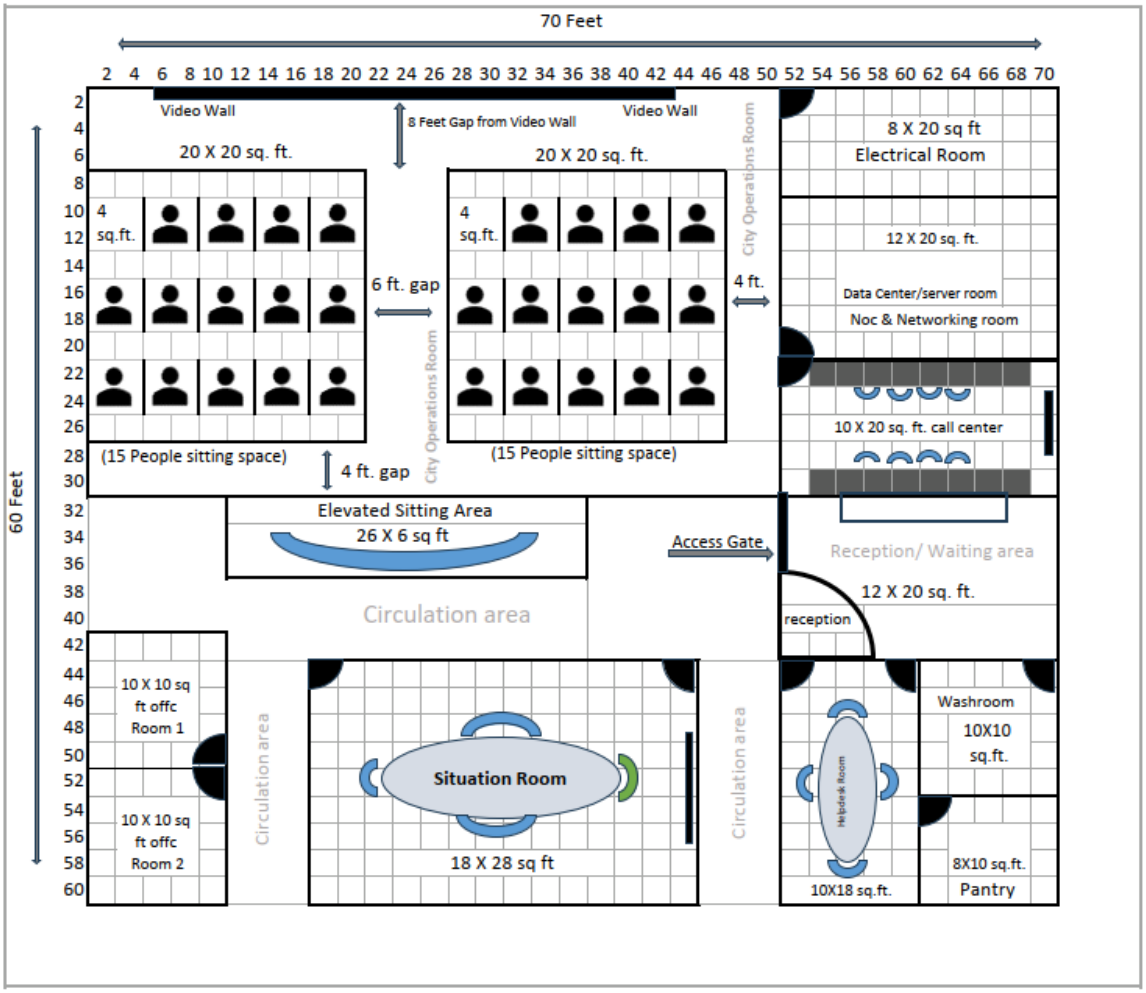
20.5. Proposed Layout for ICCC

Proposed ICCC layout Plan at JBPC Parking area, third floor (Entertainment Zone)

Area of 4200 Sq. Ft. identified for ICCC in Third floor (Entertainment Zone) at JBPC Parking

Sr. No.	Room/ Function	Approx. Area (sq. ft)
1	City Operations Room (Main Video Wall + Operators)	1500
2	Circulation Area + Elevated Sitting area	796
3	Contact Centre Room (Call center bays)	200
4	Server / Data Center Room (Racks, storage, security) and NOC / Network Room (IT, monitoring, racks consoles)	240
5	Officer Room (Room 1 + Room 2)	200
6	War Room / Situation Room (Strategy + small VC)	504
7	Technical Support / Helpdesk Room	180
8	Utility / Electrical & UPS Room	160
9	Reception / Access Control / Waiting	240

Sr. No.	Room/ Function	Approx. Area (sq. ft)
10	Pantry	80
11	Washroom (Male + Female)	100
	Total	**4200**



Tentative Floor Plan for Proposed ICCC which is planned at JBPC Parking (Approximate measurements mentioned). Third Floor (currently marked as Entertainment zone).

Odisha Computer Application Centre

RFP for Selection of Implementation Agency for Integrated City Surveillance System at Puri, Odisha for Home Department, Government of Odisha

RFP Reference No.: **OCAC-SEGP-INFRA-0023-2025-26009**
Date: 31/01/2026

PART-2

ODISHA COMPUTER APPLICATION CENTER
[Technical Directorate of E & IT Department, Government of Odisha]
N-1/7-D, Acharya Vihar, P.O. – RRL, Bhubaneshwar-751013
EPBX: 674-2567280/2567064/2567295/2567283
Fax: +91-674-2567842
E-mail ID- contact@ocac.in, Website: www.ocac.in

Table of Contents

Disclaimer

The information contained in this Request for Proposal document ("**RFP**") whether subsequently provided to the Bidders, ("**Bidder/s**") verbally or in documentary form by Odisha Computer Application Center (henceforth referred to as "**OCAC**" in this document) or any of its employees or advisors, is provided to Bidders on the terms and conditions set out in this Tender document and any other terms and conditions subject to which such information is provided.
This RFP is not an agreement and is not an offer or invitation to any party. The purpose of this RFP is to provide the Bidders or any other person with information to assist the formulation of their financial offers ("**Bid**"). This RFP includes statements, which reflect various assumptions and assessments arrived at by Authority in relation to this scope. This Tender document does not purport to contain all the information each Bidder may require. The assumptions, assessments, statements and information contained in the Bid documents, may not be complete, accurate, adequate or correct. Each Bidder must therefore conduct its own analysis of the information contained in this RFP and to seek its own professional advice from appropriate sources.

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

Authority and their employees and advisors make no representation or warranty and shall incur no liability to any person, including the Bidder under law, statute, rules or regulations or tort, the principles of restitution or unjust enrichment or otherwise for any loss, cost, expense or damage which may arise from or be incurred or suffered on account of anything contained in this RFP or otherwise, including the accuracy, reliability or completeness of the RFP, and any assessment, assumption, statement or information contained therein or deemed to form part of this RFP or arising in any way in this Selection Process. Authority also accepts no liability of any nature whether resulting from negligence or otherwise howsoever caused arising from reliance of any Bidder upon the statements contained in this RFP. Authority may in its absolute discretion, but without being under any obligation to do so, can amend or supplement the information in this RFP.

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

The Bidder shall bear all its costs associated with or relating to the preparation and submission of its Bid including but not limited to preparation, copying, postage, delivery fees, expenses associated with any Proof of Concept (PoC), demonstrations or presentations which may be required by Authority, or any other costs incurred in connection with or relating to its Bid. All such costs and expenses will remain with the Bidder and authority shall not be liable in any manner whatsoever for the same or for any other costs or other expenses incurred by a Bidder in preparation for submission of the Bid, regardless of the conduct or outcome of the Selection process.

Preamble

This RFP document (Volume -III) comprises of the following three parts:

1. **Part A: General Conditions of the Agreement**
2. **Part B: Special Conditions of the Agreement**
3. **Part C: Service Levels**

Part A: General Conditions of the Agreement
This part comprises of the general conditions which will govern the Agreement to be executed between the IA and the Odisha Computer Application Center (OCAC)

Part B: Special Conditions of the Agreement
This part comprises of the special conditions which will govern the Agreement to be executed between the IA and the Odisha Computer Application Center (OCAC)

Part C: Service Levels
This part comprises of the general procedures with respect to the service level agreements, reporting, issue management, service level change control etc.

1. PART A – General Conditions of Agreement

1.1 Definition of Terms

In this RFP, the following words and expressions shall, unless repugnant to the context or meaning thereof, have the meanings hereinafter respectively assigned to them:

1.1.1. **"Acceptance of System"** means the System, including the hardware, software, solution or any Deliverable accepted or deemed to have been accepted by the Authority, subsequent to its installation, rollout and deployment of trained manpower, when all the activities as defined in Scope of Work have been successfully executed and completed to the satisfaction of the Authority and the Authority has given its acceptance by signing the Acceptance Certificate.

1.1.2. **"Acceptance Certificate"** refers to that document/certificate issued by the Authority signifying acceptance of a hardware, software, solution, or any other Deliverable pursuant to the successful completion of the Acceptance Test of the System.

1.1.3. **"Acceptance Test"** or **"User Acceptance Test"** means the test, standard procedure, trial runs to be conducted by the IA as per this RFP or as per the Agreement in relation to the Works.

1.1.4. **"Affiliate(s)"** means, with respect to any Person, any other Person, directly or indirectly controlled by, controlling or under common control with such Person. For purposes of this Agreement, the term "control" means the power to direct the management and policies of a Person, whether through the ownership of voting securities, by agreement or otherwise. An Affiliate shall remain an Affiliate only as long as such control exists.

1.1.5. **"Agreement"** means this Master Service Agreement including the Annexures hereto and any amendments thereto made in accordance with the provisions contained in this Agreement and includes inter alia(a) the complete RFP documents being Volumes I, II and III of the RFP and Corrigendum and addendum, (b) IA offer, (c) letter of acceptance or letter of award or letter of intent issued by the Authority, (d) the acceptance of letter of award from IA, (e) notice to proceed with the Work, and (f) any other document listed in the Agreement data.

1.1.6. **Agreement Value"** means the amount quoted by the IA in its commercial Bid and which has been duly accepted by Odisha Computer Application Center for the full and proper performance of its obligations under the Agreement.

1.1.7. **"Applicable Law(s)"** means all laws in force and effect as of the date hereof and/or laws which may be promulgated or brought into force and effect after the date of execution of the Agreement and includes any statute, law, ordinance, notification, rule, regulation, judgment, order, decree, injunctions, by-laws, approval, directive, guideline, policy, requirement or other governmental restriction or any similar form of decision applicable to the relevant Party and all judgments, decrees, injunctions, and orders of any court, tribunal or any quasi-judicial authority, as may be in force and effect during the subsistence of the Project.

1.1.8. **"Applicable Permits" / "Approvals"** means all clearances, licenses, permits, authorizations, no objection certificates, consents, approvals and exemptions under or pursuant to any of the Applicable Laws or from any Government Agency or third party, required to be obtained and/or maintained by the IA or it's Sub Contractor(s)in order to implement the Project and for undertaking, performing or discharging the obligations contemplated under the Agreement, including but not limited to clearances required for importing equipment, exemption of tax/duties/levies/work permits/clearances for IA / IA's Team.

1.1.9. **"Appointed Date"** shall mean the date so specified in the by the Authority or an earlier or later date that Authority and the IA's may by mutual consent determine, prior to which all the Conditions Precedent specified in the Agreement for the full effectiveness of the provisions of the Agreement shall have to be met by Authority and the IA's.

1.1.10. **"Approved Plan"** shall mean the approval given by the Authority to the plan submitted by the IA for executing the Works under the Agreement.

1.1.11. **"Authority"/ "OCAC"** means the Odisha Computer Application Center (OCAC). The Project shall be executed in Puri and shall be owned by Odisha Computer Application Center (OCAC).

1.1.12. **"Bank Guarantee"** means an irrevocable and unconditional bank guarantee payable on demand and issued by a bank in favour of the Authority and furnished by the IA or its Sub Contractor(s) to Authority for guaranteeing the due performance of its obligations under the Agreement.

1.1.13. **"Bid"** means the documents in their entirety comprised in the bid submitted by the Bidder in response to this RFP No. **OCAC-SEGP-INFRA-0023-2025-26009,** dated 29.01.2026

1.1.14. **"Bidder"** shall mean Person, or organization submitting the proposal in response to this RFP.

1.1.15. **"Business Day"** means the working day in the city of Puri.

1.1.16. **"Change Control Note"** shall have the meaning as set forth under Article 2.14 and in the format specified under Annexure I of this RFP.

1.1.17. **"Commercial Off-The-Shelf (COTS)"** refers to software products that are ready-made and available for sale, lease, or license to the public.

1.1.18. **"Completion Date"** shall mean the date on which the Completion Clearance is issued by the Authority to the IA, upon the completion of the Project.

1.1.19. **"Conditions Precedent"** shall have the meaning set forth in Article 1.3 of this RFP.

1.1.20. **"Confidential Information"** means all information including any information (whether in written, oral, electronic or other format) which relates to the technical, financial and business affairs, dealers, suppliers, products, developments, operations, processes, data, trade secrets, design rights, know-how, plans, budgets and information and data which is proprietary to Authority and which is disclosed to or otherwise learned

by IA in the course of or in connection with the Agreement but does not include information (i) which is available lawfully in the public domain; (ii) publicly known through no fault of the IA; (iii) already known to the IA from someone other than the Authority who is not bound by confidentiality restrictions; or (iv) independently developed by the IA without access to or use of the Confidential Information disclosed.

1.1.21. **"Cure Period"** shall mean a period of 7 (seven) days, or such greater period as may be specified in the Notice of Intention to Terminate.

1.1.22. **"Data Centre"/ "DC"/ "Data Centre Site"/ "DC Site"/ "Server Room"** means the data centre sites including their respective data centre space, wherein the delivery, installation, integration, management and maintenance services as specified under the Scope of Work are to be carried out for the purpose of this Agreement. The DC Shall be hosted on cloud server.

1.1.23. **"Deliverable(s)"** shall mean all of the equipment, sub-systems, hardware, software, products accessories, software, source code, documentation, reports and/or other material/items which IA is required to supply, install and maintain under the scope of the Agreement.

1.1.24. **"Developed Materials"** shall have the meaning ascribed to it in Article 1.26.3. of Volume III of the RFP.

1.1.25. **"Document"** means any embodiment of any text or image however recorded and includes any data, text, images, sound, voice, codes, databases or any other electronic documents / records as contemplated as per Information Technology Act 2000 and the rules framed under the said Act.

1.1.26. **"Effective Date"** means the date on which the Agreement is signed, or letter of intent is issued by Authority, whichever is earlier and executed by the Parties hereto. If the Agreement is executed in parts, then the date on which the last of such Agreements is executed shall be construed to be the Effective Date.

1.1.27. **"Fixes"** means product fixes that are either released generally (such as commercial product service packs) or that are provided to IA or their Subcontractor when performing services (such as workarounds, patches, bug fixes, beta fixes and beta builds) and any derivatives of the foregoing.

1.1.28. **"Force Majeure"** or **"Force Majeure Event"** shall have the meaning set forth in as per Article 1.38.

1.1.29. **"Goods"** means all of the equipment, sub-systems, hardware, software, products, accessories, components, software and/or other material/items and includes their user manuals, technical manuals, operating manuals, service mechanisms, policies and guidelines (such as security related, data migration related) and all its modifications which IA is required to supply, install and maintain under the Agreement.

1.1.30. **"Good Industry Practice"** means the practices, methods, techniques, designs, standards, skills, diligence, procedure, efficiency, reliability and prudence which would reasonably and ordinarily be expected from a skilled and experienced contractor engaged

in activities of a similar scope and complexity to those that are the subject of the Agreement and as envisaged under this RFP and under the same or similar circumstances, where such contractor is seeking to comply with its contractual obligations and all Applicable Laws and regulatory requirements. It would include good engineering practices in the design, engineering, construction and project management and acting generally in accordance with the provisions of this RFP and would include which would be expected to result in the performance of its obligations by the IA in accordance with the Agreement, this RFP, Applicable Laws and Applicable Permits in reliable, safe, environment protected, economical and efficient manner.

1.1.31. **"Go- Live"** means installation, testing, commissioning of Project, including training as per Scope of Work mentioned in the Agreement or this RFP. IA should have the approval from Authority for carrying out User Acceptance Test.

1.1.32. **"Government Instrumentality" / "Government Agency"/ "Government Authority"** means any department, division or sub-division of the Government of India or the Government of Odisha or any other State Government, including but not limited to the OCAC, Authority, as may be applicable, including any commission, board, body, bureau, authority, agency, instrumentality, court or other judicial or quasi-judicial or administrative body, at central, state or local level, or municipal and other local authority or statutory body including Panchayat under the control of the Government of India or the Government of Odisha, as the case may be, and having jurisdiction over the IA, IA's Sub Contract or the Project or any portion thereof or the performance of all or any of the Services or obligations of the IA or IA's Sub Contractor under or pursuant to this RFP or under the Agreement;

1.1.33. **"Intellectual Property Rights"** means all rights pertaining to patent, trademarks, copyrights, trade secrets, service marks, logos, brands, trade names, internet domain names, formulae, designs, software (whether in object code or source code), know-how, processes, techniques, methods, technical data, databases, proprietary information, utility models, rights in know- how and other intellectual property rights, whether existing as of the Effective Date or arising thereafter, and all of the goodwill associated with the use of, and symbolized by, any of the foregoing, all rights of indemnification with respect to any of the foregoing, the right to prosecute and sue for past, present and future infringements, dilutions, violations or misappropriations with respect to any of the foregoing, all rights corresponding to any of the foregoing throughout the world, and all proceeds of any the foregoing, including licenses, royalties and proceeds of suit, and any right to any of the foregoing granted under any License.

1.1.34. **"Key Personnel"** means employees of IA whether employed directly on rolls of IA or engaged indirectly, providing services to IA through a contract or/and the key personnel of IA as referred in Section 3.6.3 of the RFP Volume I proposed.

1.1.35. **"Material Adverse Effect"** shall mean circumstances which may or do (i) render any right vested in a Party by the terms of the Agreement ineffective, or (ii) adversely affects or restricts or frustrates the ability of any Party to observe and perform in a timely

manner its obligations under this Agreement or the legality, validity, binding nature or enforceability of the same.

1.1.36. **"Milestone"** or **"Project Timeline(s)"** means the stipulated period fixed under the Agreement or under the RFP for completion of Works or part of the Works by the IA.

1.1.37. **"IA"** shall mean the successful bidder (Person and/or Organization) who is selected by the Authority at the end of the RFP process for execution of the Project and shall be deemed to include the IA's successors, agent(s), agency, representatives (approved by Authority), heirs, Affiliates, executors, administrators and permitted assigns, as the case may be, unless excluded by the terms of the Agreement.

1.1.38. **"IA's Team"** means the team established / formed by IA for executing the Works under the present RFP and the Agreement and shall include any and/or all the employees of IA, agent(s), agency, authorized service providers/partners and representatives or other Personnel employed or engaged either directly or indirectly by IA for the purposes of the Agreement.

1.1.39. **"Notice"** means a written notice, consent, approval or other communication required to be sent to the parties under the Agreement.

1.1.40. **"Notice of Intention to Terminate"** shall mean the notice issued by a Party to the other Party expressing its intention to terminate the Agreement.

1.1.41. **"OEM"** means the original equipment manufacturer of any equipment / system / software / product who is/are providing such Goods to the Authority under the scope of this RFP or the Agreement.

1.1.42. **"O & M"** shall mean Operations and Maintenance services for the software, hardware and other IT and Non-IT infrastructure installed as part of the project after Go-Live and for a period of 5 -months from the date of Go-Live.

1.1.43. **"Person"** includes any individual, company, corporation, partnership, joint venture, trust, unincorporated organization, government or Governmental Authority or Government Agency or any other legal entity.

1.1.44. **"Performance Bank Guarantee"/ "PBG"** means performance bank guarantee as defined under Annexure 5 of the RFP Volume I.

1.1.45. **"Project"** means the project for integrated city surveillance system for Puri, Odisha by the IA in pursuance of the terms and conditions of this RFP/Agreement.

1.1.46. **"Project Location(s)"** shall mean the location(s) / site(s) where the Works are to be executed by the IA.

1.1.47. **"Project Manager" / "Authority's Representative"** shall mean the person appointed by the Authority for supervising and managing the affairs in relation to the Project.

1.1.48. **"Project Office"** means the site office to be set up by the IA for the execution of the Project. The Project office shall be set up by the IA at a location to be suggested by the Authority.

1.1.49. **"Project Report(s)"** shall mean the report(s) or the updates to be submitted by the IA in relation to the Works at regular intervals.

1.1.50. **"Project Team"** means the IA's Key Personnel, team members or any other person duly authorized by the Authority for the execution of the Works and the Project.

1.1.51. **"Project Plan"** or **"Plan"** or **"Revised Plan"** or **"Work Plan"** or **"Program of Work(s)"** means the plan / schedule, methodology, design documents, specifications, or any other document submitted by the IA to the Authority for executing the Works under the Agreement or for the fulfilment of its various obligations under the Agreement.

1.1.52. **"Replacement Service Provider"** means the organization or agency replacing IA or its Sub-Contractor in case of termination of the Agreement for any reasons whatsoever.

1.1.53. **"RFP"** means this Request for Proposal for the selection of IA for implementation of the Project.

1.1.54. **"Scope of Work"** shall have the meaning as set forth in Article 1.4 of this RFP.

1.1.55. **"Service Levels"** shall mean the level of service to be provided / rendered by IA for executing / completing the Works and for meeting its various obligations under the Agreement and shall include the meaning set forth in Part C of this RFP.

1.1.56. **"Service(s)"** or **"Activity"** or **"Activities"** shall mean the Works / Services to be carried out or rendered by the IA and or its Sub Contractor pursuant to this RFP and the Agreement or any other specific assignment awarded by the Authority to IA.

1.1.57. **"Service Specifications"** shall mean the specifications as set out in PART C-SERVICE LEVELS of this RFP.

1.1.58. **"Steering Committee"** or **"High Powered Committee"** or **"Project Information Committee"** shall mean a committee formed to supervise / monitor the work of the Project Management Committee and also the Project Manager. It shall consist of a _ number of members as decided by the Authority and shall act as the appellate body over the decision rendered by the Project Management Committee.

1.1.59. **"Site"** means the lands and other places on, under, in or through which the permanent works are to be carried out and any other lands or places provided by the Authority for the purpose of the Agreement.

1.1.60. **"Sub-Contractor"** shall mean the entity or agency working on behalf of IA and who is named in the Agreement for any part of the Scope of Work or any Person to whom any part of the Agreement has been sublet with the consent in writing by the Authority and shall include the heirs, legal representatives, successors and assignees of such Person.

1.1.61. **"Termination Notice"** shall mean the notice issued by either Party to the other Party in accordance with the provisions of the Agreement terminating the Agreement

1.1.62. **"Work(s)"** or **"Program of Work(s)"** means the entire work or a part of it to be undertaken by IA for Implementation of Surveillance & Crowd Management System on Rental basis for Ratha Yatra 2026 in Authority as envisaged in the present RFP and the

Agreement together with all Annexures, Schedules, referenced documents and all amendments, corrigendum, addendums and changes thereto.

1.2 Interpretation

In this RFP unless a contrary intention is evident:

1.2.1. "Party" shall mean IA or Authority individually and "Parties" shall mean IA and Authority collectively.

1.2.2. the clause headings are for convenient reference only and do not form part of the Agreement.

1.2.3. unless otherwise specified a reference to a clause number is a reference to all of its sub-clauses.

1.2.4. the word "includes" or "including" shall be deemed to be followed by "without limitation" or "but not limited to" whether they are followed by such phrases.

1.2.5. unless otherwise specified a reference to a clause, sub-clause or section is a reference to a clause, sub-clause or section of the Agreement including any amendments or modifications to the same from time to time.

1.2.6. a word in the singular includes the plural and a word in the plural includes the singular.

1.2.7. a word importing a gender includes any other gender.

1.2.8. a reference to a person includes a partnership and a corporate body.

1.2.9. a reference to legislation includes legislation repealing, replacing or amending that legislation.

1.2.10. Where a word or phrase is given a particular meaning, it includes the appropriate grammatical forms of that word or phrase which have corresponding meanings.

1.2.11. In the event of an inconsistency between the terms of the Agreement and the RFP and the Bid, the terms of the RFP shall prevail.

1.2.12. In case there is a contradiction between the clauses mentioned in the RFP, the below hierarchy of clauses in order of precedence shall be applicable:

- Pre-bid clarification and Corrigendum, if any
- RFP Volume III
- RFP Volume II
- RFP volume I

1.3 Conditions Precedent

1.3.1. Save and except as expressly provided, the respective rights and obligations of the Parties under the Agreement shall be subject to the satisfaction in full of the condition's precedent specified in this Article 1.3.

1.3.2. Conditions Precedent required to be satisfied by Authority prior to the Appointed Date shall be deemed to have been fulfilled when Authority shall have granted to the IA the right of way to the Site as per provisions of the Agreement. Authority shall handover, to the IA, the right of way to the Site as per provisions of the Agreement only when the Conditions Precedent required to be satisfied by the IA have been duly fulfilled.

1.3.3. The Conditions Precedent required to be satisfied by the IA prior to the Appointed Date shall be deemed to have been fulfilled when the IA shall have:

- Furnished an unconditional and irrevocable Performance Bank Guarantee (PBG) as per (Annexure 5 of the RFP Volume I) from a nationalized bank and in a form and manner which is acceptable to the Authority, which would remain valid until such time as stipulated by the Authority.
- Obtained all statutory Approvals and Permits required for the performance of the Services under the Agreement; this may include Approvals/clearances, wherever applicable, that may be required for execution of the Agreement e.g., clearances from Government authorities for importing equipment, exemption of tax / duties / levies, work permits/clearances for IA/IA's team, etc. (as applicable)
- Furnished the notarized copies of any/all contract(s) duly executed by IA at the time of signing of the Contract in relation to the Project.

1.3.4. The Authority reserves the right to waive any or all the conditions specified in Article 1.3.3 above in writing and no such waiver shall affect or impair any right, power or remedy that the Authority may otherwise have.

1.3.5. Each Party shall make all reasonable endeavours to satisfy the Conditions Precedent within the time stipulated herein and provide the other Party with such reasonable cooperation as may be required to assist that Party in satisfying the Conditions Precedent for which that Party is responsible. The Parties shall notify in writing at least once a month on the progress made in satisfying the Conditions Precedent. The IA shall promptly inform the Authority when any Conditions Precedent for which it is responsible has been satisfied.

1.3.6. In the event that any of the conditions set forth in Clauses 1.3.2 and 1.3.3 herein above are not fulfilled within the Appointed Date, or such later date as may be mutually agreed upon by the Parties, the Authority may terminate the Contract and upon such termination, IA shall have no right to claim any damages from the Authority on such account.

1.4 Scope of Work

1.4.1. The Scope of the Work under the Agreement shall be as defined in **RFP Volume II** and Annexures thereto of the said RFP.

1.4.2. The Authority has engaged IA to provide services related to Implementation Agency for Integrated City Surveillance System at Puri, Odisha, using which the Authority intends to perform its business operations. IA with prior written approval of the Authority

would have the right to appoint a Sub Contractor for subcontracting any part of the Works/Services to such nominated Subcontractor. The Sub Contractor to be appointed and the subcontract shall be in a form and manner acceptable to the Authority. The Subcontractor shall fully abide by the terms and conditions of the Agreement. It is a fundamental term of the Agreement that appointment of a Sub Contractor would not absolve IA of any obligations to be performed by the Sub Contractor under the Agreement, and IA shall be responsible for all acts of the Sub Contractor and indemnify the Authority for losses, damages, claims suffered by the Authority due to any acts of omission and commission by the Sub Contractor while performing its obligations under the subcontract.

1.4.3. In addition to the above scope of work mentioned in Article 1.4 of this RFP, Authority may require IA to provide such Goods, Products, Services and support as the Authority may deem fit and proper and necessary, during the Term of the Agreement, and may include all such processes and activities which are consistent with the proposals set forth in the Bid, the Tender and the Agreement and are deemed necessary by the Authority, in order to meet its business requirements related to the Project.

1.5 Key Performance Measurements

1.5.1. Unless specified by the Authority to the contrary, IA shall deliver the Goods, perform the Services and carry out the Scope of Work in accordance with the terms of the RFP and the Agreement.

1.5.2. If the Agreement, Scheduled Requirements, Service Specification includes more than one Document, then unless the Authority specifies to the contrary, the later in time shall prevail over a Document of earlier date to the extent of any inconsistency.

1.5.3. The Authority may propose to amend any of the terms and conditions in relation to the Agreement/Service Specifications which shall be amended in consensus and mutual consent of IA and may issue any such directions which are not necessarily stipulated therein if it deems necessary for the fulfilment of the Schedule of Requirements and if such directions are resulting in extra time/fund requirement on part of IA; accordingly Authority shall by way of issuing a change request or otherwise extend the timelines and/or increase the price.

1.6 Commencement and Progress

1.6.1. Subject to the fulfilment of the Conditions Precedent under Article 1.3 above, IA shall commence the performance of its obligations in a manner as per the Scope of Work specified under Article 1.4 above.

1.6.2. IA shall proceed to carry out the Activities/Services with diligence and efficiently in accordance with any stipulation as to the time, manner, mode, and method of execution contained in the Agreement.

1.6.3. IA shall be responsible for and shall ensure that all Activities / Services are performed in accordance with the Agreement, Scope of Work, Scheduled Requirements and Service Specifications and that IA's Team complies with such Service Specifications

and all other standards, terms and other stipulations / conditions set out in this RFP and or the Agreement.

1.7 Standards of Performance

IA shall perform the Activities / Services and carry out its obligations under the Agreement with due diligence and in accordance with Good Industry Practices. IA shall employ appropriate advanced technology and engineering practices, shall maintain high safety standards, safe and effective equipment, machinery, material and methods and shall always act, in respect of any matter relating to this Agreement, as faithful advisors to the Authority and shall, at all times, support and safeguard the Authority's interests in any dealings with third parties.

1.8 Approvals and Required Consents

1.8.1. The Authority shall extend all necessary support to IA to obtain, maintain and observe all Applicable Permits/Approvals as may be necessary for IA to fulfil all its obligations under the Agreement and/or for providing Goods and Services to the Authority. The costs of such Applicable Permits/Approvals shall be solely borne by IA. Authority shall provide all reasonable co-operation, support and information available with it for obtaining such Approvals.

1.8.2. In the event, despite the support provided by the Authority, the Applicable Permit/Approval could not be obtained by IA within the Appointed Date, IA and the Authority shall discuss and co-operate with one another for achieving a reasonable alternative arrangement at the earliest, so that there is minimal disruption of Work or business operations, until such Approval(s) is/are obtained. However, if for any reason, no alternative arrangement could be achieved, Parties shall mutually decide the further course of action, however, until then, IA shall not be relieved of its obligations to provide the Services and to achieve the Service Levels.

1.8.3. Authority shall be responsible for paying electricity charges and shall also provide IA with tollfree helpdesk number for ICCC integration. IA will have to submit details of Monthly electrical charges that shall be borne by the authority.

1.9 IA's Obligations

1.9.1. IA's obligations shall include performance of all the Services as specified in the Scope of Work under Article 1.4 of this Volume III and under the other clauses of the RFP (Volume I, II and III), the Agreement and any amendments/changes thereof to enable the Authority to meet the objectives and operational requirements in the Agreement. It shall be IA's responsibility to ensure the proper and successful implementation, performance and continued operation of the proposed solution in accordance with and in strict adherence to the terms of its Bid, the RFP and the Agreement. In addition to the aforementioned, IA shall provide Services to manage and maintain the said system and infrastructure as mentioned in RFP Volume II.

1.9.2. IA shall ensure that the Services are performed through the efforts of IA's Team/Key Personnel and are in accordance with the terms hereof and to the satisfaction of the Authority. Nothing in this RFP or the Agreement will relieve IA from its liabilities

or obligations under the RFP or the Agreement to provide the Services in accordance with the Authority's directions and requirements and as stated in the Agreement and the Bid to the extent acceptable by the Authority and IA shall be liable for any non-performance, non-compliance, breach or other loss and damage resulting either directly or indirectly by or on account of its team.

1.9.3. IA shall be fully responsible for development /installation/ deployment and integration of all the software and hardware components and for resolving any problems/issues that may arise due to integration of components.

1.9.4. In addition to the aforementioned, IA shall provide Services to manage and maintain the said system and infrastructure as mentioned in RFP Volume II.

1.10 Selection of IA's Key Personnel

1.10.1. IA shall ensure that IA's Team/Key Personnel is/are competent, professional and possesses the requisite qualifications, skills and experience appropriate to the task they are required to perform under the Agreement.

1.10.2. The Authority reserves the right to interview and reject, if found unsuitable, the Key Personnel proposed by IA that shall be deployed as part of the Project team.

1.10.3. IA shall submit profiles of only those Key Personnel who are to be deployed on the Project.

1.11 Changes in IA's Key Personnel

1.11.1. The Authority reserves the right to require changes in IA's Key Personnel, which shall be communicated to IA.

1.11.2. With the prior approval of the Authority, IA may make additions to the Project team. IA shall provide the Authority with the resume of the proposed Key Personnel and provide such other information as the Authority may reasonably require.

1.11.3. In case of change in IA's Key Personnel/team members, for any reason whatsoever, IA shall also ensure that the exiting team members are replaced with at least equally qualified and professionally competent members.

1.11.4. In case of change in its team members and for ensuring a smooth transition between an outgoing team member with a new team member, IA shall ensure a reasonable amount of time overlap in activities to ensure proper knowledge transfer and handover / takeover of documents and other relevant materials between the outgoing and the new member.

1.12 Exit of IA's Key Personnel

IA shall ensure that none of the Key Personnel and manpower exit from the Project during the first 6 (six) months of the beginning of the Project. In cases where such exit is unavoidable, IA shall replace such Key Personnel and manpower with a suitable replacement with prior written approval from the Authority.

1.13 Services Provided by OEMs

1.13.1. IA shall ensure that the OEMs supply all Goods, including associated accessories and software required for the execution of the Works and shall support IA in the installation, commissioning, integration and maintenance of these components during the entire period of Agreement.

1.13.2. IA shall ensure that the Commercially available Off-The-Shelf (COTS) products supplied by the OEMs support IA in the installation/deployment, integration, roll-out and maintenance of the software applications during the entire period of Agreement. It must clearly be understood by IA that O&M of the System, Products and Services incorporated as part of System would commence from the day of Go-Live including all the solutions proposed.

1.13.3. IA would be required to explicitly display that it/they have a back-to-back arrangement for provisioning of warranty/O&M support till the end of Agreement period with the relevant OEMs. The maintenance support shall include patches and updates of the software, hardware components and other devices.

1.14 Software Licenses obtained by IA

1.14.1. All the software licenses that IA proposes to obtain or use for the purposes of fulfilling its various obligations under the Agreement have to be genuine. All Applicable Permits/Approvals/software licenses shall be obtained by IA in the name of Authority, or the Authority expressly agrees to give its consent in writing to do otherwise for the agreement period.

1.14.2. The Authority reserves the right to review the terms of the maintenance agreements entered into between IA and OEMs. If any such agreement /contract is executed, terminated and/ or amended / varied to the detriment of the Authority, then the Authority shall be informed and prior written consent of the Authority shall be taken for the agreements/ contracts, otherwise the authority shall have the right to consider this event as an " Event of default" of IA. The IA shall ensure that none of the components and sub-components is declared end-of-sale or end-of-support by the respective OEM at the time of submission of Bid. If the OEM declares any of the products/solutions end-of-sale subsequently, the IA shall ensure that the same is supported by the respective OEM for Agreement period.

1.14.3. If a product is de-supported by the OEM for any reason whatsoever, from the date of Acceptance of System till the end of Agreement, IA shall replace the products/solutions with an alternate that is acceptable to the Authority at no additional cost to the Authority and without causing any performance degradation.

1.14.4. IA shall ensure that the OEMs provide the support and assistance to IA in case of any problems/issues arising due to integration of components supplied by it with any other component(s)/product(s) under the purview of the overall solution. If the same is not resolved for any reason whatsoever, IA shall replace the required component(s) with an equivalent or better substitute that is acceptable to Authority without any additional

cost to the Authority and without impacting the performance of the solution in any manner whatsoever.

1.14.5. IA shall ensure that the OEMs shall provide for all hardware servers/equipment supply and/or installation of all types, updates, patches, fixes and/or bug fixes for the firmware or software from time to time at no additional cost to the Authority.

1.14.6. IA shall ensure that the OEMs for hardware, software, applications and other related equipment's/accessories or IA's trained engineers conduct the preventive maintenance on a fortnightly basis and break-fix maintenance in accordance with the Good Industry Practices. IA shall ensure that the documentation and training services associated with the components shall be provided by the OEM partner or OEM's certified training partner without any additional cost to the Authority. The training shall be conducted using official OEM course curriculum, mapped with the hardware/software product(s)to be implemented in the Project.

1.14.7. IA and their Personnel/representative shall not alter/change/replace any hardware component proprietary to the Authority and/or during operation and maintenance of third party without prior consent of the Authority.

1.14.8. IA shall keep and provide the required critical spares/components at the designated Project locations/office locations of the Authority (Collectively "Facilities") for meeting any unforeseen eventuality and for ensuring the various compliances and obligations under the Agreement.

1.15 Powers of IA's Representative(s) / Key Personnel

1.15.1. IA's representative(s) shall have all the powers requisite for the execution of Scope of Work and performance of Services under the Agreement. IA's representative(s) shall liaise with the Authority's representative for the proper coordination and timely completion of the Works and on any other matters pertaining to the Works.

1.15.2. IA's representative(s)shall extend full co-operation to Authority's representative in the manner required by them for supervision/inspection/observation of the equipment/goods/material, procedures, performance, progress, reports and records pertaining to the works. IA shall also have complete charge of IA's Team engaged in the performance of the Works and to ensure compliance of rules, regulations and safety practice. IA's representative(s) shall also cooperate with the other service providers/vendors of the Authority working at the Authority's office locations & field locations. Such IA's representative(s) shall be available to the Authority's Representative at respective CCC / OCAC/OCAC/Stakeholder Department's office during the execution of Works.

1.15.3. IA shall be responsible on an ongoing basis for coordination with other vendors and agencies of the Authority in order to resolve issues and oversee implementation of the same. IA shall also be responsible for resolving conflicts between vendors in case of borderline integration issues.

1.16 Access to Data Centre & ICCC Site

1.16.1 The access to data center and ICCC sites shall only be given to authorized representatives or at written request from authority.

1.17 Commencement of Installation

1.17.1 IA shall co-ordinate with the Authority and stakeholders for setting up of project infrastructure/components as per Scope of Work mentioned in RFP Volume II document.

1.17.2 As per guidelines of Telecom Regulatory Authority of India (TRAI), resale of bandwidth connectivity is not allowed. In such a case tripartite agreement should be entered into between the Authority, IA and internet/Network service provider(s). Tri partite agreement to be provided later.

1.17.3 The plan and design documents thus developed shall be submitted by IA for approval by the Authority.

1.17.4 After obtaining the approval from the Authority, IA shall commence the installation of products.

1.18 Reporting Progress

1.18.1 IA shall monitor progress of all the activities related to the execution of the Agreement and shall submit to the Authority progress reports with reference to all related work, Milestones and their progress during the implementation phase.

1.18.2 Formats for all above mentioned reports and their dissemination mechanism shall be discussed and finalized along with Project Plan. The Authority on mutual agreement between both Parties may change the formats, periodicity and dissemination mechanism for such reports.

1.18.3 Periodic meetings shall be held between the representatives of the Authority and IA once in every 7 days or time period as decided by the authority during the implementation phase to discuss the progress of implementation. After the implementation phase is over, the meeting shall be held as an ongoing basis, as desired by Authority, to discuss the performance of the Agreement.

1.18.4 IA shall ensure that the respective solution teams involved in the execution of Works are part of such meetings.

1.18.5 Several review committees involving representative of the Authority and senior officials of IA shall be formed for the purpose of the Project. These committees shall meet at regular intervals, as decided by the Authority at a later stage, to oversee the progress of the implementation of the Project.

1.18.6 All the Goods, Services and manpower to be provided/deployed by IA under the Agreement and the manner and speed of execution and maintenance of the Work and Services are to be conducted in a manner to the satisfaction of Authority's representative in accordance with the Agreement.

1.19 Inspection by the Authority

The Authority reserves the right to inspect and monitor/assess the progress/performance of the Works/Services/Project at any time during the course of the Agreement. The Authority may demand and upon such demand being made, IA shall provide documents, data, material or any

other information which the Authority may require, to enable it to assess the progress/performance of the Works/ Services/ Project.

1.20 Monitoring of IA's performance

1.20.1 At any time during the course of the Agreement, the Authority shall have the right to conduct, either itself or through another agency as it may deem fit, an audit to monitor the performance by IA of its obligations/functions in accordance with the standards committed to or required under the Agreement and IA undertakes to cooperate with and provide to the Authority or to the said agency any Document(s) and other details as may be necessary/required by them for this purpose. Such audit shall not include IA's books of accounts.

1.20.2 Should the rate of progress of the Works or any part of it, at any time falls behind the stipulated time for completion of any Milestone related to the Works or is found to be too slow to ensure completion of the Works by the stipulated time, or is in deviation to Tender requirements/standards, the Authority's representative shall so notify IA in writing.

1.20.3 IA shall send reply to the written notice giving details of the measures it proposes to take to expedite the progress so as to complete the Works by the prescribed time or to ensure compliance to RFP requirements/Agreement. IA shall not be entitled to any additional payment for taking such steps. If at any time it should appear to the Authority or Authority's representative that the actual progress of the Works does not conform to the Approved Plan, IA shall produce at the request of the Authority's representative a revised Plan showing the modification to the Approved Plan necessary to ensure completion of the Works within the time for completion or steps initiated to ensure compliance to the stipulated requirements.

1.20.4 The submission seeking approval by the Authority, or its representative of such Plan shall not relieve IA of any of its obligations or responsibilities under the Contract.

1.20.5 In case during execution of Works, the progress falls behind schedule or does not meet the Tender requirements, IA shall deploy extra manpower/resources to make up the progress or to meet the RFP/Agreement requirements. Plan for deployment of extra manpower/resources shall be submitted to the Authority for its review and approval. All time and cost effect in this respect shall be borne, by IA within the Agreement value.

1.21 Project Plan

1.21.1 As per the timelines mentioned in RFP Volume II, the, IA shall submit to the Authority for its approval a detailed Project Plan with details of the Project showing the sequence, procedure and method in which it proposes to carry out the Works. The Plan so submitted by IA shall conform to the requirements and timelines specified in the Agreement. The Authority and IA shall discuss and agree upon the work procedures to be followed for effective execution of the Works, which IA intends to deploy and shall be clearly specified.

1.21.2 The Project Plan shall include but not be limited to Project organization, communication structure, proposed staffing, roles and responsibilities, processes and tool sets to be used for quality assurance, security and confidentiality practices in accordance with Good Industry Practices and delivery schedule in accordance with the Agreement. Approval by

the Authority's Representative of the Project Plan shall not relieve IA of any of its duties or responsibilities under the Agreement.

1.21.3 If IA's Work Plans necessitate a disruption/shutdown in Authority's operation, the Plan shall be mutually discussed and developed so as to keep such disruption/shutdown to the barest unavoidable minimum. Any time and cost arising due to failure of IA to develop/adhere such a Work Plan shall be to its account.

1.22 Adherence to Safety Procedures, Rules, Regulations and Restrictions

1.22.1 IA's Team shall comply with the provision of all Applicable Laws including labour laws, rules, regulations and notifications issued there under from time to time. All safety and labour laws enforced by statutory Government Agencies and by Authority shall be applicable in the performance of this Agreement and IA's Team shall abide by these Applicable Laws.

1.22.2 Access to the existing Data Centre's Server Room, existing SJTA ICCC shall be strictly restricted. No access to any person except the essential members of IA's Team who are duly authorized by the Authority and are genuinely required for execution of the Works or for carrying out management/maintenance shall be allowed entry. Even if access is required to be provided to such unauthorized personnel of IA, the same shall be with prior approval of Authority's Representative and restricted to the pertaining equipment of the Authority on a need basis only. IA shall maintain a log of all activities carried out by each of its team/ Key Personnel.

1.22.3 No staff of IA, except the essential staff who have genuine work-related need, should be given access to the facilities. All such access should be logged in a loss free manner for permanent record with unique biometric identification of the staff to avoid misrepresentations or mistakes.

1.22.4 IA shall take all measures necessary or proper to protect its Key Personnel, Work and facilities and shall observe all reasonable safety rules and instructions. IA's Team shall adhere to all security requirement/regulations of the Authority during the execution of the Work. Authority's employees shall also be required to comply with safety procedures/policy.

1.22.5 IA shall report as soon as possible any evidence, which may indicate or is likely to lead to an abnormal or dangerous situation related to the Works/Project and shall take all necessary emergency control steps to avoid such abnormal situations.

1.23 Statutory Requirements

During the tenure of the Agreement nothing shall be done by IA or its team in contravention of Applicable Laws or any amendment thereof governing inter-alia customs, stowaways, foreign exchange etc. and shall keep Authority indemnified in this regard.

1.24 Authority's Obligations

1.24.1 Authority or its nominated representative shall act as the nodal point for implementation of the Agreement and for issuing necessary instructions, approvals, commissioning, acceptance certificates, payments etc. to IA.

1.24.2 Authority shall ensure that timely approvals are provided to IA as and when required, which may include approval of Project Plans, implementation methodology, design documents, specifications, or any other document necessary in fulfilment of the Agreement.

1.24.3 The Authority's representative shall interface with IA, to provide the required information, clarifications, and to resolve any issues as may arise during the execution of the Agreement. Authority shall provide adequate cooperation in providing details, coordinating and obtaining of approvals from various governmental agencies, in cases, where the intervention of the Authority is proper and necessary.

1.24.4 Authority may provide on IA's request, particulars/information/or documentation that may be required by IA for proper planning and execution of the Works and for providing Services covered under the Agreement and for which IA may have to coordinate with respective vendors.

1.24.5 Authority shall provide to IA only sitting space and basic infrastructure not including stationery and other consumables at the Authority's office locations.

1.24.6 Readiness of the Project site: Authority hereby agrees to make the Project sites ready as per the agreed specifications, within the agreed timelines. Authority agrees that IA shall not be in any manner liable for any delay arising out of Authority's failure to make the site ready within the stipulated period.

1.25 Payments

1.25.1 Authority shall make payments to IA at the times and in the manner set out in the Payment schedule as specified under Payment Milestones in RFP Volume II subject to the penalties as mentioned under Articles 3.1 and 3.2 of Section C- Service Levels of Volume III. Authority shall make all efforts to make payments to IA within 30 (thirty) days of receipt of invoice(s) and all necessary supporting documents.

1.25.2 All payments agreed to be made by Authority to IA in accordance with the Bid shall be inclusive of all statutory levies, duties, taxes and other charges whenever levied/applicable, if any, and Authority shall not be liable to pay any such levies/other charges under or in relation to the Agreement and/or the Services.

1.25.3 No invoice for extra work/change order on account of change order shall be submitted by IA unless the said extra work/change order has been authorized/approved by the Authority in writing in accordance with Change Control Note (as mentioned under Annexure I of this volume of the RFP)

1.25.4 In the event of Authority noticing at any time that any amount has been disbursed wrongly to IA or any other amount is due from IA to the Authority, the Authority may without prejudice to its rights recover such amounts by other means after notifying IA or deduct/adjust such amount from any payment falling due to IA. The details of such recovery, if any, shall be intimated to IA. Similarly, IA shall also be entitled to receive the

payment of any undisputed amount under subsequent invoice for any amount that has been inadvertently omitted in previous invoice on the part of the Authority or IA.

1.25.5 All payments to IA shall be subject to the deductions of tax at source under Income Tax Act, and other taxes and deductions as provided for under Applicable Laws. All costs, damages or expenses which Authority may have paid or incurred, for which under the provisions of the Agreement, IA is liable, the same shall be deducted/set off by Authority from any payments/dues payable to IA. All payments to IA shall be made after making necessary deductions as per terms of the Agreement and recoveries towards facilities, if any, provided by the Authority to IA on chargeable basis.

1.26 Intellectual Property Rights

1.26.1 Except for any ownership rights in any intellectual property that have been expressly granted to the IA under the Agreement, the Authority shall retain all rights, title and interest in and to any third-party licensed technology, including all worldwide technology and Intellectual Property Rights which has been used for the Project.

1.26.2 Preservation of notice: IA shall not remove, efface or obscure any copyright notices or other proprietary notices or legends from any licensed technology or materials provided under the Agreement, and shall reproduce all such notices and legends when incorporating licensed technology or materials into any integrated products.

1.26.3 Authority shall own and have a right in perpetuity to use all newly created Intellectual Property Rights which have been developed solely during execution of the Agreement, including but not limited to all processes, software, training models, technology, processes, methodologies, process improvements, ideas, concepts, products, specifications, reports and other documents which have been newly created and developed by IA or its Subcontractor solely during the performance of Services/execution of the Agreement (hereinafter "Developed Materials") and for the purposes of inter-alia use during the Project. IA shall undertake to promptly disclose to the Authority all such Intellectual Property Rights/Developed Materials created during the performance of the Services/Works. IA shall promptly assign, completely and in writing to Authority any such Developed Materials and shall execute all such agreements/documents and obtain all permits and approvals that may be necessary to perfect Authority's rights in the Developed Materials. It is a fundamental provision of the Agreement that IA will not violate or breach any Intellectual Property Rights of the Authority.

1.26.4 Pre-existing work: All Intellectual Property Rights existing prior to the Effective Date of the Agreement shall belong to the Party that owned such rights immediately prior to the Effective Date. Subject to the foregoing, the Authority will also have rights to use and copy all Intellectual Property Rights, process, specifications, reports and other document, drawings, manuals etc. provided or used by the IA / Sub-Contractors as part of the Scope of Works under the Agreement for the purpose of the Agreement on non-exclusive, non-transferable, perpetual, royalty-free license to use basis.

1.26.5 Commercially off the Shelf (COTS) / third party products: All COTS products and related solutions and fixes provided pursuant to the Agreement shall be licensed according to the terms of the license agreement packaged with or otherwise applicable to such products. Such licenses shall be brought on behalf of and in the name of the Authority or mentioning

the Authority as the end user of such licenses. IA shall be responsible for arranging any licenses associated with products. Unless otherwise specifically restricted by the licensing terms of the COTS products, all Intellectual Property Rights in any development/enhancement/customization etc. done on the COTS products pursuant to the Agreement shall be owned by the Authority.

1.26.6 Further, the IA shall be obliged to ensure that all Applicable Permits which are, inter-alia, necessary for use of the Deliverables, Goods, Services, applications work etc. provided/undertaken by the IA / Sub-Contractors under the Agreement shall be acquired in the name of the Authority and to use such permits till the term of such permits on behalf of the Authority solely for the purpose of execution of any of its obligations under the terms of the Agreement. However, even subsequent to the Term/expiry of the Agreement, such Approvals/Applicable Permits shall endure to the exclusive benefit of the Authority.

1.26.7 IA shall not copy, reproduce, translate, adapt, vary, modify, disassemble, decompile or reverse engineer or otherwise deal with or cause to reduce the value of the Products except as expressly authorized by Authority in writing.

1.26.8 In the event IA's Intellectual Property Rights are embedded in the Deliverables, IA grants to Authority a non-exclusive, non-transferable, irrevocable, royalty free and perpetual license for the Authority's internal use of the same as part of the Deliverables in which they are embedded. Nothing contained in this Agreement shall be construed to grant the Authority any right to use or exploit such IA's Intellectual Property Rights in its stand-alone form separate and apart from the Deliverables.

1.27 Taxes

1.27.1 IA shall bear all personal taxes levied or imposed on its Personnel, or any other member of IA's Team, etc. on account of payment received under the Agreement. IA shall bear all corporate taxes, levied or imposed on IA on account of payments received by it from the Authority for the Work done/Services provided under the Agreement.

1.27.2 IA shall bear all outgoings, cess, taxes (including municipal taxes), levies, import duties, fees (including any license fees) rates and other user charges (excluding those applicable for existing utility connections and any other dues, assessments or outgoings payable in respect of implementation of the Project, (excluding new utility connections obtained by it, if any) or in respect of the materials stored therein which may be levied by any Government Authority as may be levied or imposed on IA under or in relation to the Agreement and under the Applicable Laws including but not limited to Goods & Services Tax (GST) (including any IGST,CGST & SGST) and all Income Tax levied under Indian Income Tax Act – 1961 or any amendment thereof during the entire Agreement period and thereafter till such time the liability relates to IA's obligation under the Agreement, i.e., on account of Goods supplied and Services rendered and payments received by it from the Authority under the Agreement. It shall be the responsibility of IA to submit to the concerned Indian authorities the returns and all other connected documents required for this purpose. IA shall also provide the Authority such information, as it may be required in regard to IA's details of payment made by the Authority under the Agreement for proper assessment of taxes and duties as may be imposed under Applicable Laws. The

amount of tax withheld by the Authority shall at all times be in accordance with Indian Tax Law or any other Government Agency and the Authority shall promptly furnish to IA original certificates for tax deduction at source and paid to the Tax authorities.

1.27.3 IA agrees that it shall comply with the Indian Income Tax Act or any other Applicable Laws in force from time to time and pay Indian Income Tax or other applicable taxes and duties, as may be imposed/levied on them by the Indian Income Tax Authorities/Government Authorities, for the payments received by them for the Works performed under the Agreement.

1.27.4 IA shall fully familiarize themselves about the taxes applicable to the Bidders under Applicable Laws on the amounts payable by the Authority to them under the Agreement. All such taxes must be included by Bidders in their financial proposal. (Bidder to find out applicable taxes for the components being proposed.)

1.27.5 Should IA fail to submit returns/pay taxes in times as stipulated under applicable Indian/State Tax Laws, and consequently, any interest or penalty is imposed by the concerned authority on Authority/IA, IA shall bear the same. IA shall indemnify Authority from and against any and all claims, liabilities, losses or damages arising out of the Agreement or in connection with such taxes, including interest and penalty levied/assessed by any such tax authority against the Authority/IA.

1.27.6 The goods and services tax (GST) on Works (central or state) if levied on supplies made from indigenous vendors for the Works shall be borne by IA within the Agreement Value.

1.27.7 The Authority shall if so, required by Applicable Laws in force, at the time of payment, deduct income tax payable by IA at the rates in force, from the amount due to IA and pay to the concerned tax authority directly.

1.28 Indemnity

1.28.1 The IA hereby indemnifies and agrees and undertakes that from the Effective Date and thereafter during the Term and even after expiry of the Term, it shall keep indemnified and otherwise saved and harmless the Indemnified Parties from and against any and all third party claims for Liabilities, demands made against and/or loss caused and/or the damages suffered and/or cost, charges/expenses incurred or put to and/or penalty levied and/or any claim due to injury or death of any person and/or loss or damage caused or suffered to any property owned or belonging to Authority, their agents and employees or third party as a result of any acts, deeds or thing done or omitted to be done by IA (or any personnel, agent, representative, or Sub-Contractors thereof) or on the failure of the IA to perform any of its statutory duty and/or obligations or failure or negligence on the part of IA to comply with any applicable Laws applicable to the IA as an IT Service Provider or applicable Permits or as a consequence of any notice, show cause notice, action, suit or proceedings, given, initiated, filed or commenced by any third party (including end users or Government Authority) or as a result of any failure or negligence or default of the IA or the Sub-Contractors and/or their invitees as the case may be, in connection with or arising out of the Agreement or arising out of or in connection with IA's use and occupation of the Site located thereon. Notwithstanding anything to the contrary contained herein, in no event shall any of the Indemnified Parties be liable to indemnify the IA for any matter arising out of or in connection with the Agreement in respect of any indirect or consequential loss, including loss of profit, suffered by the IA.

1.28.2 The indemnity provisions herein and under the Agreement shall survive expiry or earlier termination of the Agreement.

1.29 Notice and Contest of Claims / Demands

In the event that any Party hereto receives claims or demands from a third party in respect of which it is entitled to the benefit of an indemnity under Article 30 or in respect of which it is entitled to reimbursement (the "'Indemnified Party"), it shall notify the other Party responsible for indemnifying such claim hereunder (the "Indemnifying Party") within 15 (fifteen) days of receipt of the claim and/or shall not settle or pay the claim/ demand without the prior approval of the Indemnifying Party, which approval shall not be unreasonably withheld or delayed. In the event that the Indemnifying Party wishes to contest or dispute the claim, it may conduct the proceedings in the name of the Indemnified Party and at its (Indemnifying Party's) risk, costs and expense. The Indemnified Party shall provide all cooperation and assistance in contesting any claim and shall sign all such writings and documents as the Indemnifying Party may reasonably require.

1.30 Representations and Warranties

Representations and Warranties of IA: The IA hereby represents and warrants to Authority that as on the Effective Date (which representations and warranties shall be continuing representations and warranties and deemed to have been repeated on each day of the term of the Agreement):

1.30.1 It is duly organized and validly existing under the laws of India and that it has been in continuous existence since incorporation.

1.30.2 It has full power and authority to execute, deliver and perform its obligations under the Agreement and to carry out the Project.

1.30.3 It has taken all necessary corporate and other actions under Applicable Laws and its Memorandum and Articles of Association to authorize the execution, delivery and performance of its obligations under the Agreement.

1.30.4 It has complied with all Applicable Laws and has not been subject to any fines, penalties, injunctive relief or any other civil or criminal liabilities, or any order, writ, injunction or decree of any court or any legally binding order of any governmental authority, which in the aggregate have or may have Material Adverse Effect on its ability to perform its obligations and duties under the Agreement and undertake the Project in terms of the Agreement.

1.30.5 It has the technical and financial standing and capacity to undertake and complete the Project.

1.30.6 All the employees, officials, personnel, agents, contractors and/ or Sub-Contractors utilized/ proposed to be by the IA for the purposes of the Project, possess/ shall possess the relevant technical and financial standing and capacity to undertake and complete the Project.

1.30.7 The obligations under the Agreement shall be legally valid, binding and enforceable obligations against it in accordance with the terms hereof.

1.30.8 The information furnished in the Bid by the IA (and as updated on before the date of the Agreement) is true and accurate in all respects.

1.30.9 The execution, delivery and performance of the Agreement, does not and will not conflict with, or result in the breach of, or constitute a default under, or affect performance required by any of the provisions of its Memorandum and Articles of Association or any Applicable Laws or any covenant, agreement, understanding, decree or order to which it is a party or by which it or any of its properties or assets are bound or affected.

1.30.10 There are no actions, suits, proceedings or investigations pending, or, to the best of the IA's knowledge, threatened against it before any court or before any judicial, quasi-judicial or other authority, the outcome of which may result in the breach of or constitute a default of the IA under the Agreement or which individually or in the aggregate may result in any Material Adverse Effect on its business, properties, assets or its condition, financial or otherwise, or in any impairment of its ability to perform its obligations under the Agreement.

1.31 Design Warranties

Without prejudice to the generality of the foregoing provisions of this Article 32, the IA represents and warrants that all work performed by the IA and Sub-Contractor shall be executed with due care and diligence, in conformity with the Agreement and free of defects and deficiencies, including that:

1.31.1 The design and engineering of the Project shall satisfy the minimum requirements set forth in the Agreement and shall be free of defects and deficiencies. Such engineering and design shall be such that the Project shall function properly in accordance with the terms of the Agreement and the Specifications and shall meet all design, engineering, safety, and operability criteria as specified in the Agreement.

1.31.2 The Project shall be in accordance with the designs, drawings and Specifications prepared in accordance herewith and approved by Authority, in accordance with the terms hereof, and all workmanship of the IA and Sub-Contractors shall be in full conformity with the requirements of the Agreement and free of defects and deficiencies (including latent defects and deficiencies).

1.31.3 All plant, equipment and materials supplied under the Agreement shall not be nearing end of sale/End of support; and shall be supported by the IA and respective OEM along with Service and spares support to ensure its efficient and effective operation for the entire duration of the Agreement. They shall be in full conformity with the Specifications and other requirements of the Agreement, shall be of specified quality and where quality is not specified then of suitable quality for the purposes and uses intended and shall be free of defects and deficiencies (including latent defects).

1.31.4 Without prejudice to the generality of the foregoing, the entire Project shall be designed, engineered, constructed, and otherwise implemented and developed so as to ensure that the Assets and the Project Utilities, meet the Design Life.

1.31.5 The IA's obligation to design, engineer, procure and construct the Project correctly and in accordance with the Agreement and its warranties set forth above shall not be reduced or

affected by Authority's approval or grant of NOC, in respect thereof, including for any designs, plans, phasing, drawings or specifications thereof.

1.31.6 All Goods supplied by the IA under the Agreement shall be maintained through Support and Maintenance Contracts, with the original equipment manufacturer (OEM), outlining regular check-ups and routine work to regulate the performance and quality output. IA shall enter into such maintenance contracts for an efficient upkeep of the equipment and installations. IA will indemnify the Authority that all the machines and equipment will remain functional during the contractual period.

1.31.7 Technical support for entire system shall be provided by IA / the respective OEMs for the period of Agreement. The technical support shall also include all upgrades, updates and patches to the software applications.

1.31.8 The IA further warrants that the Goods supplied under the Agreement shall be free from all encumbrances and defects/faults arising from design, material, manufacture or workmanship (except insofar as the design or material is required by the Authority's specifications) or from any act or omission of the IA, that may develop under normal use of the supplied Goods in the conditions prevailing at the respective SJTC ICCC / city field locations.

1.31.9 The Authority shall promptly notify the IA in writing of any claims arising under this warranty.

1.31.10 Upon receipt of such notice, the IA shall, with all reasonable speed, repair or replace the defective Goods or parts thereof, without prejudice to any other rights which the Authority may have against the IA under the Agreement.

1.31.11 If the IA, having been notified, fails to remedy the defect(s) within a reasonable period, the Authority may proceed to take such remedial action as may be necessary, at the IA's risk and expense and without prejudice to any other rights which the Authority may have against the IA under the Agreement.

1.32 Representations & Warranties of Authority

Authority hereby represents and warrants to the IA that as on the Effective Date:

1.32.1 It is duly organized and validly existing under the laws of India and has been in continuous existence since its constitution.

1.32.2 It has full power and authority to execute, deliver and perform its obligations under the Agreement.

1.32.3 Authority has power and authority to grant the Lease Rights under and pursuant to this Development Agreement

1.32.4 It has taken all necessary actions under Applicable Laws to authorize the execution, delivery and performance of the Agreement.

1.32.5 The obligations of Authority under the Agreement will be legally valid, binding and enforceable against Authority in accordance with the terms of the Agreement.

1.32.6 It has no knowledge of any violation or default with respect to any order, writ, injunction or any decree of any court or any legally binding order of any Government Authority

which may result in any Material Adverse Effect or impairment of Authority's ability to perform its obligations and duties under the Agreement.

1.32.7 To the best of Authority's knowledge and belief, there are no actions, suits, proceedings or investigations pending against it, before any court or Government Authority in relation to the Project, the outcome of which may result in the breach of or constitute a default of Authority under the Agreement or result in impairment of Authority's ability to perform its obligations and duties under the Agreement.

1.33 Disclosure

In the event at any time after the date hereof, any event or circumstance comes to the attention of IA that renders any of its abovementioned representations or warranties untrue, inaccurate or incorrect, then such Party shall immediately notify the Authority of the same. Such notification shall not have the effect of (a) remedying any breach of the representation or warranty that has been found to be untrue, inaccurate or incorrect; or (b) adversely affecting the rights of Authority or releasing any obligation of IA under the Agreement.

1.34 Term and Extension of the Agreement

1.34.1 The Agreement Term/period shall commence from the date of signing of Agreement or issuance of letter of intent/letter of award, whichever is earlier, and shall remain valid till project completion/ tenure.

1.34.2 If any delay occurs due to circumstances beyond control of IA such as strikes, lockouts, fire, accident, defective materials, delay in obtaining Applicable Permits/Approvals or any cause whatsoever beyond the reasonable control of IA, a reasonable extension of time/ Term, upon a request being made by IA in writing at least 15 days in advance shall be granted by the Authority in writing.

1.34.3 Notwithstanding what has been stated under Article 1.33, the Authority shall reserve the sole right to grant any such extension to the Term above mentioned and shall notify in writing to IA, at least 15 days before the expiration of the Term hereof, whether it shall grant IA an extension of the Term or not. The decision to grant or refuse the extension of the Term shall be at the Authority's sole discretion and such extension of the Agreement, if any, shall be as per terms agreed mutually between the Parties.

1.34.4 Where the Authority is of the view that no further extension of the Term should be granted to IA, the Authority shall notify IA of its decision at least 15 days prior to the expiry of the Term. Upon receipt of such notice, IA shall continue to perform all its obligations hereunder till the duration of the Term. During the notice period, the Authority shall either appoint an alternative agency/Replacement Service Provider/reappoint IA for a short extension or create its own infrastructure to operate such Services as are provided under the Agreement.

1.34.5 In the event of any failure or delay by Authority to hand over the right of way to the Site or Approvals to the IA, such failure or delay shall in no way affect or vitiate the Agreement or alter the character thereof or entitle the IA to damages or compensation thereof, but in

any such case, Authority may grant such extension or extensions of the Completion Date, as may be considered reasonable.

1.35 Dispute Resolution

1.35.1 In case, a dispute is referred to arbitration, the arbitration shall be under the Indian Arbitration and Conciliation Act, 1996 and any statutory modification or re-enactment thereof.

1.35.2 If during the subsistence of the Agreement or thereafter, any dispute between the Parties hereto arising out of or in connection with the validity, interpretation, implementation, breach or any alleged breach of any provision of the Agreement or regarding any question, including as to whether the termination of the Agreement by one Party hereto has been legitimate/valid, the Parties hereto shall endeavour to settle such dispute amicably through joint discussion and/or by Conciliation to be governed by the Arbitration and Conciliation Act, 1996. However, despite such efforts, if the dispute, differences or controversy still remains unresolved for a period of 30 days of its having been raised, then the same shall be referred to Arbitration.

1.35.3 The Arbitration proceedings shall be held in the following manner:

- The Arbitration proceedings shall be held in a court of law to which the jurisdiction of the High Court of Odisha Extends.
- The Arbitration proceeding shall be governed by the Arbitration and Conciliation Act, 1996 and any re-enactment(s) and/or modification(s) thereof and of the Rules framed thereunder shall apply to arbitration proceedings.
- The proceedings of Arbitration shall be in English language.
- Any dispute, difference or question to be referred to arbitration shall be initially referred to a mutually acceptable sole arbitrator. In case the Parties are unable to agree upon the sole arbitrator, then each Party shall appoint one arbitrator each and the two arbitrators so appointed shall appoint the third arbitrator, who shall be the Presiding Arbitrator.
- In case, a Party fails to appoint an arbitrator within 30 days from the receipt of the request to do so by the other Party or if the two Arbitrators so appointed fail to agree on the appointment of third Arbitrator within 30 days from the date of their appointment upon request of a party, in a court of law to which the jurisdiction of the High Court of Odisha Extends or any person or institution designated by him shall appoint the Arbitrator/Presiding Arbitrator upon request of one of the Parties.
- Any letter, notice or other communications dispatched to IA relating to either arbitration proceeding or otherwise whether through the post or through a representative on the address last notified to the Authority by IA shall be deemed to have been received by IA although returned with the remarks,

refused 'undelivered' where about not known or words to that effect or for any other reasons whatsoever.

- If the Arbitrator so appointed dies, resigns, incapacitated or withdraws for any reason from the proceedings, it shall be lawful for the Authority to appoint another person in his place in the same manner as aforesaid. Such person shall proceed with the reference from the stage where his predecessor had left if both Parties consent for the same; otherwise, he shall proceed de novo.
- It is a term of the Agreement that the Party invoking arbitration shall specify all disputes to be referred to arbitration at the time of invocation of arbitration and not thereafter.
- It is also a term of the Agreement that neither Party to the Agreement shall be entitled for any interest on the amount of the award.
- The Arbitrator shall give reasoned award and the same shall be final, conclusive and binding on the Parties.
- The fees of the arbitrator, costs and other expenses incidental to the arbitration proceedings shall be borne equally by the Parties.

1.36 Conflict of interest

IA shall disclose to the Authority in writing, all actual and potential conflicts of interest that exist, arise or may arise (either for IA or IA's Team) in the course of providing Goods and performing the Works/Services as soon as practical after it becomes aware of that conflict.

1.37 Publicity

IA shall not make or permit to be made a public announcement or media release about any aspect of this Agreement unless the Authority first gives IA its written consent.

1.38 Force Majeure

1.38.1 The IA or Authority, as the case may be, shall be entitled to initially suspend the performance of its respective obligations under the Agreement to the extent that the IA or Authority, as the case may be, is unable to render such performance due to a Force Majeure Event.

1.38.2 In the Agreement, no event or circumstance and/or no combination of events and circumstances shall be treated as a Force Majeure Event unless it satisfies all the following conditions:

- materially and adversely affects the performance of an obligation.
- are beyond the reasonable control of the affected Party.
- such Party could not have prevented or reasonably overcome with the exercise of Good Industry Practice or reasonable skill and care.

- do not result from the negligence or misconduct of such Party or the failure of such Party to perform its obligations hereunder; and
- which, by itself or consequently, has an effect described in Article 1.37.1

1.38.3 "Force Majeure Event" includes the following events and/ or circumstances to the extent that they or their consequences satisfy the requirements set forth in Article 1.37.2:

a. war (whether declared or undeclared), invasion, armed conflict or act of foreign enemy in each case involving or directly affecting the Project Land

b. revolution, riot, insurrection or other civil commotion, act of terrorism or sabotage in each case within the Project Land or near vicinity

c. nuclear explosion, radioactive or chemical contamination or ionizing radiation directly affecting the Project Land and/or the Assets, unless the source or cause of the explosion, contamination, radiation or hazardous thing is brought to or near the Project Land by the Developer or any Affiliate of the Developer or any Sub-Contractor of the Developer or any of their respective employees, servants or agents

d. strikes, working to rule, go-slows and/or lockouts which are in each case widespread, nationwide or political and affects the Project Land

e. any effect of the natural elements, including lighting, fire, earthquake, unprecedented rains, tidal wave, flood, storm, cyclone, typhoon or tornado, within the Project Land or near vicinity

f. explosion (other than a nuclear explosion or an explosion resulting from an act of war) within the Project Land or near vicinity.

g. epidemic or plague within the Project Land or near vicinity; and

h. any event or circumstances of a nature analogous to any events set forth in Article 1.37.3 within the Site or near vicinity.

1.38.4 It is clarified that non-availability of any plant, equipment, materials or financial resources for any reason whatsoever shall not be deemed to be an event of Force Majeure.

1.38.5 Force Majeure shall not include any events caused due to acts/omissions of IA resulting in a breach/contravention of any of the terms of the Agreement and/or IA's Bid. It shall also not include any default on the part of IA due to its negligence or failure to implement the stipulated/proposed precautions, as were required to be taken under the Agreement.

1.38.6 In such an event, the affected Party shall inform the other Party in writing within 5 (five) days of the occurrence of such event. Any failure or lapse on the part of IA in performing any obligation as is necessary and proper, to negate the damage due to projected Force Majeure Events or to mitigate the damage that may be caused due to the above-mentioned events or the failure to provide adequate disaster management/recovery or any failure in setting up a contingency mechanism would not constitute Force Majeure, as set out above.

1.38.7 In case of a Force Majeure Event, all Parties shall endeavour to agree on an alternate mode of performance in order to ensure the continuity of the Service/ Works and

implementation of the obligations of a Party under the Agreement and to minimize any adverse consequences of Force Majeure.

1.38.8 If at any time, during the Term, the performance in whole or in part by either Party of any obligation under the Agreement is prevented or delayed by reason of any Force Majeure Event, and notice of the happening of any such event is given by the affected Party to the other Party in accordance with Article 37, neither Party shall by reason of such event, be entitled to terminate the Agreement nor shall either Party have any claim for damages against the other in respect of such non-performance or delay in performance and the Project (or the parts so affected) due to such Force Majeure Event and the Agreement shall be resumed as soon as practicable after such event has come to an end or ceased to exist and the decision of the Authority as to whether the Project have been so resumed or not shall be final and conclusive.

1.39 Delivery

1.39.1 IA shall bear the cost for packing, transport, insurance, storage and delivery of all the Goods for implementation of the Project in Puri)" at all locations identified by the Authority in Puri.

1.39.2 The Goods under the Agreement shall conform to the standards mentioned in the RFP, and when no applicable standard is mentioned, to the authoritative standards, such standard shall be approved by Authority.

1.39.3 IA shall only procure the hardware and software after approvals from a designated committee/Authority.

1.39.4 IA's Key Personnel shall have the required experience and proper qualifications to perform the Services, and the Authority shall have the right to reject any such Personnel if found unfit by Authority to provide the Services. IA shall also impart the appropriate training to its engineers and Personnel on the current and emerging technologies, concepts and configurations in order to provide the Services in a more efficient manner.

1.40 Insurance

1.40.1 The Goods supplied under the Agreement shall be comprehensively insured by IA at its own cost, against any loss or damage, for the entire period of the Agreement. IA shall submit to the Authority, documentary evidence issued by the insurance company, indicating that such insurance has been taken.

1.40.2 IA shall bear all the statutory levies like customs, insurance, freight, etc. applicable on the Goods and also the charges like transportation charges, GST etc. that may be applicable till the Goods are delivered at the respective sites of installation shall also be solely borne by IA.

1.40.3 IA shall take out and maintain at its own cost, on terms and conditions approved by the Authority, all necessary insurance against the risks, and for the coverages, as specified below:

- At the Authority's request, shall provide evidence to the Authority showing that such insurance has been taken out and maintained and that the current premiums therefore have been paid; and
- Employer's liability and workers' compensation insurance in respect of the Personnel of the IA, in accordance with the relevant provisions of the Applicable Laws including personal accident and death in respect of its Personnel or any other insurance as may be appropriate and the proof of such insurances shall be provided to Authority, when so requested. Notwithstanding the above, the Key Personnel of IA shall be and shall remain the employees of IA and IA alone shall be responsible for the payment of all dues with respect to them or meeting any statutory obligations under the Applicable Laws with respect to such Personnel.

1.40.4 All Commercially off the Shelf (COTS) products/ Open-Source Solutions and related solutions and fixes provided pursuant to this Agreement shall be licensed according to the terms of the license agreement packaged with or otherwise applicable to such products. Such licenses shall be brought on behalf of and in the name of Authority or mentioning Authority as the end user of such licenses. IA shall be responsible for arranging any licenses associated with products. "Product" means any computer code, web-based services, or materials comprising commercially released, pre-release or beta products (whether licensed for a fee or no charge) and any derivatives of the foregoing which are made available to the Purchaser for license which is published by product owner or its affiliates, or a third party. "Fixes" means product fixes that are either released generally (such as commercial product service packs) or that are provided to you when performing services (such as workarounds, patches, bug fixes, beta fixes and beta builds) and any derivatives of the foregoing. Unless otherwise specifically restricted by the Licensing Terms of the COTS products / Open-Source Solutions, all intellectual property rights in any development/enhancement/customization etc. done on the COTS products/ Open-Source Solutions pursuant to this Agreement shall be owned by Authority. Further, the IA shall be obliged to ensure that all approvals, registrations, licenses, permits and rights which are, inter-alia, necessary for use of the Deliverables, goods, services, applications, services etc. provided by the IA / subcontractors under this Agreement shall be acquired in the name of the Authority and IA shall have the non-exclusive, limited right to use such licenses till the Term on behalf of the Authority solely for the purpose of execution of any of its obligations under the terms of this Agreement. However, subsequent to the term of this Agreement, such approvals etc. shall endure to the exclusive benefit of the Authority.

1.40.5 Forthwith upon expiry or earlier termination of the Agreement and at any other time on demand by the Authority, IA shall deliver to the Authority all Documents provided by or originating from the Authority and all Documents produced by or from or for IA in the course of performing the Services, unless otherwise directed in writing by the Authority at no additional cost. IA shall not, without the prior written consent of the Authority store, copy, distribute or retain any such Documents.

1.41 Exit Management Plan

1.41.1 An Exit Management plan shall be furnished by IA in writing to the Authority within 90 (ninety) days from the date of signing of the Agreement, which shall deal with at least the following aspects of exit management in relation to the Agreement as a whole and in relation to the Project implementation, and Service Level monitoring:

- A detailed program of the transfer process that could be used in conjunction with a Replacement Service Provider including details of the means to be used to ensure continuing provision of the Services throughout the transfer process or until the cessation of the Services and of the management structure to be used during the transfer.
- Plans for provision of contingent support to Project and Replacement Service Provider for a reasonable period after transfer.
- Exit Management Plan in case of normal termination of Agreement period.
- Exit Management Plan in case of any eventuality due to which Project is terminated before the Agreement period; and
- Exit Management Plan in case of termination of IA.

1.41.2 In the event of termination or expiry of the Agreement, Project implementation, or Service Level monitoring, both IA and Authority shall comply with the exit management plan.

1.41.3 During the exit management period, IA shall use its best efforts to deliver the Works/Services.

2. PART B – Special Conditions of Agreement

2.1 Performance Security

To guarantee its performance under the Agreement, the IA shall provide to Authority in its favour a Performance Bank Guarantee (PBG) which is unconditional, unequivocal and irrevocable for an amount equivalent to 10% of the Total Project Cost at the commencement of Project in the format prescribed in RFP, issued by any of the nationalized banks only. The Performance Bank Guarantee shall be kept valid up to a period of 3 (Three) months after the project completion timelines.

The Performance Bank Guarantee shall be encashed by the Authority in the event of IA's failure to complete obligations or breach by IA of any of the terms and conditions of the Agreement.

2.2 Liquidated Damages

2.2.1 If IA fails to supply, install or maintain any or all of the Goods or fails to complete the Works or fails to provide the Services as per the Agreement, within the time period(s) specified in the RFP Vol II, the Authority without prejudice to its other rights and remedies under the Agreement, deduct from the Agreement value, as liquidated damage per week of 1% of the payment to be remitted on successful Go-Live of System i.e. 40% of order value per week till such time the default continues.

2.2.2 The deduction shall not in any case exceed 10 % of the payment to be remitted on successful Go-Live of System i.e. 40% of order value and upon reaching such limit, the Authority shall, in its sole discretion, be entitled to terminate the Agreement. The Authority may without prejudice to its right to effect recovery by any other method, deduct the amount of liquidated damages from any payments due to IA in its hands (which includes the Authority's right to claim such amount against IA's Bank Guarantee) or which may become due to IA at a prospective date. Any such recovery or liquidated damages shall not in any way relieve IA from any of its obligations to complete the Work or from any other obligations and liabilities under the Agreement.

2.2.3 Delay not attributable to IA shall be considered for exclusion for the purpose of computing liquidated damages.

2.3 Limitation of Liability

2.3.1 Notwithstanding anything to the contrary in this Agreement, the liability of one Party towards the other Party for any damages or compensation of any nature whatsoever under this Agreement, shall not exceed Total Project Cost. For avoidance of doubt, the limitation hereunder shall not apply to any or all liabilities in respect of third parties. The Parties agree that the IA's liability will be uncapped in case of any liabilities arising due to:

- any amount payable as indemnity to the Authority due to its acts or omissions
- or fraud, gross negligence and wilful misconduct
- breach of any Applicable Laws or any Applicable Permits
- any claims or loss on account of Intellectual Property rights violation by the IA
- any personal bodily injury or death of any person caused by, arising out of or in connection with its performance of this Agreement; or
- any loss of or physical damage to property of the Authority or any third party caused by, arising out of or in connection with the performance of this Agreement.

2.3.2 The provisions of Article 1.44 shall survive Termination.

2.4 Ownership and Retention of Documents

2.4.1 The Authority shall own the Document(s), prepared by or for IA arising out of or in connection with the Agreement.

2.4.2 Forthwith upon expiry or earlier termination of this Agreement and at any other time on demand by the Authority, IA shall deliver to the Authority all Documents provided by or originating from the Authority and all Documents produced by or for IA in the course of performing the Services, unless otherwise directed in writing by the Authority at no additional cost. IA shall not, without the prior written consent of the Authority store, copy, distribute or retain any such Documents.

2.5 Information Security

2.5.1 IA shall not carry any written/printed document, layout diagrams, compact disk, hard disk, storage tapes, other storage devices or any other goods/material proprietary to Authority into/out of any Project Location without written permission from the Authority.

2.5.2 IA shall not destroy any unwanted documents, defective tapes/media present at any location on their own. All such documents, tapes/media shall be handed over to the Authority.

2.5.3 All documentation and media at any location whether at the Project Location or otherwise, shall be properly identified, labelled and numbered by IA. IA shall keep track of all such items and provide a summary report of these items to the Authority whenever asked for.

2.5.4 Access to Authority's data and systems, internet facility by IA at any location shall be in accordance with the written permission by the Authority. The Authority shall allow IA to use its facilities in a limited manner subject to availability. It is the responsibility of IA to prepare and equip itself in order to meet the requirements of providing the Services.

2.5.5 IA must acknowledge that Authority's business data and other Authority proprietary information or materials, whether developed by Authority or being used by Authority pursuant to a license agreement with a third party (the foregoing collectively referred to herein as "proprietary information") are confidential and proprietary to Authority; and IA along with its team agrees to use reasonable care to safeguard the proprietary information and to prevent the unauthorized use or disclosure thereof, which care shall not be less than reasonable care used by IA to protect its own proprietary information. IA recognizes that the goodwill of Authority depends, among other things, upon IA keeping such proprietary information confidential and that unauthorized disclosure of the same by IA or its team could damage the goodwill of Authority, and shall be considered as a material breach of the Agreement terms and conditions by IA. IA may come into possession of such proprietary information, even though IA does not take any direct part in or furnish the Services performed for the creation of said proprietary information and it shall limit access of such proprietary information thereto only such employees with a need to such access to perform the Services. IA and or its Key Personnel shall use such information only for the purpose of performing the said Services.

2.5.6 IA shall, upon termination of the Agreement for any reason, or upon demand by Authority,

whichever is earlier, return any and all information provided to IA by Authority, which would include any Confidential information or any proprietary information including any copies or reproductions, both hardcopy and electronic of such information.

2.5.7 By virtue of the Agreement, IA team may have access to information of the Authority and/or a third party which would include any Confidential Information or any proprietary information of such parties and will use such information only with prior approval of the Authority on a need only basis and to the extent required for performing the Services.

2.6 Records of Agreement Documents

2.6.1 IA shall at all-time make and keep sufficient copies of the process manuals, operating procedures, specifications, Agreement documents and any other documentation as may be required to fulfil the obligations under the Agreement.

2.7 Security and Safety

2.7.1 IA shall comply with the directions issued from time to time by the Authority and the standards related to the security and safety, in so far as it applies to the provision of the Services.

2.7.2 IA shall upon reasonable request by the Authority, or its nominee(s) participate in regular meetings when safety and information technology security matters are reviewed.

2.8 Confidentiality

2.8.1 IA shall not, either during the Term or after expiration of the Agreement, disclose any proprietary or Confidential Information relating to the Services/Agreement and/or Authority's business/operations, information, application/software, hardware, business data, architecture schematics, designs, storage media and other information/documents without the prior written consent of the Authority.

2.8.2 The Authority reserves the right to adopt legal proceedings, civil or criminal, against IA in relation to a breach of obligation by IA under this Article.

2.8.3 IA shall do everything reasonably possible to preserve the confidentiality of the Confidential Information including execution of a confidentiality agreement with the Authority to the satisfaction of the Authority.

2.8.4 IA shall notify the Authority promptly if it is aware of any unauthorized disclosure of the Confidential Information otherwise than as permitted by the Agreement or with the authority of the Authority.

2.8.5 IA shall be liable to fully recompense the Authority for any loss of revenue arising from breach of confidentiality.

2.9 Events of Default

Events of Default by IA:

2.9.1 In the event that the any of the following events of default shall have occurred, the IA shall be deemed to be in default of the Agreement ("Event of Default"), save and except to the extent that the same is attributable to a Force Majeure Event, which, if not remedied

within the Cure Period upon receipt of Notice of Intention to Terminate from Authority, shall provide Authority the right to terminate this Agreement. The defaults referred to above shall mean the following default of obligations of the IA under the Agreement:

- The IA becomes bankrupt or insolvent.
- The IA is under liquidation.
- The IA assigns the Agreement, or any part thereof otherwise than as permitted under the Agreement or by Authority
- The IA abandons the Agreement.
- The IA persistently disregards the instructions of the Authority, or contravenes any provision of the Agreement.
- The IA does or permits to do any act, matter, deed or thing in violation of Applicable Law and/or Applicable Permits
- The IA fails to maintain insurance (s) as required under the Agreement.
- The IA uses or permits or causes the use of the Site for purposes other than those specified in the Agreement.
- The IA fails to complete the Project within the time specified in the Agreement or within such extensions as granted by the Authority in terms of the Agreement.

2.9.2 IA / IA's Teams failure to confirm/adhere to any of the key performance indicators as laid down in the Key Performance Measures/Service Levels, or if IA has fallen short of matching such standards/benchmarks/targets as the Authority may have designated with respect to the System or any Goods, task or service, necessary for the execution of the Scope of Work and performance of Services under this Agreement. The above-mentioned failure on the part of IA may be in terms of failure to adhere to performance, quality, timelines, specifications, requirements or any other criteria as defined by the Authority.

2.9.3 IA's failure to remedy a defect or failure to perform its obligations in accordance with the Service Specifications as per this RFP or any other specifications issued by the Authority, despite being served with a default notice which laid down the specific deviance on the part of IA/IA's Team to comply with any stipulations or standards as laid down by the Authority

2.9.4 IA / IA's Teams failure to demonstrate or sustain any representation or warranty made by it in the Agreement, with respect to any of the terms of the Bid, the RFP and the Agreement.

Events of Default by Authority:

Each of the following events or circumstances, to the extent not caused by a Force Majeure Event, shall be considered, as Event of Default by Authority which, if not remedied within the Cure Period upon receipt of Notice of Intention to Terminate, shall provide the IA with the right to terminate the Agreement:

- Authority fails to provide to the IA the right of way to the Site within agreed and decided timelines by Authority.
- Authority breaches any obligation which has a Material Adverse Effect on the IA's ability to perform its obligations under the Agreement.

Where there has been an occurrence of such defaults inter alia as stated above, the non-defaulting Party shall issue a notice of default to the defaulting Party, setting out specific defaults /deviances /omissions/ non-compliances/non-performances and providing a notice of Cure Period to enable the defaulting Party to rectify such default committed.

Where despite the issuance of a default notice to defaulting Party, it fails to remedy the default within the 30 days period provided to the satisfaction of the non-defaulting Party, then the non-defaulting Party may proceed to issue a Notice of Intention to Terminate the Agreement forthwith.

2.10 Termination

2.10.1 Without prejudice to any other rights or remedies which the non-defaulting Party may have under the Agreement or under the Applicable Laws, upon the occurrence of either an Event of Default IA or Authority, the defaulting Party shall be liable for the breach caused and consequences thereof and the non-defaulting Party shall have the right to issue a Notice of Intention to Terminate. Upon the issuance of a Notice of Intention to Terminate, the defaulting Party shall have the right to rectify or cure the breach within the Cure Period. If the breach is not rectified by the defaulting Party within the Cure Period, the non-defaulting Party shall have the right to terminate the Agreement by issuance of a Termination Notice.

2.10.2 Termination by Authority

The Authority may, terminate the Agreement in whole or in under the following circumstances:

- Where the Authority is of the opinion that there has been such Event of Default on the part of IA/IA's Team which would make it proper and necessary to terminate the Agreement and may include failure on the part of IA to adhere to any part of its obligations under its Bid, the RFP or under the Agreement.
- Where it comes to the Authority's attention that IA (or IA's Team) is in a position of actual conflict of interest with the interests of the Authority, in relation to any of terms of IA's Bid, the RFP or the Agreement.
- Where IA's ability to survive as an independent corporate entity is threatened or is lost owing to any reason whatsoever, including inter-alia the filing of any bankruptcy proceedings against IA, any failure by IA to pay any of its dues to its creditors, the institution of any winding up proceedings against IA or the happening of any such events that are averse to the commercial viability of IA. In the event of the happening of any events of the above nature, the Authority shall reserve the right to take any steps as are necessary, to ensure the effective transition of the sites, pilot site to a successor agency, and to ensure business continuity.

- Termination for Insolvency: The Authority may at any time terminate the Agreement by giving written notice to IA, without compensation to IA, if IA becomes bankrupt or otherwise insolvent, provided that such termination shall not prejudice or affect any right of action or remedy which has accrued or shall accrue thereafter to the Authority.

2.10.3 Termination by IA

- IA may, subject to written approval by the Authority, terminate the Agreement before the expiry of the Term by giving the Authority a prior and written notice at least 3 (three) months in advance indicating its intention to terminate the Agreement.
- In case of Deliverables / milestone which is approved by the Authority and payment is undisputed, the IA may terminate the Agreement in case of non-payment after 90 (ninety) days of serving the invoice to the Authority.

2.11 Consequences of Termination

2.11.1 In the event of termination of this Agreement, Authority shall pay a Termination Payment to IA as follows after recovering the outstanding dues if any, toward the Authority, any claims for losses/damages suffered by Authority due to any action by the IA or its Subcontractors/ Sub-Lessees:

2.11.2 In the event of Termination before the Appointed Date, no payment shall be paid by the Authority to IA till the date of Termination.

2.11.3 In the event of Termination after the Appointed Date, the Authority shall pay to IA, an amount for goods delivered and services and accepted by the Authority and rendered satisfactorily as per the Payment Schedule, till the date of Termination.

2.11.4 In the event of termination, the Authority shall be entitled to impose any such obligations and conditions and issue any clarifications as may be necessary to ensure an efficient transition and effective business continuity of the Project which IA shall be obliged to comply with and take all available steps to minimize loss resulting from that termination/breach, and further allow and provide all such assistance to the Authority and/or the successor agency/service provider, Replacement Service Provider as may be required, to take over the obligations of IA in relation to the execution/continued execution of the requirements of the Agreement.

2.11.5 Without prejudice to any other rights, the Authority may retain such amounts from the payment due and payable by the Authority to IA as may be required to offset any losses caused to the Authority as a result of any acts of omissions or commission by IA. In case of any loss or damage due to default or inability on the part of IA in performing any of its obligations with regard to executing the Schedule of Requirements under the Agreement, IA shall compensate the Authority for any such loss, damages or other costs, incurred by the Authority.

2.11.6 In case the Agreement is terminated due to Event of Default by IA, Authority shall have the right to invoke the Performance Guarantee.

2.11.7 The termination hereof shall not affect any accrued right or liability of either Party nor affect the operation of the provisions of the Agreement that are expressly or by implication intended to come into or continue in force on or after such termination.

2.11.8 Upon termination or after expiration of Agreement, IA shall forthwith return to the Authority, all papers, material and other properties held by/provided to IA during the Term of the Agreement, including all Confidential Information and proprietary information provided to IA for its use during the Project.

2.12 Miscellaneous

2.12.1 Under this Agreement, the relationship between the Parties is that of independent contractors and no other relationship is intended, including a partnership, franchise, joint venture, agency, employee/employer, fiduciary, master/servant relationship, or other special relationship. Neither Party shall act in a manner, which expresses or implies a relationship other than that of independent contractors, nor bind the other Party. IA and the Sub-contractor shall take care of all liabilities, statutory or otherwise, in relation to persons employed by it or otherwise and the Authority shall not be responsible for the same in any manner whatsoever.

2.12.2 IA or any of its Affiliates shall not directly or indirectly, solicit for employment or engagement any employees of the Authority.

2.12.3 It is also agreed between the Parties that the Authority is under no obligation, whatsoever, to procure Services/execute Works from IA alone. By executing the Agreement, the Authority does not commit/guarantee any minimum number of payments due to IA for the Services/Works performed by IA and holds the right to increase or decrease the Scope of Work provided under the Agreement and in these cases, the Parties shall mutually agree upon any amendment to the charges which are payable to IA for the Works/Services performed.

2.12.4 The Authority reserves the right to propose amendment or modification, of the terms of the Agreement or any part of it by giving IA a notice in writing. No variation, amendment, modification or addition to the Agreement shall be effective or binding on either of the Parties unless set forth in writing and executed by them through their authorized representatives.

2.12.5 The Agreement shall be governed by and construed in accordance with the laws of India. The Parties agree to accept the non-exclusive jurisdiction of the competent in a court of law to which the jurisdiction of the High Court of Odisha Extends

2.12.6 The Agreement sets forth the entire agreement and understanding between the Parties as to the subject matter therein and shall supersede and override all previous communications, negotiations, commitments, agreements, and understandings, either oral or written, between the Parties with respect to the subject matter of the Agreement.

2.13 Notice

2.13.1 Unless otherwise provided herein, all notices or other communications to be given pursuant to the Agreement shall be made in writing, in English and by letter/email (save as otherwise stated) and shall be deemed to be duly given or made, in the case of personal delivery of the letter, when delivered; in the case of email, when sent, or, in the case of a letter, 3 (three) Business Days after being deposited in the post (by registered post, with acknowledgment due), postage prepaid, to such Party at its address or facsimile number specified herein or at such other address or facsimile number as such party may hereafter

specify for such purposes to the other by notice in writing.
The addresses referred to above are:

- In the case of a notice to the Authority:

  Address : [●]

  Attention : [●]

  Telephone : [●]

  Email : [●]

- In the case of the IA

  Address : [●]

  Attention : [●]

  Telephone : [●]

  Email : [●]

2.13.2 A notice or other communication received on a day other than a Business Day, or after business hours in the place of receipt, shall be deemed to be given on the next following Business Day in such place.

2.13.3 The address or email address for serving notices can be changed by any Party by properly serving notices on the other Parties informing them of the changes of address.

2.13.4 In the event that a Party refuses delivery or acceptance of a notice, request or other communication, under the Agreement, it shall be deemed that the notice was given upon proof of the refused delivery, provided the same was sent in the manner specified in the Agreement.

2.13.5 No failure by either party to enforce any rights hereunder shall be construed as a waiver of such right(s).

2.13.6 If any provision of the Agreement is held to be inoperative or unenforceable as applied in any particular case because it conflicts with any other provision hereof or any statute, ordinance, rule of law or public policy, or for any other reason, such holding shall not have the effect of rendering the provision in question inoperative or unenforceable in any other case, or of rendering any other provision herein contained inoperative or unenforceable to any extent whatsoever. The invalidity of any one or more phrases, sentences or Clauses contained in the Agreement shall not affect the remaining portions of the Contractor any part hereof, and they shall otherwise remain in full force and effect.

2.13.7 Neither IA nor its employees or its Subcontractor shall have the right, power, or authority to create any Agreement or obligation, express or implied, on behalf or, in the name of or binding on Authority.

2.13.8 The rights and obligations under the Agreement are personal to IA and shall not be assigned by it, to any third party, without the express prior written authorization of the Authority.

2.14 Change Control Note (CCN)

2.14.1 This applies to and describes the procedure to be followed in the event of any proposed change to Agreement, site Implementation, and Service levels. Such change shall include changes in the scope of services provided by IA and changes to the terms of payment.

2.14.2 Change requests in respect of the Agreement, the site implementation, or the Service levels shall emanate from the Parties' representative who shall be responsible for obtaining approval for the change and who shall act as its sponsor throughout the Change Control Process and shall complete Part A of the CCN (Annex I of this Vol III). CCNs shall be presented to the other Party's representative who shall acknowledge receipt by signature of the authorized representative of the Authority.

2.14.3 IA and the Authority while preparing the CCN, shall consider the change in the context of whether the change is beyond the scope of Services including ancillary and concomitant services required. The CCN shall be applicable for the items which are beyond the stated/implied scope of work as per the RFP document.

2.14.4 IA shall assess the CCN and complete Part B of the CCN. In completing Part B of the CCN IA shall provide as a minimum:

- a description of the change
- a list of Deliverables required for implementing the change.
- a timetable for implementation
- an estimate of any proposed change; or any relevant acceptance criteria
- an assessment of the value of the proposed change
- Material evidence to prove that the proposed change is not already covered within the scope of the RFP, Agreement and Service Levels

2.14.5 Prior to submission of the completed CCN to the Authority or its nominated agencies, IA shall undertake its own internal review of the proposal and obtain all necessary internal approvals. As a part of this internal review process, IA shall consider the materiality of the proposed change in the context of the Agreement, the sites, Service levels affected by the change and the total effect that may arise from implementation of the change.

2.14.6 Each Party shall be responsible for its own costs incurred in the quotation, preparation of CCNs and in the completion of its obligations described in this process provided IA meets the obligations as set in the CCN. In the event IA is unable to meet the obligations as defined in the CCN then the cost of getting it done by third party shall be borne by IA. Change requests and CCNs shall be reported monthly to each Party's representative who shall prioritize and review progress.

3. PART C – Service Levels

3.1 Purpose of Service Levels

The purpose is to define / measure the levels of the Service provided by IA to the Authority for the duration of the Agreement. The benefits of this are:

3.1.1 Implement a process to define Service level parameters or permissible threshold within which IA would be required to perform the Services, and failure of performing the Services by IA within the said acceptable parameters would be considered as a deficiency in Services.

3.1.2 Help the Authority control the levels and performance of IA's Services.

3.1.3 Alert IA to improve its Services and/or remove deficiencies in Services in case the Service Levels agreed between the Authority and IA are breached by IA.

3.2 Service Level Agreements & Targets

3.2.1 The IA agrees and acknowledges that the works and services in relation to the Project are to be performed in strict compliance with the requirements of the Agreement. In the event of the failure of the IA to duly perform the said works and services in accordance with the aforesaid requirements, the IA agrees and acknowledges that it shall be required to pay the corresponding extent of liquidated damages as specified in respect thereto in terms of the Schedules, which amounts, shall be deemed to not be by way of penalty, and shall represent a genuine pre-estimate of the loss and damage occurring to Authority, on account of the relevant non-compliance and/ or failure of the IA.

3.2.2 Provided however that, on or prior to the Appointed Date, the IA shall provide a report to Authority setting out the specific provisions of the scope of the service level standards that it would not be able to comply with, and request for a waiver or relaxation thereto. Authority may, but shall not be obliged to, grant such a waiver or relaxation to the IA. It is clarified that:

- Such waiver or relaxation granted by Authority shall only apply for such time period as may be prescribed by Authority, and upon the expiry of such time period, the obligation of the IA to comply with the requirements of service level standards shall stand reinstated in its entirety; and
- Any such waiver or relaxation shall not extend to any period beyond the Completion Date.

3.2.3 The IA shall, provide to Authority, a fortnightly report, within 5 days of the fortnight, or at such intervals as specified in the Agreement, setting out the extent of its compliance with the aforesaid service level standards, and the remedial action undertaken by the IA in this regard.

3.2.4 This section is agreed to by Authority and IA as the key performance indicator for the Project. This may be reviewed and revised according to the procedures detailed in Article64 (Service Level Change Control).

3.2.5 The following section reflects the measurements to be used to track and report system's

performance on a regular basis. The targets shown in the following tables are for the period of Contact.

3.2.6 The procedures in Article 1.34 shall be used if there is a dispute between Authority and IA on what the permanent targets should be.

3.3 Maintenance Manual

3.3.1 Without prejudice to the other obligations of the IA, the IA agrees and acknowledges that it shall be required to undertake the Operations and Maintenance of the Project, in accordance with certain pre-identified work schedules.

3.3.2 The Maintenance Manual shall be consistent with the requirements of service level standards as laid down in the Agreement, unless a waiver or relaxation is sought and granted by Authority in accordance with Article 56.2 above (whereupon such requirements shall be appropriately deemed to be modified for the relevant approved period). Such Maintenance Manual shall inter alia, provide for the following:

- The mode and manner of carrying out of the O&M of the Project, including specifically the proposed measures of the IA for ensuring compliance requirements of the service level standards.
- The manner of scheduling and deployment of manpower and resources
- Arrangements and procedures for carrying out urgent repairs.
- Criteria and process to be adopted for deciding maintenance needs.
- A cleaning schedule, for cleaning of Project assets and utilities
- An inspection schedule for inspection and examination of the condition, state of repair and operational efficiency of various components of the Project

3.3.3 The aforesaid Maintenance Manual shall, upon being approved by Authority (and subject to the comments of Authority thereon), be binding on the IA, and the O&M of the Project shall be undertaken in accordance with the said approved Maintenance Manual. Provided that approved Maintenance Manual (and the approval thereof by Authority), shall not relieve the IA of its obligation to duly undertake the O&M of the Project as per Applicable Laws and Good Industry Practices, and the other provisions of the Agreement.

3.4 General Principles of Service Level Agreements

The Service Level Agreements have been logically segregated in the following two categories:

Liquidated Damages

The liquidated damages shall come into effect once the notification of Award has been issued by the Purchaser. It would be mainly applicable on the implementation phase of the project.

Service Level Agreements (SLA)

3.4.1. The IA has to comply with service level standards and requirements to ensure adherence to project timelines, quality and availability of services, throughout the period of this O&M period i.e., for a period mentioned in the project timeline of volume II of the RFP. The IA has to supply appropriate software/hardware/automated tools as may be required to monitor and submit reports of all the SLAs mentioned in this section.

3.4.2. SLA would be applicable in operations and maintenance phase of the project. The penalties shall be applicable on monthly payment for Operations & Maintenance period i.e. 10% of contract value for each of respective month. SLA would be applicable on:

- Network Connectivity and Bandwidth Services
- ANPR Cameras
- Analytic Engine
- Data Centre (DC) & Disaster Recovery (DR) Infrastructure
- Parking Management System
- Surveillance System
- Variable Message Display
- AI based video Analytics.
- Contact Centre System/Helpdesk
- Other Systems and components covered under the Scope of Work in Volume II of this RFP.

3.4.3. For purposes of the SLA, the definitions and terms as specified in the Document along with the following terms shall have the meanings set forth below:

- **"Total Time"** - Total number of hours in the month (or the concerned period) being considered for evaluation of SLA performance.
- **"Uptime"** – Time period for which the specified services/outcomes are available in the period being considered for evaluation of SLA. Formulae for calculation of Uptime: Uptime (%) = {1-[(Downtime)/ (Total time- scheduled maintenance time)]} *100
- **"Downtime"** - Time period for which the specified services / components / outcomes are not available in the concerned period, being considered for evaluation of SLA, which would exclude downtime owing to Force Majeure & Reasons beyond control of the successful bidder.
- **"Scheduled Maintenance Time"** - Time period for which the specified services/components with specified technical and service standards are not available due to scheduled maintenance activity. The successful bidder is required to take at least 7 days prior approval from Authority for any such activity. The scheduled maintenance should be carried out during non-peak

hours (like post-midnight and should not be for more than 4 hours. Such planned downtime would be granted once in a month.

- **"Incident"** - Any event/abnormalities in the service being rendered, that may lead to disruption in normal operations and services to the end user.
- **"Response Time"** - Time elapsed from the moment an incident is reported in the Helpdesk over phone or by any applicable mode of communication, to the time when a resource is assigned for the resolution of the same.
- **"Resolution Time"** - Time elapsed from the moment incident is reported to Helpdesk either in person or automatically through system, to the time by which the incident is resolved completely and services as promised are restored.

3.5 Measurement of SLA-

3.5.1. The Service Level parameters defined in this Article shall be monitored on a periodic basis, as per the individual parameter requirements. IA shall be responsible for providing appropriate web based online SLA measurement and monitoring tools for the same. IA shall be expected to take immediate corrective action for any breach in SLA. In case issues are not rectified to the complete satisfaction of Authority, within a reasonable period of time defined in this Agreement, then the Authority shall have the right to take appropriate penalizing actions, or termination of the contract.

3.5.2. Service levels during Implementation phase: During the implementation phase, the performance measurement parameters include timely delivery of the Scope of Work and shall be as under

Definition	**Timely delivery of Deliverables would comprise entire bill of material and the application systems, and as per successful UAT of the same.**
Service Level Requirement	All the Deliverables defined in the Agreement has to be submitted on-time on the date as mentioned in the Agreement with no delay.
Measurement of Service Level Parameter	To be measured in Number of weeks of delay from the timelines mentioned in the section "Project Timelines"
Penalty for non-achievement of SLA Requirement	Any delay in the delivery of the Project Deliverables (solely attributable to vendor) would attract a liquidated damage per week of 1% of the payment to be remitted on successful Go-Live of System i.e. 40% of order value till such time the default continues. If the liquidated damage reaches 10% of the payment to be remitted on successful Go-Live of System i.e. 40% of order value, Authority may invoke termination Article.

3.5.3. Service levels during Operations and Maintenance phase: The performance measurement parameters for assessing performance under SLA during the O&M phase are laid down in Annexure IV. During the O&M phase, a maximum level of performance penalties is established and described in the section.

Service Level	Penalty as a Percentage of Applicable Payment Milestone
9	Event of default and termination respectively, along with forfeiture of Performance Bank Guarantee
8	5%
7	4%
6	2%
5	1%
4	0.5%
3	0.4%
2	0.3%
1	0.2%
0	No penalty

- Performance Penalty for not meeting a measurement parameter for any two months shall result in twice the penalty percentage of that respective measurement parameter for all the three.

3.6 Conditions for No Penalties

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

3.6.1. There is a Force Majeure event effecting the SLA which is beyond the control of the IA. Force Majeure events shall be considered in line with the Article 1.37 mentioned in RFP.

3.6.2. The non-compliance to the SLA has been due to reasons beyond the control of the IA.

3.6.3. Theft cases by default / vandalism would not be considered as "beyond the control of IA". Hence, the IA should be taking adequate anti-theft measures, spares strategy, Insurance as required to maintain the desired Required SLA.

3.7 General Service Level Change Control

3.7.1. It is acknowledged that the Service levels may change as Authority's business needs evolve over the course of the Agreement period.

3.7.2. Any changes to the levels of service provided during the Term of the Agreement shall be requested, documented and negotiated in good faith by both Parties. Either Party can request a change.

3.7.3. Service Level Change Process: The Parties may amend Service Level by mutual agreement. Changes can be proposed by either Party. Unresolved issues shall also be addressed. IA's representative shall maintain and distribute current copies of the Service Level document as directed by Authority. Additional copies of the current Service Levels shall be available at all times to authorized parties.

3.7.4. Version Control / Release Management: All negotiated changes shall require changing the version control number. As appropriate, minor changes may be accumulated for periodic release or for release when a critical threshold of change has occurred.

4. Annexures

4.1 Annexure I: Change Control Note

Change Control Note	**CCN Number:**
Part A: Initiation	
Title	
Originator	
Sponsor	
Date of Initiation	
Details of Proposed Change	
(To include reason for change and appropriate details/specifications. Identify any attachments as A1, A2, and A3 etc.)	
Authorized by Authority	Date
Name	

Signature	
Received by the IA	Date
Name	
Signature	
Change	
Change Control Note	**CCN Number:**
Part B: Evaluation	
(Identify any attachments as B1, B2, and B3 etc.) Changes to Services, payment terms, payment profile, documentation, training, service levels and component working arrangements and any other contractual issue.	
Brief Description of Solution:	
Deliverables:	
Timetable:	
Charges for Implementation:	
Other Relevant Information: (Including value-added and acceptance criteria)	
Authorized by Authority	Date
Name	
Signature	
Change Control Note	**CCN Number:**
Part C: Authority to Proceed	
Implementation of this CCN as submitted in Part A, in accordance with Part B is: (tick as appropriate)	
Approved	
Rejected	

Requires Further Information (as follows, or as Attachment 1 etc.)	
For Authority and its nominated agencies	**For IA**
Signature	Signature
Name	Name
Title	Title
Date	Date

4.2 Annexure II: Form of Agreement

This Agreement (hereinafter "Framework Agreement") made on this _____ day of _____, 2024 BETWEEN Odisha Computer Application Center (hereinafter referred to as the "Authority", which expression shall include its successors and assigns) of the One Part;

AND

_____ (hereinafter referred to as the "IA" which expression shall include its successors and assigns) of the Other Part.

AND WHEREAS, the Authority invited bids for the [Selection of Implementation Agency for RFP for Selection of Implementation Agency for Integrated City Surveillance System at Puri, Odisha].

AND WHEREAS, pursuant to the bid submitted by the IA, vide _____ (here in after referred to as the "Bid or Offer") for the execution of Works, the Authority by its Letter of Acceptance dated _____ accepted the offer submitted by the IA for the execution and completion of such Works as specified in the RFP documents and on the conditions in accordance with the documents listed in para 2 below.

AND WHEREAS, the IA by a deed of undertaking dated _____ has agreed to abide by all the terms of the Bid, including but not limited to the amount quoted for the execution of Agreement, as stated in the Bid, and also to comply with such terms and conditions as may be required from time to time.

AND WHEREAS, pursuant to the Bid submitted by the IA vide _____ (hereinafter referred to as the "the Offer"), the Authority has by its Letter of Acceptance no. _____dated _____ accepted the Offer submitted by the IA for the execution and completion of such Works and the remedying of any defects therein, on terms and conditions of the Framework Agreement;

AND WHEREAS, the IA has agreed to undertake such Works and has furnished Performance Security in form of a Performance Bank Guarantee pursuant to Article 45 of the Agreement.

NOW THIS AGREEMENT WITNESSETH as follows:

1. In this Framework Agreement words and expressions shall have the same meanings as are respectively assigned to them in the conditions of Agreement hereinafter referred to;

2. The following documents shall be deemed to form and be read and constructed as part of this Framework Agreement viz. (a) Complete Request for Proposal (RFP) documents being Volumes I, II and III of the RFP and Corrigendum and addendum, (b) IA's Offer, (c) Letter of Acceptance or Letter of Award OR Letter of Intent issued by the Authority, (d) the acceptance of Letter of Award from IA, (e) Notice to Proceed with the Work, and (f) Any other document listed in the Agreement Data.

3. The foregoing documents shall be constructed as complementary and mutually explanatory one with another. Should any ambiguities or discrepancy be noted then the order of precedence of these documents shall subject to the condition of particular application be as follows:

(a) Complete Request for Proposal (RFP) documents being Volumes I, II and III of the RFP and Corrigendum and addendum,

(b) Framework Agreement,

(c) IA's Offer,

(d) Letter of Acceptance or Letter of Award or Letter of Intent issued by the Authority,

(e) the acceptance of Letter of Award from IA,

(f) Notice to Proceed with the Work, and

(g) Any other document listed in the Agreement Data.

4. In consideration of the payments to be made by the Authority to the IA as hereinafter mentioned, the IA hereby covenants with the Authority to execute and complete the Works and remedy any defects therein in conformity in all respect with the provisions of the Agreement.

5. the Authority hereby covenants to pay the IA in consideration of the execution and completion of the Works and the remedying of defects therein the Agreement price or such other sum as may become payable under the provisions of the Agreement at the times and in the manner prescribed by the Agreement.

IN WITNESS WHEREOF, the Parties here to have caused this Framework Agreement to be executed on the day and year first before written.

For and on behalf of	For and on behalf of
Odisha Computer Application Center	IA (Company Name)
By……..	By……..
Signature	Signature
……..	……..
Print Name	Print Name
……..	……..
Title	Title
Witness……..	Witness……..
Print Name	Print Name
……..	……..

Print Address Print Address

4.3 Annexure III: Non-Disclosure Agreement

This Non-Disclosure Agreement ("Agreement") is made and entered into ___ day of ……., 2024 by and between ……..having its office at _____ (hereinafter referred to as "Authority"')

And

……., having its office at _____ (hereinafter referred to as: Implementation Agency " and/or "IA")

"Authority" and "IA" shall be individually referred to as Party and collectively as Parties to this Agreement.

Whereas, the Parties have entered into an Agreement bearing reference number _____ dated _____ for _____ provision of _____ (hereinafter referred to as 'Agreement'); and

Whereas, during the execution of the Agreement, PARTIES may disclose to each other certain information which is confidential and proprietary in nature and as such they wish to protect such information from unauthorized disclosure and use;

NOW, THEREFORE, in consideration of the foregoing and the covenants and agreements contained herein and, in the Agreement, the Parties agree as follows:

1. **Definitions as used herein:**

(a) The term "Confidential Information" shall include, without limitation, all information and materials, furnished by a Party ("Discloser") to another Party (Recipient) in connection with Government/corporates/citizen/users/persons/customers data, products and/or services, including information transmitted in writing, orally, visually, (e.g. video terminal display) or on magnetic or optical media, and including all proprietary information, customer & prospect lists, trade secrets, trade names or proposed trade names, methods and procedures of operation, commercial or marketing plans, licensed document know-how, ideas, concepts, designs, drawings, flow charts, diagrams, quality manuals, checklists, guidelines, processes, formulae, source code materials, specifications, programs, software packages, codes and other intellectual property relating to such Party's data, computer database, products and/or services. Confidential Information shall also include results of any tests, sample surveys, analytics, data mining exercises or usages etc. carried out by Discloser in connection with the Recipients' or any

government department's / Corporates information including citizen/users/persons/customers personal or sensitive personal information as defined under any law for the time being in force.

(b) The term, "IA" shall include the directors, officers, employees, agents, consultants, contractors and representatives of IA including its affiliates, subsidiary companies and permitted assigns and successors.

2. **Protection of Confidential Information**: With respect to any Confidential Information disclosed by the Discloser to the Recipient or to which any Party has access, both the Parties agree that it shall:

(a) Use the Confidential Information only for accomplishment of the Services to be performed under the Agreement and in accordance with the terms and conditions contained herein;

(b) Maintain the Confidential Information in strict confidence and take all reasonable steps to enforce the confidentiality obligations imposed hereunder, but in no event take less than reasonable care than it takes to protect the confidentiality of its own proprietary and confidential information and that of its clients;

(c) Not make or retain copy of any Confidential Information except as necessary, under prior written permission from other Party in connection with the Services to be performed under the Agreement, and ensure that any such copy is immediately returned to the other Party even without express demand from such Party to do so;

(d) Not disclose or in any way assist or permit the disclosure of any Confidential Information to any person or entity without the express written consent of discloser except as provided in Article 6 below; and

(e) Return to Discloser, or destroy, at Discloser's direction, any and all Confidential Information disclosed in a printed form or other permanent record, or in any other tangible form (including without limitation, all copies, notes, extracts, analyses, studies, summaries, records and reproductions thereof) immediately upon the earlier to occur of:

(i) expiration or termination of the Agreement, or

(ii) on request of Discloser.

(f) Not discuss with any member of public, media, press or any other person about the nature of arrangement entered between the Parties or the nature of services to be provided by the IA to the Authority.

3. **Onus:** Recipient shall have the burden of proving that any disclosure or use inconsistent with the terms and conditions hereof falls within any of the exceptions provided in Article 4 below.

4. **Exceptions:** The obligations of confidentiality as mentioned in this Agreement shall not apply to any information:

(a) Which has become generally available to the public without breach of this Agreement by Recipient; or

(b) Which at the time of disclosure to Recipient was known to Recipient free of confidentiality restriction as evidenced by documentation in Recipient's possession; or

(c) Which either Party agrees in writing is free of such confidentiality restrictions.

5. **Remedies:** The Parties acknowledge and agree that

(a) any actual or threatened unauthorized disclosure or use of the Confidential Information by Recipient would be a breach of this Agreement and may cause immediate and irreparable harm to Discloser;

(b) Damages from such unauthorized disclosure or use may be impossible to measure accurately and injury sustained by Authority may be impossible to calculate and remedy fully. Recipient acknowledges that in the event of such a breach or threatened breach of any provision of this Agreement, Discloser shall be entitled to specific performance by Recipient of Recipient's obligations contained in this Agreement. Recipient shall indemnify, save, hold harmless and defend Discloser promptly upon demand and at its expense, at any given point in time from and against any and all suits, proceedings, actions, demands, losses, claims, damages, liabilities, costs (including reasonable attorney's fees and disbursements) and expenses (collectively "Losses") to which Discloser may become subject to, in so far as such Losses arise out of, in any way relate to, or result from breach of obligations under this Agreement by Recipient . Such Party shall also be entitled, without the requirement of posting a bond or other security, to seek preliminary and final injunctive relief, as well as any and all other applicable remedies at law or equity, including the recovery of damages.

6. **Need to Know:** The Parties shall restrict disclosure of Confidential Information to its employees and/or consultants who have a need to know such information for accomplishment of Services under the Agreement provided such employees and/or consultants have agreed to abide by the terms and conditions of this Agreement and agree that they shall not disclose such Confidential Information to any affiliates, subsidiaries, associates and/or third party without prior written approval of Discloser.

7. **Intellectual Property Rights Protection**: No license to Recipient, under any trademark, patent, copyright, design right, mask work protection right, or any other intellectual property right is either granted or implied by the conveying of Confidential Information to Recipient by the Discloser.

8. **No Conflict:** The Parties represent and warrant that the performance of their obligations hereunder does not and shall not conflict with any other agreement or obligation of the respective Parties to which they are a party or by which the respective Parties are bound.

9. **Authority:** The Parties represent and warrant that they have all necessary authority and power to enter into this Agreement and perform their obligations hereunder.

10. **Governing Law**: This Agreement shall be interpreted in accordance with and governed by the substantive and procedural laws of India and the Parties hereby consent to submit to the exclusive jurisdiction of Courts and/or Forums situated at Puri, Odisha, INDIA only.

11. **Entire Agreement:** This Agreement constitutes the entire understanding and agreement of the Parties, and supersedes all previous or contemporaneous agreement or communications, both oral and written, representations and under standings among the Parties with respect to the subject matter hereof.

12. **Amendments:** No amendment, modification and/or discharge of this Agreement shall be valid or binding on the Parties unless made in writing and signed on behalf of each of the Parties by their respective duly authorized officers or representatives.

13. **Binding Agreement:** This Agreement shall be binding upon and inure to the benefit of the Parties hereto and their respective successors and permitted assigns.

14. **Severability:** It is the intent of the Parties that in case any one or more of the provisions contained in this Agreement shall be held to be invalid or unenforceable in any respect, such provision shall be modified to the extent necessary to render it, as modified, valid and enforceable under Applicable Laws, and such invalidity or unenforceability shall not affect the other provisions of this Agreement.

15. **Waiver:** If either Party should waive any breach of any provision of this Agreement, it shall not thereby be deemed to have waived any preceding or succeeding breach of the same or any other provision hereof.

16. **Survival:** The Parties agree that all of their obligations undertaken herein with respect to Confidential Information received pursuant to this Agreement and obligations of indemnity shall survive for a period of 10 years after any expiration or termination of this Agreement.

17. **Non-solicitation:** During the term of this Agreement and thereafter for a further period of two (2) years post termination/expiry of Term of the Agreement in case the Parties execute the Agreement, the Parties shall not solicit or attempt to solicit each other's employees and/or consultants, for the purpose of hiring/contracting with such employees and/or consultants. In addition, IA shall not proceed to conduct operations/business similar to the Authority with any employee and/or consultant of the Authority who has knowledge of the Confidential Information, without the prior written consent of the Authority. This section will survive irrespective of the fact whether there exists a commercial relationship between IA and Authority.

18. **Term:** This Agreement shall come into force on the date first written above and, subject to aforesaid Article 1.15, shall remain valid up to two (2) years from the expiry or termination of the Agreement.

IN WITNESS HEREOF, and intending to be legally bound, the Parties have executed this Agreement to make it effective from the date and year first written above.

For Authority	For: Implementation Agency(IA)
Name:	Name:
Title:	Title:

WITNESSES:

4.4 Annexure IV: Service Levels

4.4.1 Penalty Clauses

Penalties apply when the SI fails to meet SLA obligations. The penalty framework is structured as per industry standards.

4.4.1.1. Camera Uptime Penalties

For every 1% drop below the SLA uptime:

- **High-Criticality Cameras → ₹1,500 per camera per day**
- **Medium-Critical Cameras → ₹800 per camera per day**
- **Low-Critical Cameras → ₹500 per camera per day**

If uptime drops below 90%, camera is considered "NON-FUNCTIONAL" and full-day penalty applies.

4.4.1.2. ANPR Camera Penalties

- ₹2,000 per camera per day if uptime < 98%

4.4.1.3. Analytics Engine Penalties

If analytics engine uptime < 98% → ₹10,000 per day penalty
If analytics fail to detect events in UAT benchmarking → recalibration

4.4.1.4. Network & ICCC Infrastructure Penalties

Component	Penalty
Core Switch / Storage Unavailability	₹25,000 per hour
VMS Application Downtime	₹10,000 per hour
EMS/NMS Downtime	₹5,000 per hour

4.4.1.5. Manpower Penalties

For each missing resource per shift:

- ₹2,000 per shift (Normal Days)
- ₹5,000 per shift (Rath Yatra Event Period)

4.4.1.6.PM Activity Non-Compliance

If PM is skipped or delayed beyond the defined cycle → ₹5,000 per day per device cluster.

4.4.1.7. Recurring Penalty Escalation Rule If a component violates SLA for three consecutive months:

- SI must replace the device at its own cost, and

- Penalty increases by 50% for next 3 months

4.4.1.8. Maximum Penalty Cap

- Maximum penalty per quarter shall not exceed 10% of quarterly O&M payment.
- If penalty crosses 10% for two consecutive quarters, it constitutes material breach, enabling OCAC to initiate corrective actions, including contract termination.

4.4.1.9. SLA Enforcement & Governance

- SLA performance will be reviewed monthly by OCAC.
- Penalties shall be deducted from the SI's quarterly invoice.
- Repeated violation may result in:
  - Suspension of payments
  - Performance guarantee invocation
  - Contract termination