REQUEST FOR PROPOSALFOR

SELECTION OF SYSTEM INTEGRATOR

FOR INTELLIGENT CITY SURVEILLANCE SYSTEM IN GUWAHATI

ON

DESIGN, SUPPLY, IMPLEMENTATION AND O&M (5-YEARS) BASIS

Volume 2: Scope of Work including Functional and Technical Specification

GUWAHATI SMART CITY LIMITED

Guwahati Smart City Limited,
Guwahati, Assam

Tender Notice No: SPV/GSCL/DEV/214/2023/194

Disclaimer

The information contained in this Request for Proposal (“**RFP**”) document whether subsequently providedto the bidders (“**Bidder/s**”), verbally or in documentary form by Guwahati Smart City Limited (henceforth referred to as “Authority” 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 neither an agreement nor an offer or invitation to any party. The purpose of this document is to provide the Bidders or any other person with information to assist inthe formulation of their Techno- commercial offers (“**Bid**”). This RFP includes statements, which reflect various assumptions and assessments which may be arrived at by the Authority in relation to the project scope. This RFP does not purport to contain all the information which each Bidder may require. This RFP may not be appropriate for all persons, and it is not possible for the Chief Executive Officer, Authority and their employees or advisors to consider the objectives, technical expertise and particular needs of each Bidder. The assumptions, assessments, statements and information contained in the bid documents may not be complete, accurate, adequate or correct. Hence, each Bidder must therefore conduct their own independent analysis of the information contained in the RFP and seek its own professional advice from appropriate sources.

Information provided in this RFP to the Bidder is on a wide range of matters, some of which may depend upon the interpretation of the 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. The authority accepts no responsibility for the accuracy or otherwise for any interpretation of opinion on law expressed herein.

The authority also accepts no liability of any nature whether resulting from negligence or otherwise howsoever caused arising from a 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/modify or supplement the information in this RFP.

This RFP 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 **thereof**.

TABLE OF CONTENTS

1. **Introduction**………11
   1.1. *Introduction to Intelligent City Surveillance Project in Guwahati*……………………………………………11
   1.2. *Project Objectives*………………………………………………………………………………………………11
   1.3. *Strategic Objective of the Project*………………………………………………………………………………12
   1.4. *Project Outcomes & Benefits*…………………………………………………………………………………13
2. **Scope of Work for the Project**……………………………………………………………………………14
   2.1. *Intelligent City Surveillance System*……………………………………………………………………………14
   2.2. *Variable Message Signage* ……………………………………………………………………………………15
   2.3. *Public Announcement and Emergency Call Box*………………………………………………………………15
   2.4. *Geographical Information System (GIS)*………………………………………………………………………15
   2.5. *Integrated Command Control Center for Intelligent Surveillance System*……………………………………16
   2.6. *Key activities under the scope of the SI*………………………………………………………………………16
   2.7. *Operations and Maintenance (O&M) services*…………………………………………………………………23
   2.8. *Convergence*……………………………………………………………………………………………………24
   2.9. *Responsibility Matrix*……………………………………………………………………………………………24
   2.10. *Project Deliverable, Milestones and Timelines*…………………………………………………………………27
3. **Payment Schedule**…………………………………………………………………………………………29
   3.1. *Payment Schedule – Implementation Phase*……………………………………………………………………29
   3.2. *Payment Schedule – Operation & Maintenance Phase*…………………………………………………………30
4. **Solution Overview of Proposed Intelligent City Surveillance System**…………………30
   4.1. *Installation of cameras*…………………………………………………………………………………………30
   4.2. *Installation of Public Address System and Emergency Call Back*……………………………………………30
   4.3. *Installation of Poles*……………………………………………………………………………………………31
   4.4. *Provisioning hardware and software*……………………………………………………………………………31
   4.5. *Connectivity*……………………………………………………………………………………………………32
   4.6. *Site Clearance obligations and other relevant permission*………………………………………………………33
   4.7. *Electrical works and power supply*………………………………………………………………………………33
   4.8. *Civil and Electrical works*………………………………………………………………………………………33
   4.9. *Surge and Lightning-proof measures*……………………………………………………………………………34
   4.10. *Earthing System*………………………………………………………………………………………………34
   4.11. *Junction Box, Poles (Gantries and Cantilever)*…………………………………………………………………34
   4.12. *Cabling Infrastructure*…………………………………………………………………………………………34
   4.13. *Design, Supply, Installation and Commissioning of the Field Equipment*………………………………………35
   4.14. *Cameras*………………………………………………………………………………………………………35
   4.15. *Public Address System*…………………………………………………………………………………………35
   4.16. *Emergency Call Box System*……………………………………………………………………………………36
   4.17. *Design, Supply, Installation, Testing and Commissioning of Network and Backbone Connectivity*…36
   4.18. *Design, Supply, Installation, Testing and Commissioning of ICCC*……………………………………………36
   4.19. *Design, Supply, Installation, Testing and Commissioning of IT Infrastructure for DR over cloud*…………37
   4.20. *Capacity Building and Training*…………………………………………………………………………………38

4.21. *Factory Acceptance Testing (FAT)*……………………………………………………………………………………39
4.22. *Third Party Audit*……39
4.23. *Final Acceptance Testing*………………………………………………………………………………………………40
4.24. *System Documents and User Manuals*………………………………………………………………………………40
4.25. *Operations and Maintenance during contract period*……………………………………………………………..41
4.26. *Project Management and Operation Maintenance*…………………………………………………………………..41
4.27. *Indicative resource requirement*……………………………………………………………………………………41
4.28. *Hand-over of the system before contract expiry*………………………………………………………………43
4.29. *Other requirements*…………………………………………………………………………………………………..43
4.30. *Video Analytics for the project*…………………………………………………………………………………….43

5. **Intelligent City Surveillance System – Functional Requirement & Technical Specifications……………………………………………………………………………………**44

5.1. *Camera Specification*……………………………………………………………………………………………………44
5.2. *IP Public Address System Specification*……………………………………………………………………………48
5.3. *Emergency Call Box Specification*…………………………………………………………………………………..49
5.4. *Video Monitoring, Recording & Management software*……………………………………………………………..50
5.5. *Technical Specifications of AI Based Video Intelligence Platform*………………………………………………..60
5.6. *VMD (Variable Messaging Display)*…………………………………………………………………………………79
5.7. *Environmental Monitoring Sensors*…………………………………………………………………………………83
5.8. ***Uninterrupted Power Supply (UPS)*……………………………………………………………………………87**
5.9. ***DG- 180 KVA Silent DG Set with AMF Panel*…………………………………………………………………..94**
5.10. *Integrated Command and Control Centre (ICCC)*…………………………………………………………………98
5.11. ***Enterprise Management System*……………………………………………………………………………….124**
5.12. ***Video wall*………………………………………………………………………………………………………132**
5.13. ***IP-PBX System*………………………………………………………………………………………………..134**
5.14. ***Industrial Grade Switch*……………………………………………………………………………………….148**
5.15. *Internet Router & Core Router*……………………………………………………………………………………..150
5.16. *24 Port L3 Switch (fully loaded)*……………………………………………………………………………………151
5.17. *24 Port Distribution Switch (Fully Loaded Non PoE)*………………………………………………………………..152
5.18. *24 Port PoE Switch*……………………………………………………………………………………………………153
5.19. *SAN Switch*………154
5.20. *SAN Storage*……155
5.21. *Backup Software*……………………………………………………………………………………………………..156
5.22. *Server Load Balancer*………………………………………………………………………………………………157
5.23. *Servers*……157
5.24. *Server for Video Analytics*…………………………………………………………………………………………..158
5.25. *KVM Module*……159

5.26. *Rapid Deployable System………..160*

5.27. *24 Port Copper Patch Panel, fully loaded……………………………………………………………………………………….162*

5.28. *40 MM HDPE Duct……..162*

5.29. *Specifications for Passive Components……………………………………………………………………………………….163*

5.30. *Rack with Fire Suppression System…………………………………………………………………………………………..168*

5.31. *Pole For CCTV Camera……..168*

5.32. *Next Generation Perimeter Firewall…………………………………………………………………………………………169*

5.33. *Next Generation Core Firewall……………………………………………………………………………………………………175*

5.34. *Next Generation Firewall for Viewing Station……………………………………………………………………………179*

5.35. *Zero Day Network Threat Protection System…………………………………………………………………………….183*

5.36. *Next Generation Anti-Virus and Endpoint Detection & Response………………………………………………….186*

5.37. *Privileged Access Management Solution…………………………………………………………………………………189*

5.38. *Security Information & Event Management(SIEM)……………………………………………………………………200*

5.39. *Threat Intelligence Management …………………………………………………………………………………………….204*

5.40. *VAPT Certification & STQC Audit for DC for every year……………………………………………………………..206*

5.41. *Integrated Command and Control Center(ICCC) Room Interior …………………………………………………..207*

5.42. *Safety and Security System for Integrated Command and Control Center (ICCC)…………………………..214*

5.43. Cloud Service (DR)……216

5.44. Geographical Information Systems (GIS)…………………………………………………………………………………226

5.45. Estimated MPLS network Plan and bandwidth requirement…………………………………………………………235

6. Bill Of Material(BoM)**…………………………………………………………………………………………………**236

7. Location details ……236

Glossary

Terms	Meaning
ANPR	Automatic Number Plate Recognition
AP	Access Points
ATCS	Adaptive Control System
AVLS	Automated Vehicle Locator System
BOM/BOQ	Bill of Material/Bill of Quantity
BQS	Bus Queue Shelters
CCHS	Central Clearing House solution
CCTV	Closed Circuit Television
CCC	Command and Control Centre
CONOPS	Concept of Operations
COP	Common Operating Platform
CSP	Cloud Service Provider
DBA	Database Administrator
DC	Data Centre
DNS	Domain Name Server
DR	Disaster Recovery
DRC	Disaster Recovery Centre
EMD	Earnest Money Deposit
EMS	Enterprise Management System
ETA	Estimated Time of Arrival
ETD	Estimated Time of Departure
ETM	Electronic Ticketing Machine

E-Procurement Portal	Means electronic tendering system of Authority
FMS	Facility Management Services
FRS	Functional RequirementSpecifications
GIS	Geographical InformationSystems
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communication
GUI	Graphical User Interface
IaaS	Infrastructure as a Service
IMS	Infrastructure Management System
HDPE	High-Density Polyethylene
HO	Head Office
ICCC	Integrated Command and Control Centre
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IMS	Infrastructure Management System
IOE	Internet of Everything
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
ITIL	Information Technology Infrastructure Library
LAN	Local Area Network

LOI	Letter of Intent
LOA	Letter of Award
KPI	Key Performance Indicator
MCC	Mobile Command Centre
MeitY	Ministry of Electronics & Information and Technology
MLCP	Multi-Level Car Parking
MoHUA	Ministry of Housing & Urban Affairs
MoU	Memorandum of Understanding
MPLS	Multi-Protocol Label Switching
MTBF	Mean Time Between Failure
MTTR	Mean Time to Repair
NFC	Near Field Communication
NIC	National Informatics Centre
ONVIF	Open Network Video Interface Forum
O&M	Operations and Maintenance
OEM	Original Equipment Manufacturer
OFC	Optical Fibre Cable
OGC	Open Geospatial Consortium
OS	Operating System
OTP	One Time Password
OWASP	Open Web Application Security Project
PaaS	Platform as a Service
PKI	Public Key Infrastructure

PIS	Public Information System
PA System	Public Address System
PDUs	Power Distribution Units
PIS	Passenger Information System
PMC	Project Management Consultant
PoE	Power over Ethernet
PoP	Point of Presence
PTZ	Pan Tilt Zoom
QR Code	Quick Response Code
RF	Radio Frequency
RFID	Radio Frequency Identification
RFP	Request for Proposal
RLVD	Red Light Violation Detection
RoW	Right of Way
RTO	Recovery Time Objective
RPO	Recovery Point Objective
SaaS	Software as a Service
SCADA	Supervisory control and data acquisition
SCM	Smart Cities Mission
SDWAN	Software Defined Wide Area Network
SI	System Integrator
SLA	Service Level Agreement
SMPS	Switched Mode Power Supply

SMS	Short Message Service
SNMP	Simple Network Management Protocol
SOP	Standard Operating Procedures
SOS	Save Our Souls. SOS is International Morse code distress signal
SRS	System Requirement Study
TPA	Third Party Auditor
TRAI	Telecom Regulatory Authority of India
TRS	Technical Requirement Specifications
TSP	Telecom Service Provider
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
VMS	Video Management Software/System
WAN	Wide Area Network
GMC	Guwahati Municipal Corporation
Authority	Guwahati Smart City Limited

1. Introduction

1.1 Introduction to Intelligent City Surveillance Project in Guwahati

Guwahati has incorporated a special purpose vehicle (SPV) – Guwahati Smart City Limited (GSCL) (the 'Authority') to plan, design, implement, co-ordinate and monitor the smart city projects in Guwahati. GSCL is a company incorporated under Indian Companies Act 2013 with equal shareholding from Govt. of Assam. The city being gateway to the North East India, has been facing several issues across the city for which proper surveillance is required.

The SPV is introducing ICT based applications as per an action plan to monitor and manage the city and improve its efficiency, by providing better maintenance and public delivery services. As part of this plan, the Intelligent City Surveillance Project will ensure a safe and secure environment and also help in urban planning.

1.2 Project Objectives

One of the key objectives of GSCL is to promote a better quality of life for residents by enhancing the safety & security and improving the efficiency of services. In order to achieve this objective, GSCL desires to foster the development of a robust ICT infrastructure that supports digital applications and ensures seamless steady operations.

This project aims to converge multiple types of camera feeds to a centralized point, which is the Intelligent Command and Control Room and co-located Data Center and DR in Private Cloud. Fixed Box, PTZ, and ANPR cameras and other Smart City elements like Emergency Call Box (ECB), Public Announcement System (PA) , Environmental Sensor and Visual Message Display System (VMD) will be deployed across Guwahati to enhance women, child, and elderly safety. The camera feeds will travel from the source to the destination via MPLS connectivity, with the SI being responsible for network backbone and last mile connectivity through an Internet Service Provider. The Data Center will have Tier III provisions and High Availability measures for IT and Non-IT components. The success of this project will be driven by Video Analytics using AI and ML methodologies. The MSI must write and execute well-considered SoPs and workflows of all the use-cases to ensure project success and a sustainable, scalable system. The implemented platform will be used to leverage video feeds from other schemes, so data lake formulations and approaches must be clearly defined. The project implementation must be time-bound and professional to meet all the outlined objectives.

The vision of the project is to implement a citizen friendly, holistic, integrated and responsive Intelligent City Surveillance System to achieve the following objectives:

1.2.1 **Safety Improvement:** Real-time safety management, and intelligent surveillance can help prevent criminal activities and also respond to potentially dangerous situations in advance. Further, city surveillance will improve women's safety by providing a constant monitoring and alert system, deterring potential offenders, and aiding in the identification and prosecution of perpetrators, promoting a safer and more secure environment for citizens, especially women.

1.2.2 **Higher Productivity:** Achieving improvement in productivity, logistics and other economic activities by obtaining precise real-time information in key areas of the city through video surveillance system.

1.2.3 **Enforcement:** Law enforcement is improved through continued monitoring of the city, specifically at crowded areas and aids in detection of criminal activity, enabling timely response and investigation through the use of video analytics.

1.2.4 **Effective & Preventive Policing:** Geographical Information System (GIS) combined with city surveillance can enhance preventive policing by identifying crime hotspots, tracking criminal activity patterns, and enabling targeted resource deployment.

1.2.5 **Event Tracking and Real Time Information:** The real-time information at the Integrated Command and Control Center (CCC) from Cameras, Environmental Sensors and other technology interventions like GIS shall enable the operator to take necessary actions based on the type of information and send out emergency notifications through Variable Message Signages or inform other urban bodies as per set SOPs.

1.2.6 **Integration with existing Traffic Management System:** Video and analytic data from traffic management system will further strengthen the effectiveness of the city surveillance system for real time policing as well as help to identify trends and patterns, which can inform city planning and infrastructure improvements.

With this RFP, GSCL intends to set-up an Intelligent City Surveillance System through a process of competitive bidding for selecting a System Integrator (SI)/ Implementation Agency (IA) for Supply, Installation, Testing, Commissioning and Five (5) years of operations and maintenance. The selected SI shall have the overall responsibility to design, build, implement, operate, and maintain the CCC from the date of Go-Live / successful commissioning of the Intelligent City Surveillance Project. Overall, the selected System Integrator (SI) will be responsible for designing, deliver and maintain a sustainable, productive, scalable and reliable system for the benefit of citizens of Guwahati.

1.3 Strategic Objective of the Project

The system is to be designed taking into consideration the future scalability and integration with upcoming systems. The system should help to meet the following strategic objectives:

1. Safety and Security
2. Improved Responsiveness
3. Effective Policing
4. Improved Management

1	Safety and Security	● Live Monitoring and control of movement of Crowd at Important locations of the city including entry and exit points ● Live alerts in case of an event/ incident ● Help to identify, apprehend and prosecute offenders ● Monitoring of suspicious activity, vehicles, objects etc. with respect to protecting life & property

2	Improved Responsiveness	● Access to Police by the Citizens for quick and effective response, improved visibility and transparency ● Provide assistance to emergency services and faster turn-around time
3	Effective Policing	● Assist in management and policing of large-scale events ● Aid to investigation by Police Department by integration of analytic tools ● Providing evidence for criminal and civil action in the courts
4	Improved Management	● Help in maintaining Law & Order situations ● Help in improving the administration work

1.4 Project Outcomes & Benefits

The project once implemented shall benefit all the stakeholders. The envisaged key benefits to the City Administration and Citizen are as under:

City Administration	● The implementation of Intelligent City Surveillance System in Guwahati will ensure safety and crowd surveillance. ● The central command and control will ensure efficient continued working of the field equipment ● Continuous surveillance would help in reduction in number of criminal and unlawful activities, unnecessary gathering, women safety. ● Prompt emergency response in cases of accidents, fires, disasters, epidemics, etc. due to availability of real time data and response mechanisms ● To lower the costs by adopting a centralized architecture, enabling the platform to be administered and supported from one location ● Instant MIS reports for planning, budgeting, monitoring & evaluation ● Instant identification of delay points enabling prompt administrative action ● Facilitate cross-department collaboration with the help of online systems in compliance with various standard operating procedures will bring transparency in city administration
Citizen	● Increased public safety through crime prevention and quicker incident response ● Enhanced accountability of public officials and citizens ● Deterrence of criminal activity due to the visible presence of surveillance cameras, especially increased safety of citizens, especially women ● Protection of critical infrastructure, such as airports and railway stations, from potential terrorist attacks and other threats ● Better management of public spaces, such as parks and markets, through real-time monitoring and response ● Improved emergency response capabilities through better situational awareness and coordination ● Reduced public disorder and nuisance behavior, such as littering and public urination, through the fear of being monitored ● Increased trust between citizens and law enforcement due to the perception of improved safety and security ● The potential to use surveillance data for urban planning and decision-making

2. Scope of Work for the Project

The SI's scope of work shall include but is not limited to the following broad areas. Details of each of these broad areas have also been outlined in subsequent sections of this document. The project will be implemented throughout the city of Guwahati. The list of places along with detailed indicative BoQ is mentioned in subsequent section (Ref Sec. 6) of this volume of RFP.

The SI shall deploy the team based out of Guwahati proposed for the project upon signing of the agreement and ensure that a Project Inception Report and Detailed Engineering Report are submitted to Authority as per the schedule in the subsequent section of this tender document, 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 SI anticipates and the plans they have towards their mitigation
- Detailed project plan specifying dependencies between various project activities/ sub-activities and their timelines
- Any other items specified in subsequent sections of this tender document

The SI shall conduct a comprehensive As-Is study of existing infrastructure, systems and associated processes in the city in line with project requirement.

The below ILLUSTRATIVE EXAMPLE explains various aspects to be considered during AS-IS study.

The existing infrastructure study of junctions/intersections to be done during various time periods of day including peak and non-peak hours to establish the key performance indicators (KPI) for the Intelligent City Surveillance System.

The report shall also include the expected measurable improvements against each KPI as well as use cases to be implemented under INTELLIGENT CITY SURVEILLANCE SYSTEM, once the command & control centre is commissioned. The benchmarking data should also be developed to track current situation and desired state.

Additionally, the SI 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 modeling 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)
- KPI design for the Video wall to visualize important events on real time

SI shall implement and deliver the following modules:

2.1 Intelligent City Surveillance System

The City Surveillance System will improve the livability of Guwahati by enhancing public safety, reducing crime rates, and promoting efficient resource allocation. It will enable the authorities to monitor public areas and respond quickly to any potential safety or security threats. It will help in creating a safe and secure environment for residents, reducing crime rates, and increasing their quality of life. The data collected by the surveillance system can be used to make informed decisions about resource allocation, such as transportation, energy, and waste management, improving the overall efficiency of the city. Overall, a city surveillance system can significantly contribute to creating a livable and sustainable urban environment.

By analyzing the data collected by surveillance cameras, AI algorithms will identify patterns, anomalies, and potential threats that might be missed by human operators. This will help to improve the speed and accuracy of threat detection, enabling the authorities to respond quickly and effectively. Analytics will be used to analyze data from multiple sources, such as social media or weather forecasts, providing additional context and insights that can be used for informed decision-making.

Facial Recognition technology can help identify suspects in real-time, enabling the authorities to respond quickly to potential threats. Crowd Estimation can monitor large gatherings and detect potential safety concerns, while Abandoned Object Detection can identify unattended bags or packages that might pose a threat. Person Collapsing can identify people who have collapsed or are in distress, alerting emergency responders. Stray Animal Detection can identify animals in urban areas, improving animal control efforts. Vandalism detection can help authorities prevent property damage and maintain a clean city. Women's safety analytics can help authorities prevent harassment or violence against women. Encroachment Detection can identify violations of public spaces and rights-of-way, enabling authorities to enforce regulations. People Fighting analytics can detect fights in public areas, enabling authorities to quickly intervene and restore order. Perimeter Protection can monitor city boundaries or specific locations, detecting any breaches or intrusions. Overall, these analytics can help authorities detect potential safety threats, allocate resources more efficiently, and maintain a safer and more secure urban environment.

2.2 Variable Message Signage

Messages, Announcements and Public Awareness Messages should display on Variable Message Signages located at different locations in city and controlled from the Integrated Command and Control Center (ICCC). Real-time information can be shared with motorists about traffic conditions, accidents, and road closures, enabling better traffic management and reduced congestion. Additionally, VMS can be used to display emergency alerts and public safety messages, providing critical information to residents and visitors. VMS can be used for public outreach campaigns and promoting civic engagement. Real-time environmental data from the sensors installed across the city will also be shared through the signages. VMS will play an essential role in improving the efficiency, safety, and overall livability of a city.

2.3 Public Announcement and Emergency Call Box

Emergency notifications, Announcements and Public Awareness Messages will be announced via Public Address system located at different locations in city. PA Systems integrated with Emergency Call Boxes enable effective communication with the public during emergencies or critical situations, such as natural disasters. The PA system can be used to broadcast emergency announcements, warnings, and evacuation instructions to a large audience quickly.

Integrating the PA system with ECBs can enable direct communication between the public and emergency response teams, allowing for more rapid and effective response to incidents. The ECBs can also be used to summon medical or law enforcement assistance in case of emergencies, providing a critical lifeline for those in need. PA system can be used for public service announcements, traffic updates, and other informational messages, providing residents and visitors with real-time information that can improve their safety and quality of life.

2.4 Geographical Information System (GIS)

GIS platform integrated with a city surveillance system will provide significant benefits to the security of Guwahati. By leveraging GIS technology, the system will gain a comprehensive understanding of the city's physical layout and infrastructure, allowing security operators to quickly respond to incidents and emergencies. The integration of GIS layers, such as camera positioning, building structures, and utility resources, can provide real-time, actionable intelligence to operators during an incident. The GIS platform can also be used to monitor and analyze crime patterns and hotspots, allowing for proactive and preventative measures to be taken.

The single integrated , deployed GIS platform will be able to do Image feature extraction, geoprocessing, image mosaicking, sub setting, classification (supervised, unsupervised) change detection, AI/ML based object Detection components , 3D , network analysis, SAR based processing and analysis, Photogrammetry, Terrain analysis.

2.5 Integrated Command Control Center for Intelligent Surveillance System

Guwahati has envisaged to develop state of the Art Integrated Command and Control Center (ICCC) to enable city administrators including Guwahati Police and other administrative bodies for real time monitoring of the various facets of management of Guwahati City and its related components. Integrated Command and Control Center (ICCC) will be the heart of this project, where the overall monitoring and control of major functions of the data / communication network resides.

While the information gathered at ICCC can rapidly be shared across various agency lines to accelerate problem response and improve better coordination. Furthermore, the ICCC will help in anticipating the challenges and minimizing the impact of disruptions on city road / Junctions. The scope of the project includes implementation of ICCC at location identified by GSCL.

SI has to provide edge devices, network connectivity, application softwares and other required components. Compute and storage components of the solution shall be housed at the co-located Data Center. The DR will be on cloud to ensure high reliability of the system. The SI will make all the arrangements related to its safety and security.

All the services related to ICT components of Intelligent City Surveillance System project such as Cameras, Public Address System, Emergency Call Back System, IPPBX etc. and any future ICT initiatives which will act either as upstream or downstream interfaces to the Integrated Operations Platform. Feed from all these field devises will be monitored and controlled from ICCC. ICCC will be the single platform from where all decision making shall be done.

This platform should be compatible and integrable with the National Informatics Centre (NIC) portal and infrastructure. The data and analytics generated by the system should be accessible through both web and mobile applications. These applications should provide both textual and graphical information enabling a comprehensive understanding of the surveillance data.

2.6 Key activities under the scope of the SI

- CONOPS (Concept of Operations)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.
- Training- general awareness, Use cases, SoP management, governance, Command & Control Centre operation, System maintenance.
- Business Process Reengineering and KPIs for the selected applications/ services
- UAT & Go-live
- Capacity Building
- Operation & Maintenance (O&M) for 05 Years from Go-live date
- STQC Certification and system audit
- **Cyber Security audit and compliance**

MSI's key responsibilities under the Scope of Work

The summary of MSI responsibilities is as follows:

- **Initiation and Planning for each Phase**

a. Define Project Implementation Plan as per phased approach.

b. Conducting site survey, obtaining necessary permissions, developing systemrequirements, standard operating procedures, etc.

c. Finalization of exact locations of the Cameras, Junction Boxes, Pole, Power Metres atdifferent junctions

d. Finalization and submission of a detailed scalable & secured technical architecture and submission of detailed project plan which includes

  - Deployment of the Team, Project Manager, Their Roles & Responsibility
  - Responsibility Matrix of the stakeholders
  - Approach & Methodology to be adopted

e. Risk & Its mitigation

f. Detailed project Plan, Specifying dependencies between various projects activities/Sub activities, Coordination with Civic agencies, & The timeline of the project

g. Quality Management plan

h. Communication Plan

i. Stakeholder management plan

j. Finalize the detailed Technical Architecture in coordination with ISP, Coordination & Execution Plan for seamless Integration

k. Design the LAN connectivity diagrams for approx. 800 Locations from each Junction Box to Pole, From Power Meter to Junction Box & Prepare the Implementation plan in coordination with ISP

l. Design the Architecture, Concept of Operations for ICCC, Datacenter and DR on cloud and prepare the 3D Diagrams, DC Floor Strengthening Plan.

m. Assessment of IT Infrastructure and Non-IT Infrastructure requirements, assessment of business processes, assessment of software requirements, assessment of integration requirements, assessment of connectivity requirement all locations (including buildings).

n. MSI will adopt latest finishing items and construction materials so that better finish and quality is achieved at reasonable cost.

o. Formulation of solution architecture, detailed design of safe citysolutions, development of test cases (Unit, System Integration and User Acceptance),
SoP documentation

p. Finalization of Bill of Material for the DC, ICCC and DR on cloud

q. Finalization of Bill of Material of Cameras, UPS, Field Switches, ECB, PA system, Rapid deployable Surveillance system and Environmental Sensor etc.

r. Finalization of Bill of Material of Application Softwares

s. Prepare the Approach & Methodology document for Integration

t. Plan to Integrate Community Surveillance & Existing Cameras in other projects

u. Inventory management for all items/ equipment, software, licenses, Warranty, CAMC Certificates, etc.

v. MSI shall ensure that system confirms technical specifications, however, equipment/items of better version may be acceptable.

w. Any other, meeting the RFP requirement.

- **Implementation**

a. Phase-wise time bound procurement and implementation.

b. Obtain all necessary Legal/Statuary Clearance for Installing Poles & Junction Boxes

c. Provisioning for Electricity

d. Develop, Deploy, Test & Commission the surveillance system

e. Supply, Install & Configure all User Level Components (Active & Passive)

f. Installation of on-premises DC and DR on Cloud

g. Supply & Installation of Rapid deployable Surveillance System

h. Installation of Video wall, Workstations, LEDs, UPS, etc.

i. Project Implementation & Phase wise Planning

j. Physical Setup of ICCC as per the layout approved.

k. Helpdesk setup, procurement of equipment, edge devices, COTS software (if any), licenses. Physical Security and Housekeeping setup

l. IT and Non-IT Infrastructure installation, development, testing and production environment setup

m. Safety and security of IT and Non-IT Infrastructure

n. Establishment and configuration of Network Connectivity in coordination with ISP contracted by MSI

o. Software Application customization (if any), development of bespoke solution (if any), data migration, integration with third party services/application (if any) User Manuals, training curriculum and training materials Role-based training(s)

p. Preparation of Standard Operating Procedures (SOPs) for operation of the system andto ensure implementation/ operation of the system as per SOPs

q. SOP preparation in consultation with GSCL, implementation, Integration with GIS Platform, Integration of solutions with Command and Control Center, KPI Development. SOP needs to be approved by GSCL

r. Information Security Policy, Backup Policies

s. Portal to monitor project activities.

t. Training to GSCL / Police Officials

u. Testing Phase

  - Unit & Integration Testing
  - End to End Testing
  - Regression Benchmarking Testing
  - User Acceptance Testing

v. UAT and Phase Wise Go-Live

w. Final Acceptance Test & GO Live

x. Submission of System Documents, User Documents

  - Project Commencement Documentation
  - Equipment Manual
  - Training Manual
  - Installation Manual
  - User Manual
  - System Manual
  - Standard Operational Procedure (SOP) Manual, Business plan and Sustainable system designing Manual

y. Testing Phase

  - Unit & Integration Testing
  - End to End Testing
  - User Acceptance Testing
  - Roll Out

z. Facilitating UAT and conducting the prelaunch security audit of applications.

aa. Integration of the various services & solution with ICCC platform Develop provisionsfor a scalable system

bb. MSI shall furnish a progress report periodically (monthly) of project activities etc. indicating date of start, date of completion and progress made till the date of report (approximate percentage of work done).

cc. MSI will ensure that safety code, as per applicable laws, including health and sanitary arrangement for the deployed staff/personnel, has been complied with.

dd. MSI shall maintain a site order book and inspection book containing the details of orders issued at site and their compliance. The same shall be opened for checking by TSP or any agency authorized by GSCL or GSCL itself.

ee. Any other, meeting the RFP requirement.

ff. Responsibility towards ISP work handshake:

  - Marking of the final pole locations at the junctions
  - Power availability & MCB 16amp on junction box for ISP's network devices

- Power meter & power cable availability
- Providing Multiple switch strip inside the junction Box
- Outdoor IP65/66/67 junction box with 5 years warranty and support
- Making of platform for the pole and pole installation
- Approval of designs from customer and civic bodies
- Space inside the junction box with the gap of 1U between the devices.
- Hot air exhaust and cooling system inside the junction box
- MSI should design the junction box to block the dust & External Particles
- Regular preventive maintenance of the junction boxes which involvesmaintenance of basic hygiene
- Chemical earthling availability and maintenance
- UPS power with 1 hour battery backup for all installed devices
- Connectivity between camera and switch
- Connectivity between switch & MUX/router
- Providing High security lock system in junction boxes to ensure the safety andsecurity of the devices
- Lightening arrester with GI strip
- Providing access for the ISP team at each junction/pole & DC/DR location
- Supporting and coordinating with the ISP in facilitating ROW/Digging andnetwork extension
- permissions from different authorities
- Warning signboards at each junction point
- Acrylic Board mentioning this area in surveillance
- Cross connect availability in DC & DR locations and other if applicable
- Providing safety & security at the junction locations
- Ensuring no access to trespasser or any other than the authorized person at thejunction
- locations
- Providing cable conduit with in junction box
- First Level Troubleshooting needs to be done by the MSI engineer
- Electrician if required at all locations must be arranged by the MSI.

Post Implementation (Operation & Maintenance)

a. Deploying manpower Security of ICCC premises Annual technical support

b. Preventive, repair maintenance and replacement of hardware and software components

c. Provide a centralized Help Desk and Incident Management Support till the end of contractual period Recurring refresher trainings for the users and Change Management activities

d. Provide required access and information for Audits

e. Preventive, repair maintenance and replacement of non-ICT components

f. Overall maintenance of the ICCC facility and continuity of operations as per SLAs.

g. Monitoring of Network Connectivity (provided by service provider) as per servicelevel and report the non- compliance.

h. Submit Quarterly Reports

i. Adhere to defined SLAs

j. Any other, meeting the RFP requirement.

k. Setting up the Help Desk for O&M

l. Manpower Deployment for O&M Phase

m. Preparing the Document and Reporting Mechanism

n. Completing the documentation of Warranty, License & Agreement

o. Pent scanning & Network Dressing & Internal Audit

p. Third Party Administrator (TPA)

q. Security & Network Audit - Format & SOPs

r. Helpdesk Management

s. Reporting & Dashboards

t. SLA Management - ISP & MSI

u. Setting up Governance Team

v. Exit Management

w. Closure of the contract

Note: Any additional item/hardware/software/services etc. required for successful completion and operation of the system shall be provided by the MSI, without any additionalcost to the project.

- **Support and warranty:**

Operations and Maintenance phase will require technical support and comprehensive warranty on 24*7 *365 basis for all hardware and software parts as envisaged in the project.A comprehensive warranty applicable on goods supplied under this contract shall be provided for the period mentioned in the document.

The MSI has to ensure comprehensive maintenance with OEM warranty and the AMC for all the component items under this project. The electronic/ online warranty of the items is a criterion wherein the OEM has to officially email the adherence of the warranty terms for thedefined time period with GSCL and the MSI. It will be the prime responsibility of the MSI to ensure seamless and uninterrupted functioning of the system with all compliances asper project requirements and thereby regulate the OEM(s) accordingly.

- **Standards of Performance**

The MSI shall provide the services and carry out their obligations under the Contract with due diligence, efficiency and professionalism/ethics in accordance with generally accepted professional standards and practices. The MSI shall always act in respect of any matter relating to this contract. The MSI shall abide by all the provisions/Acts/Rules/Regulations, Standing orders, etc. of Information Technology and other relevant legality as prevalent in the country. The MSI shall also ensure to maintain the standards laid down by User department from time to time for carrying out work in office or at public places.

The MSI will ensure that there is no damage caused to any private or public property in execution of work in field. In case such damage is caused, MSI shall immediately bring it to the notice of GSCL office in writing and MSI will pay necessary charges towards fixing of the damage. GSCL instructs MSI that no traffic congestion/public inconvenience is caused while carrying out work at public places.

The MSI shall ensure that its employees/representatives or the agencies hired by them to carry out the contract don't breach privacy of any citizen or establishment during the course of execution or maintenance of the project.

- **Deployment of adequate Key Personnel and support Staff by MSI**

It is very crucial for MSI to deploy adequate required manpower for the time bound successof project implementation along with sufficient helpdesk, Technical Support, training and facility staff to bring efficient outcomes of the system operability.

The deployment of man-power must not come out as an inefficient and adversely impactingparameter towards the project success. GSCL reserves the rights to ask for immediate replacement of the deployed man-power with regards to the inefficient performance as per the requirement of the project. Inefficient performance may attract termination of the contract.

Key Personnel shift to Scope of Requirement

a. Initial Composition; Full Time Obligation; Continuity of Personnel

Bidder shall ensure that each member of the Key Personnel devotes substantial working timeas per the staffing schedule/ manpower plan to perform the services to which that person has been assigned as per the Bid.

Bidder shall not make any changes to the composition of the Key Personnel and not requireor request any member of the Key Personnel to cease or reduce his or her involvement in theprovision of the Services during the defined term of the engagement unless that person resigns, is terminated for cause, is long-term disabled, is on permitted mandatory leave under Applicable Laws or retires. In any such case, GSCL's prior written consent would be mandatory.

b. Evaluations of Personnel

Bidder shall carry out an evaluation of the performance of each member of the Key Personnel in connection with the Services at least once in each Contract Year. Bidder shall provide reasonable written notice to GSCL of the date of each evaluation of each member of the KeyPersonnel. GSCL shall be entitled to provide inputs to the Bidder for each such evaluation. Bidder shall promptly provide the results of each evaluation to GSCL, subject to ApplicableLaw(s).

c. Replacement

In case any proposed resource resigns, then the Bidder has to inform GSCL within one weekof such resignation.

Bidder shall promptly initiate a search for a replacement to ensure that the role of any member of the Key Personnel is not vacant at any point in time during the contract period, subject to reasonable extensions requested by Bidder to GSCL

Before assigning any replacement member of the Key Personnel to the provision of the Services, Bidder shall provide GSCL with:

- a resume, curriculum vitae and any other information about the candidate that is reasonably requested by GSCL; and

 An opportunity to interview the candidate.

The Bidder has to provide replacement resource of equal or better qualification and experience as per the requirements of this RFP.

If GSCL objects to the appointment, Bidder shall not assign the individual to that position and shall seek an alternative candidate in accordance with the resource requirements of thisRFP.

The Bidder needs to ensure at least 4 weeks of overlap period in such replacements. GSCL will not be responsible for any knowledge transition to the replacement resource and any impact/escalation of cost incurred by the bidder due to resource replacement.

d. **High Attrition causing adverse impacts to Project flow**

If in the first 6 month period from the Contract Effective Date in case of replacement of the projected man power resourcing, a penalty of INR 2,00,000 for first fifteen days and INR 10,000 per day can be imposed on the Bidder (for one replacement) till appropriate and approved replacement is done. Bidder shall:

e. Provide GSCL with a reasonably detailed explanation as to the reasons for such change, including, where applicable and permitted, notes from any exit interviews conducted by Bidder with any departing member of the Key Personnel; and

f. If such change to Key Personnel has or is likely to have any material adverse impact on the provision of the Services or any substantial part thereof, undertake, at its own costs, such remediation acts as are reasonably necessary in order to improve the retention of the Key Personnel including making reasonable changes to the human resources policies and procedures applicable to the Key Personnel (including those related to compensation, benefits and other conditions so that they are competitive with the market) as may be necessary to ensure that such policies and procedures comply with Good Industry Practice.

 Compliance with labour regulations

The MSI shall pay fair and reasonable wages to the workmen employed by him, for the contract undertaken by him and comply with the provisions set forth under the Minimum Wages Act and the Contract Labor Act 1970 and other relevant provisions of the Law.

 Operation Power charges

Operational power charges for the field electrical meter will be paid by MSI after readiness & final acceptance of the site and reimbursed by GSCL. MSI will be responsible of arranging the power for installation, implementation & testing of the site till final acceptance by GSCL. Field Electrical Meters will be issued in the name of GSCL. One time electrical meter connection installation & implementation, cabling charges and the operation & maintenanceIncident management, complaint logging for any fault in meter or field electrical connectionswill be responsibility of MSI during the entire contract period. The power connections (electrical meters) charges will be paid by MSI and the recurring power charges will be borne by the GSCL from Go-Live phase respective to each phase. Appointed MSI will coordinate the execution of connections with Electrical Department. The DG gen set, UPS willbe installed at the ICCC approved site and the operational expenses of fuel consumed by DG gen set till the time of acceptance will be borne by MSI.

2.7 Operations and Maintenance (O&M) services

The SI shall undertake the O&M services for a period of 5 years in the project from Project Go-Live. Warranty period of the product supplied under project i.e. hardware, software, IT/Non-IT etc., will be considered after Go-Live. In case, the project implementation gets delayed the O&M period will be accordingly adjusted/reduced/increased so that the overall project tenure remains for complete 5 Years.

2.8 Convergence

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

2.9 Responsibility Matrix

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

#	Key Activities	SI	GMC	GSCL	Police	PMC	Other Deptt.
1	Project Kick Off	R/A	C	C	C	C	I
2	Deployment of manpower	R/A	I	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	I	R	A	R	I
5	Providing As-Is information			R/A	R/A		
6	Assessment of Business processes	R/A	C	C	C	C	I
7	Acceptance of changes and ownership of business process post assessment	I		R	A	R	
8	Assessment of Software/ Application requirements	R/A		C	I	C	I
9	Assess the Integration requirement	R/A		C	C	C	I

10	Assess the connectivity requirement all locations (Field level+ CCC/DC/DR site)	R/A		C	C	C	I
11	Providing relevant data sets for identified use cases			R	A		
12	Preparation and finalization of use cases	R/A	I	R	C	C	I
13	Assessment of training requirement	R/A	I	R	A	C	I
14	Develop the Concept of Operations (CONOPS)	R/A	C	R	R	C	C
15	Formulation of Solution Architecture	R/A		C	C	C	I
16	Preparation of Detailed Drawing	R/A		C	C	C	I
17	Preparation of detailed Design of CCC Solution	R/A		C	C	C	I
18	Development of test cases (Unit, System Integration and User Acceptance)	R/A	I	R	R	R	I
19	Preparation of phase wise bill of material	R/A		C		C	
20	Approval of material for procurement	C		R/A		C	
21	SoP preparation	R	C	A	A	C	I
22	Material Procurement including software licenses	R/A		C		C	
23	Physical Infrastructure setup	R/A	C	C	C	C	C

24	IT and Non-IT Infrastructure Installation	R/A	I	C	I	C	I
25	Development, Testing and Production environment setup	R/A	I	C	I	C	I
26	Software Application customization (if any)	R/A	I	C	I	C	I
27	Development of Bespoke Solution (if any)	R/A	I	C	I	C	I
28	Implementation, testing of Solutions	R/A	I	C	C	C	
29	Integration of Map and other subsystems in CCC	R/A		C	I	C	
30	Training contents preparation	R/A					
31	Integration with city level/Third party services/application (if any)	R/A	I	C	C	C	I
32	SoP and KPI implementation	R/A	I	C	C	C	I
33	User Acceptance Testing	R/A	I	C	C	C	I
34	Helpdesk setup	R/A	I	C	C	C	I
35	Preparation of manual/ documents for system installation, system operation, User guide, SoPs	R/A	I	C	C	C	I
36	Role based training(s) on the INTELLIGENT CITY SURVEILLANCE SYSTEM Solutions	R/A	I	C	C	C	I
37	Go Live	R/A	C	R/A	C	C	I
38	Operation and Maintenance of IT, Non-IT infrastructure and	R/A	I	C	C	C	I

	Applications						
39	SLA and Performance Monitoring	R/A	I	R	R	C	I
40	Logging, tracking and resolution of issues.	R/A	I	C	C	C	I
41	Patch & Version Updates/upgrades	R/A	I	C	C	C	I
42	Future Integration with other services/infrastructure	R/A	I	C	C	C	I
43	Business process re-engineering	R/A	I	C	C	C	I
44	Use-cases enhancements	R/A	I	C	C	C	I

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

SI have to arrange own warehouse during Project phase to store the material in Guwahati as well as they have to take proper insurance during project delivery and O&M time period.

2.10 Project Deliverable, Milestones and Timelines

LEGENDS:

- T0 = Date of Signing of Agreement
- T1 = After Go-Live & Final Acceptance Testing

Sl. No.	Milestone	Deliverables (Phase 1)	Timelines (in months)
1	Project Initiation	· Project Team deployment, Detailed Survey Report including infrastructure AS-IS and TO BE assessment, phase wise location distribution.	T0+2
		· Design Built Report (DBR) containing the High Level Design, Low Level Design, BOQ	

		· Detailed Project deployment plan including Operations Management, Contract Management, Risk Management, Information Security and Business Continuity, Capacity Building Plan	
Phase 2 (ICCC & At 30% of identified Field Locations)			
2a	Supply of Materials for ICCC and 30% Field Locations	Material Delivery, Inspection Reports (Component- wise)	T0+4
2b	Installation of Materials at ICCC and 30 % Field Locations.	Installation of Materials at ICCC and 20 % Field Locations. (Component Wise)	T0+5
2c	Commissioning of Materials at ICCC and 30 % Field Locations	Commissioning of Materials at ICCC and 20 % Field Locations (Component Wise)	T0+6
Phase 3 (At next 30% of identified Field Locations)			
3a	Supply of Materials for 30% Field Locations	Material Delivery, Inspection Reports (Component- wise)	T0+5
3b	Installation of Materials at 30 % Field Locations.	Installation of Materials at 30 % Field Locations. (Component Wise)	T0+6
3c	Commissioning of Materials at 30 % Field Locations	Commissioning of Materials at 30 % Field Locations (Component Wise)	T0+7
Phase 4 (At remaining 40% of identified traffic junctions)			
4a	Supply of Materials for 40% Field Locations	Material Delivery, Inspection Reports (Component- wise)	T0+6
4b	Installation of Materials at 40 % Field Locations.	Installation of Materials at 40 % Field Locations. (Component Wise)	T0+7
4c	Commissioning of Materials at 40 % Field Locations	Commissioning of Materials at 30 % Field Locations (Component Wise)	T0+8
Phase 5 (Final Go Live and O&M)			
5	Final Go Live and UAT	Overall System Go Live and UAT	T0+9 (T1)
5B	Operation and Maintenance phase (O&M) - After Final Acceptance Testing & Go-Live of entire solutions	· Monthly SLA Compliance Report	T1 + 60 months

3.Payment Schedule

- ### 3.1 Payment Schedule – Implementation Phase

Based on findings of the site survey activity done by the SI, the SI may propose a change in the number of sites or individual units to be deployed for the entire project as well as overall scope of work and a consequent change in phasing. GSCL also retains the right to Suo-Moto change the number of sites or individual units to be deployed for each components of the Project. The final decision on change in phasing and related change in payment schedules shall be at the discretion of GSCL.

It should be noted that SI has to take prior approval from GSCL on a request order before supplying the project components for phase wise implementation of the project.

SI should complete all the activities within the defined timelines as indicated in Timeline of this project. The timeline will be reviewed regularly during implementation phase and may be extended in case GSCL feels that extension in a particular Request Order/Integration or any track is imperative, for the reason beyond the control of the bidder. In all such cases GSCL's decision shall be final and binding. The SI will be eligible for the payment based on the completion of activities and approval of the relevant deliverables.

- The request for payment shall be made to the Authority in writing, accompanied by invoices describing, as appropriate, the services performed, and by the required documents -Pre-Acceptance Testing, Test Results, Audit Reports etc.
- All payments shall be made after Verification of documentation by the GSCL or any person authorized by GSCL.
- Due payments shall be made promptly by the Authority, generally within Thirty (30) days after submission of an invoice or request for payment by SI.
- The currency in which payments shall be made to the SI under this Contract shall be Indian Rupees (INR) only.
- 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.
- Taxes and duties, as applicable, shall be deducted / paid, as per the prevalent rules and regulations as on date of the invoice. Any change in rates of Taxes and duties during the project shall adjusted upwards or downwards as per the latest regulations.
- All payments shall be made on pro-rata basis on actual supplies or services provided.

The payments shall be made as per the following schedule:

1) 10% of the CAPEX cost shall be released on submission of following and consequent approval by GSCL:

   - Detailed Survey Report including infrastructure AS-IS and TO BE assessment, phase wise location distribution.
   - Design Built Report (DBR) containing the High Level Design, Low Level Design, BOQ
   - Detailed Project deployment plan including Operations Management, Contract Management, Risk Management

2) 50% of the CAPEX cost shall be released on Supply of material on pro-rata basis and as per the approved supply plan by GSCL.

3) 15% of the CAPEX cost shall be released on Installation on pro-rata basis and as per the approved supply plan by GSCL.

4) 15% of the CAPEX cost shall be released on Commissioning on prorate basis and as per the approved supply plan by GSCL.

5) 5% of the CAPEX cost shall be released on Go Live of individual systems on prorate basis and as per the approved supply plan by GSCL.

6) 5% of the CAPEX cost shall be released on overall Go Live of the complete project.

- **3.2 Payment Schedule – Operation & Maintenance Phase**

The Operations and maintenance phase will start as soon as Go-Live for each phase occurs. The SI will be required to adhere to the SLA and provide post implementations support of warranty and O&M for the remaining project period after implementation/Go Live. Payment towards Operation & Maintenance shall be made subject to fulfillment of SLAs.

Payment of Operations and maintenance phase will be made on quarterly basis (at completion of each quarter) based on the adherence to SLA, for the amount quoted for each respective year.

4. Solution Overview of Proposed Intelligent City Surveillance System

4.1 Installation of cameras

The cameras which will be installed at the junctions will be connected to the UPS installed in the junction boxes for providing alternate power source. The main source of power will be from the existing power infrastructure used by GSCL for power supply to signals. The SI will size the panels as per the requirement of each junction. The SI should have to consider following check-points while installing/ commissioning cameras:

1. Ensure objective is met while positioning the camera such that the required field of view is being captured as finalized in primary survey.
2. Ensure camera is protected from the on-field challenges of weather, physical damage and theft.
3. Make proper adjustments to have the best possible image / video captured.
4. Ensure that the pole is well placed for vibration resistance adhering to the Road safety norms.
5. Collusion preventive barriers around the junction box and pole foundation in case its installed in collision prone place.
6. Appropriate branding or color coding (Police /GSCL Branding) of poles and junction boxes, to warn mischief mongers against tampering with the equipment at the junction.
7. Ensure the laws/regulations and privacy in the area regarding CCTV installation are considered. The camera's field of view has to adjust to abide by those.
8. Proper signage will be used to indicate CCTV surveillance uses.
9. Ensure the right type of camera (e.g., bullet/dome/PTZ) is installed based on the requirement in the area.

4.2 Installation of Public Address System and Emergency Call Box

Public Address System with Emergency Call Back System to be installed at various junctions

4.3 Installation of Poles:

1. The SI shall ensure that all the installations to be as per satisfaction of GSCL. Ensure that the power and signal connections are properly installed in the pole such that they are protected from damage and tempering. During pole installation, the line-of-sight/field-of-view should be checked with test cameras

2. For installation of Cameras, PA-ECB etc. the SI shall provide appropriate poles (Depending on the location and weather conditions a durable, corrosion-resistant, and wind-resistant pole material should be chosen) and any supporting equipment

3. SI to ensure that the poles erected to house cameras, PA-ECB etc. are good, both qualitatively and aesthetically

4. SI should use the industry best practices while positioning and mounting the cameras and ensure that the pole implementation is vibration resistant. Arrangements for bird scare spikes on top of camera shall be made to prevent birds from sitting on top of camera/ camera box.

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

6. Base frames and screws shall be delivered together with poles and installed by the SI

7. In case the cameras need to be installed besides or above the signal heads, suitable stainless-steel extensions for poles have to be provided and installed by the SI, so that there is clear line of sight

8. The successful SI shall provide the structural calculations and drawings for approval to GSCL. The design shall match with common design standards as applicable under the jurisdiction of Guwahati city and NHAI guidelines to be followed.

9. All necessary coordination related to this installation will be done by SI in discussion with the GSCL

10. Poles and cabinet shall be so designed that all elements of the field equipment can be easily installed and removed.

11. All the poles, junction boxes and necessary infrastructure deployed on the field shall be marked with logo of GSCL with text (as required). SI shall ensure its provisioning and proper numbering shall be done for all field equipment / inventory. Documentation for the inventory list with numbering and GIS coordinates shall be submitted by SI to GSCL at regular intervals and also at the time of Go-Live.

12. Need to share the safety and Quality Assurance Plan for entire project and considered during design phase and need to follow/comply the CPWD rules for entire field activity, specially for Civil/Electrical work like trenching, restoration, foundation and Electrical/Signal cabling in Field.

4.4 Provisioning hardware and software

It includes design, supply, installation and commissioning of IT Infrastructure at CCC with Cloud Data Center. This consists of:

- Basic Site preparation services.
- IT Infrastructure including all hardware, application portfolio, licenses etc.
- Centralized platform for data analytics and signal optimization.
- Command and Control Center (CCC) infrastructure (architectural, civil and electrical cabling work) including operator workstations, video wall etc.
- Establishment of LAN and WAN connectivity at CCC with field components.
- Application integration services with other Government systems.

- Monitoring the data and the network in Command-and-Control Centre (CCC) to prevent unauthorized access or cyber-attacks and a warning system should be in place.
- Backup plans (Manual and Auto) in case of system failures should be in place and as well should be consider during design phase.
- Requirements of database management systems and their security should be consider during design phase.
- Requirement of cloud storage and any restrictions in server location (should be located only within India) should be consider in design and detailed engineering phase.
- Would be good to have a provision for adding feature add-ons later as necessary.

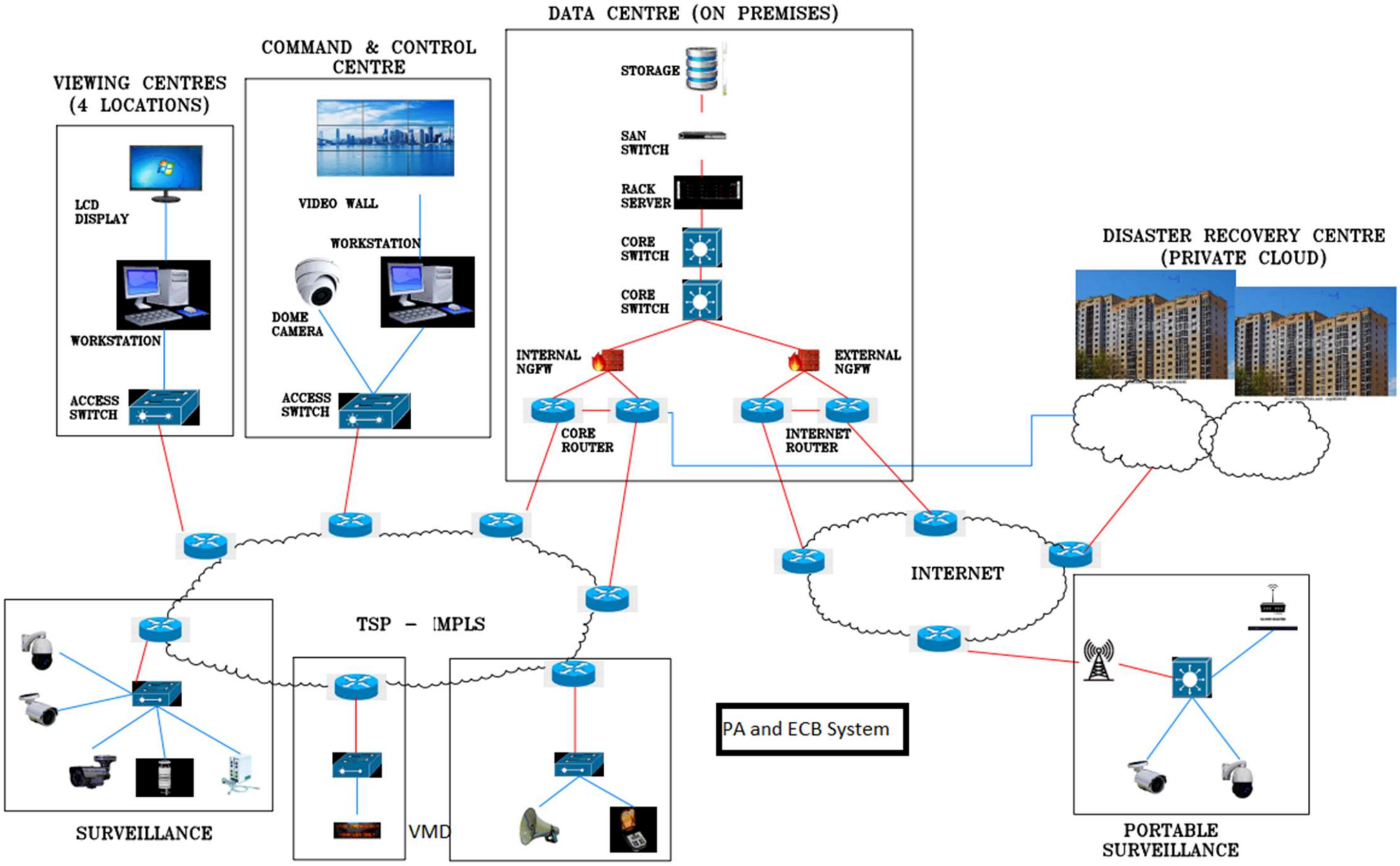
4.5 Connectivity

The SI shall conduct detailed study for connectivity of all filed devises / cameras considering feasibility, design optimization reliability.

The testing and monitoring procedures need to submit, to ensure the quality and performance of the connectivity over the time should also be in place and consider the same during detailed engineering and design phase.

The overall Architecture is given below

OVERALL ARCHITECTURE



4.6 Site Clearance obligations and other relevant permissions

Prior to starting the site clearance, the SI shall carry out survey of field locations as specified in this RFP, for buildings, structures, fences, trees, existing installations, etc. The authority shall be fully informed of the results of the survey and the amount and extent of the demolition and site clearance shall then be agreed with the authority. The Authority shall facilitate SI to take all requisite approvals and take necessary clearances for activities like Right of Way (ROW) etc.

The environmental and social impact assessment and mitigation measures for the site clearance activities should also be considered.

4.7 Electrical works and power supply

The SI needs to ensure fluctuation free power supply to the cameras for smooth functioning. Any physical infrastructure, like laying of cables etc. required for providing power supply from the existing junction boxes to the cameras will be done by SI.

Electricity charges for all the field elements/command and control center shall be borne by the authority. The SI shall directly interact with electricity board (APDCL) for provision of mains power supply at all the identified locations for INTELLIGENT CITY SURVEILLANCE SYSTEM field solution before Go-Live. The electricity charges after Go-Live of the project shall be borne by the authority as per actual consumption. The SI shall be responsible to submit the electricity bill including connection charge, meter charge etc. to the electricity board (APDCL) directly. SI shall have to submit the challan of bill submission to authority. Authority will reimburse the amount submitted to the SI after verification in next billing cycle.

SI is responsible for Maintenance and repair of the electrical works and power supply. SI is responsible for the backup and alternative power sources in case of a power outage or disruption. SI will be responsible for any damages happen due to any nonstandard work.

4.8 Civil and Electrical works

a) SI is responsible for carrying out all the civil work required for setting up all the field components of the system including:
   - Preparation of concrete foundation for MS-Poles & cantilevers
   - Laying of Pipes complete with fitting
   - Hard soil deep digging and backfilling after cabling
   - Soft soil deep digging and backfilling after cabling
   - Chambers with metal cover at every junction box, pole and at road crossings
   - Concrete foundation from the Ground for outdoor racks

b) The SI will be required to provide electricity to the cameras through the aggregation point. Since this component has dependency on approval from local authorities, it is recommended that Bidder plans this requirement well in advance & submits the application to the concerned electricity distribution agency with requisite fees if applicable.

c) The SI to carry out study and identify locations to provide UPS backup, depending upon power situation across city, so as to meet the camera uptime requirements.

d) SI is responsible for carrying out all the electrical work required for powering all the components of the system

e) Electrical installation and wiring shall conform to the electrical codes of India.

f) SI must make provisions for providing electricity to the cameras, field elements, the JB (Junction Box) housing the UPS/ SMPS power supply with minimum backup as defined in this RFP, using UPS/inverter.

g) Registration of electrical connections at all field sites shall be done in the name of SI/GSCL as agreed and finalized in the contract document.

h) SI has to also arrange for alternate or redundant power supply in form of UPS etc. in case the primary source of power fails for all surveillance, INTELLIGENT CITY SURVEILLANCE SYSTEM equipment as described in the RFP.

i) SI should house the electricity meters inside the power cabinet as mentioned in this RFP document.

4.9 Surge and Lightning-proof measures

The SI shall comply with lightning-protection, surge-protection and anti–interference measures for system structure, equipment type selection, equipment earthing, power, signal cables laying etc.

The SI shall describe the planned lightning-protection and anti –interference measures in the feasibility report. Corresponding lightning arrester shall be erected for the entrance cables of power line, video line, data transmission cables. All crates shall have firm, durable shell. Shell shall have dustproof, antifouling, waterproof function and should capable to bear certain mechanical external force.

4.10 Earthing System

All electrical components are to be earthen by connecting two earth tapes from the frame of the component ring and will be connected via several dedicated earth electrodes. The cable arm will be earthen through the cable glands. The entire applicable IT infrastructure i.e. signal junction or command Center shall have adequate earthing. Further, earthling should be done as per Local state National standard in relevance with IS standard. The SI has to provide maintenance free chemical earthing for all electrical equipment to be used in this project.

Earthing should be done for the entire power system and provisioning should be there to earth UPS systems, Power distribution units, AC units, etc. so as to avoid a ground differential. Department shall provide the necessary space required to prepare the earthing pits.

4.11 Junction Box, Poles(Gantries and Cantilever)

The SI shall provide the Junction Boxes, poles, gantries and cantilever to mount the field sensors like the cameras, sensors, light aspects, active network components, controller and UPS at all field locations, as per the functional and technical requirements given in the RFP.

The Junction Box needs to be appropriately sized in-order to accommodate the systems envisaged at the Junctions. The junction box should be designed with lock and key facility.

4.12 Cabling Infrastructure

The SI shall provide standardized cabling for all devices and Subsystems in the field and Command and Control center.

SI shall ensure the installation of all necessary cables and connectors between the field sensors/devices assembly, outstation junction box, for pole mounted field sensors/devices the cables shall be routed down the inside of the pole and through underground duct to the outstation cabinet. All cables shall be clearly labeled with indelible indications that can clearly be identified by maintenance personnel. The proposed cables shall meet the valid directives and standards. Arrangements pertaining to provision and maintenance of man holes shall be in scope of SI.

The potential problem of flash floods in the city of Guwahati and frequent road reconstruction in the city should be considered while laying the cabling infrastructure and need to be consider in design phase.

4.13 Design, Supply, Installation and Commissioning of the Field Equipment

The Scope includes supply, installation, commissioning and up-gradation (as required) of various field systems which include Cameras, Public Address, Emergency Call Back, Weather Sensors other IT infrastructure required for successful operation of the.

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

- The SI shall be responsible for obtaining all permits and approvals necessary to install the Intelligent City Surveillance System components from authority. However, authority shall borne the ROW charges and provide permissions from various government departments.
- The SI shall be required to submit a detailed installation report post installation of all the equipment at approved locations. The report shall be utilized during the acceptance testing period of the project to verify the actual quantity of the equipment supplied and commissioned under the project.
- Finally approved/accepted solution for each component of Intelligent City Surveillance System including enforcement system shall be accompanied with "Intelligent City Surveillance System Configuration" document and the same should be referenced for installation of Intelligent City Surveillance System including enforcement system at Junctions that are identified within the scope of this project.
- The implementation methodology and approach must be based on the global best practices in-order to meet the defined Service Levels during the operation.
- Best efforts have been made to define major functionalities for each sub- system of Intelligent City Surveillance System including enforcement System. However, SI should not limit its offerings to the proposed solution in this RFP and is suggested to propose any associated item part of RFP BOQ already been given in this tender.

4.14 Cameras

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

- The SI shall install the cameras at the specified junctions/locations across the city.
- The SI shall design, supply, and install the camera system as defined in the RFP, all camera accessories , camera housing and mounting shall be installed by the SI. The SI shall supply all of the necessary equipment for the camera poles, warning signs and shall make the final connections to the camera.
- The SI shall be responsible for providing the necessary IT infrastructure for detection, analysis, retrieval of the information at Command and Control Center.
- For more details on technical and functional specifications of Cameras, bidder should refer to Functional and Technical Requirements in this RFP.
- The SI will responsible for the maintenance and Regular updates of the camera systems.

.

4.15 Public Address System

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

- The SI shall install the Public Address System at the specified junctions/locations across the city.
- The SI shall design, supply, and install the public address system as defined in the RFP, all accessories and mounting shall be installed by the SI. The SI shall supply all of the necessary equipment for the poles and shall make the final connections.

- The SI shall be responsible for providing the necessary IT infrastructure for announcement to be made from the information at Command and Control Center.
- For more details on technical and functional specifications of Public Address System, bidder should refer to Functional and Technical Requirements in this RFP.

4.16 Emergency Call Box System

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

- The SI shall install the Emergency Call Back System at the specified junctions/locations across the city.
- The SI shall design, supply, and install the Emergency Call Back system as defined in the RFP, all accessories and mounting shall be installed by the SI. The SI shall supply all of the necessary equipment for the poles and shall make the final connections.
- The SI shall be responsible for providing the necessary IT infrastructure for receiving and accepting Voice command and retrieval of the same at Command and Control Center.
- For more details on technical and functional specifications of Emergency Call Back System, bidder should refer to Functional and Technical Requirements in this RFP.
- System should detect the false alarms.
- The CCTV cameras should have a field-of-view that include the view of the emergency call box system.

4.17 Design, Supply, Installation, Testing and Commissioning of Network and Backbone Connectivity

- Network and Backbone Connectivity is an important component of the Intelligent City Surveillance System and needs attention in assessment, planning and implementation. It is important not only to ensure that the required connectivity is provisioned within the required timelines but also ensure that it is reliable, secure and supports the required SLA parameters of Latency, Jitter, Packet Loss and Performance.
- The SI shall procure bandwidth as a service for the contract duration in order to meet the requirements as defined within the service level agreement (SLA).
- The SI should provide detailed network architecture of the overall system, incorporating findings of site survey exercise. The network so envisaged should be able to provide real-time data streams to the CCC. All the components of the technical network architecture should be of industry’s best standard and assist SI in ensuring that all the connectivity SLAs are adhered to during the operational phase.
- The SI shall prepare the overall network connectivity plan for this project. The plan shall comprise of deployment of network equipment at the junctions to be connected over the network, any clearances required from other government departments for setting up of the entire network.
- SI is also required to do the estimation of bandwidth requirements considering the specifications mentioned in this RFP document.
- As per TRAI guidelines, the resale of bandwidth connectivity is not allowed. In such a case tripartite agreement may be formed between Purchaser, selected Bidder and Internet Service Provider (s). In order to meet the RFP requirement, Selected Bidder may have a to form tripartite agreement with multiple ISPs.

4.18 Design, Supply, Installation, Testing and Commissioning of CCC

The SI shall also set up a CCC at an identified location in Guwahati. The CCC shall be established in an approximate area of ~3000 Sq. ft. SI should refer to the indicative plan of the CCC attached with this RFP document. It will be SI’s responsibility to:

- Supply, Install, and Commission of IT Infrastructure including site preparation in CCC. A secured environment will be provided to the SI at the CCC. As well as need to share a feasibility report for the shifting of infrastructure would be in case of relocalization of CCC during design phase.

- Supply Smart Network Rack, Network Switches, and required accessories at CCC.
- The SI shall establish a state-of-the-art CCC, the key components of the CCC will be as follows:

4.18.1 Video Wall system
4.18.2 Operator workstations
4.18.3 Active Networking Components (Switches, Routers)
4.18.4 Passive Networking Components
4.18.5 Electrical Cabling and Necessary LED Illumination Devices for approx. ~3000 Square feet area
4.18.6 Office Workstations
4.18.7 UPS (1-hour backup)
4.18.8 Furniture & Fixtures as specified in subsequent sections of this RFP document
4.18.9 Physical and electronic Security systems for authorized entry (Biometric access control)
4.18.10 Safety System for protection against Fire, Theft and any other possible damage.

- The SI shall provide system integration services to customize and integrate the applications procured through the project. The Intelligent City Surveillance System applications proposed by the SI should have open APIs and should be able to integrate and share the data with other third- party systems already available.
- The SI must ensure that redundancy is provided for all the key components to ensure that no single point of failure affects the performance of the overall system.
- The above are only indicative requirements of IT and Non-IT Infrastructure requirements at CCC. The exact quantity and requirement shall be proposed as part of the technical proposal of the SI.
- The implementation roll-out plan for hosting of the data center over the cloud shall be approved by authority. The detailed plan shall ensure the scalability, expandability and security.
- The SI shall be required to submit a detailed installation report post installation of all the equipment at approved locations. The report shall be utilized during the acceptance testing period of the project to verify the actual quantity of the equipment supplied and commissioned under the project.

4.19 Design, Supply, Installation, Testing and Commissioning of IT Infrastructure for DR over cloud

The SI shall be responsible for deploying Disaster – Recovery for the Intelligent City Surveillance System on Cloud. The SI shall select a MeitY empaneled Cloud Service Provider (CSP). The SI may refer to the details of MeitY empaneled CSPs over, http://meity.gov.in/content/gi-cloud-meghraj. It should also comply with the empanelment requirements published by the MeitY.

All the requirements/scope of work mentioned in this section shall be the responsibility of the SI. SI shall also ensure that as a SI, the CSP provides the features in the cloud and also performs the scope of work which is directly attributable to CSP.

i. The SI is required to prepare and submit along with their technical proposal, the details of methodologies & computations for sizing & capacity of storage, compute, backup, network and security.
ii. There should be sufficient capacity (compute, network and storage capacity offered) available for real time provisioning during any unanticipated spikes in the user load.
iii. The SI will be responsible for adequately sizing the necessary compute, memory, and storage required, building the redundancy into the architecture (including storage) and load balancing to meet the service levels mentioned in the RFP.
iv. While the initial sizing & provisioning of the underlying infrastructure (including the system software and bandwidth)

may be carried out for the first year; subsequently, it is expected that the SI along with the CSP, based on the growth in the user load (peak and non-peak periods; year-on year increase), will scale up or scale down the compute, memory, storage, and bandwidth requirements to support the scalability and performance requirements of the solution and meet the SLAs.

v. Ensure redundancy at each level

vi. SI shall provide interoperability support with regards to available APIs, data portability etc. for GSCL to utilize in case of:

  a) Change of Cloud Service Provider,
  b) Migration back to in-house infrastructure,
  c) Burst to a different cloud service provider for a short duration, or

vii. Required support to be provided to GSCL in migration of the VMs, data, content and any other assets to the new environment created by the GSCL or any Agency (on behalf of GSCL) on alternate cloud service provider's offerings to enable successful deployment and running of GSCL solution on the new infrastructure.

viii. The SI/CSP should configure, schedule and manage backups of all the data including but not limited to files, folders, images, system state, databases and enterprise applications:

  a) Perform and store data and file backups consisting of an initial full back up with daily incremental backups for files;
  b) For the files, perform weekly backups;
  c) For the databases, perform a twice weekly full database backup, with a three times daily backup of database log files
  d) Encryption of all backup files and data and management of encryption keys as a service that can be enabled for GSCL that require such a service.
  e) Retain database backups for five (5) years on system and thereafter on tapes which can to be restored when required.

ix. SI/CSP shall not delete any data at the end of the agreement (for a maximum of 90 days beyond the expiry of the Agreement) without the express approval of GSCL.

x. The SI is fully responsible for technology refreshes, patch management and other operations of infrastructure that is in the scope of the SI.

xi. The SI should offer dashboard to provide visibility into service via dashboard.

4.20 Capacity Building and Training

Capacity Building is an important aspect of this Project. SI has to conduct a proper training need analysis of all the concerned staff and draw up a systematic training plan in line with the overall Project plan. For all these training programs the SI has to provide necessary course material and reference manuals (user/maintenance/ administration) along with training schedules for all phases. The course and documentation required shall be prepared in English language. The training shall be held at various office/department locations as finalized by GSCL.

Training shall be provided to the following trainees:

i. Senior Officers: Officers from Guwahati Police and other departmental stakeholders

ii. Functional users: Field staff, the staff of command and control Center and other departmental stakeholders

- SI should ensure that the knowledge transfer to the concerned department staff happens effectively post training.
- Prepare the training material in consultation with authorities. Detailed training manuals would be prepared by the

SI prior to the start of the training. Master copies of all training material should be submitted to the Authority for approval.

4.21 Factory Acceptance Testing (FAT)

The Factory Acceptance Test (FAT) is a process that evaluates the equipment during and after the assembly process by verifying that it is built and operating in accordance with design specifications. Successful Implementation.

SI must submit Factory Acceptance Test Certificate for the below mentioned materials before the actual supply of the items. These items include all the IT / Non-IT / Active and Passive components as per RFP

4.21.1 Acceptance testing

GSCL shall review and finalize the detailed acceptance test plan proposed by the SI. The authority would also conduct audit of the process, plan and results of the Acceptance Test carried out by the SI for both IT and non-IT components. The authority would issue certification of completion for which, authority shall verify availability of all the defined services as per the contract signed between the SI and GSCL. The SI shall be required to demonstrate all the services, features, functionalities as mentioned in the agreement.

Testing and Commissioning shall be carried out before the commencement of Operations.

4.21.2 Partial Acceptance Testing

Partial Acceptance Test shall involve scrutiny of documents for various IT / Non-IT components to verify if the specifications conform to the technical and functional requirements mentioned in the Tender and subsequent corrigendum.

Authority reserves right to conduct physical inspection of the equipment delivered to ensure that they arrive at the sites in good condition and are free from physical damage and incomplete shipments and shall return the products to the supplier at the supplier’s expenses if required quality is not maintained.

Physical inspection of hardware will also include physical checking and counting of the delivered equipment in presence of the SI.

The equipment will only be acceptable as correct when each received item corresponds with the checklist that will be prepared by the SI prior to shipment.

Any shortfalls in terms of number of items received may render the delivered equipment incomplete.

4.22 Third Party Audit

GSCL reserves the right to respect and monitor/assess the performance / maintenance of the project systems at any time during the course of the contract. GSCL may demand and upon such demand being made, GSCL or its authorized Third Part Agency (TPA) shall be provided with any documents, data, materials or any other information which it may require, to enable it to assess the progress / performance of the project.

GSCL also have the right to conduct itself or through another third part audit agency as it may deem fit, an audit to monitor the performance by the bidder on its obligations/functions in accordance with the standards committed to or required by GSCL undertake to cooperate with and provide to GSCL / Audit agency. All documents and other details or information as may be required by them for this purpose. Any deviation or contravention identified as a result of such audit / assessment would need to be rectified by the bidder.

The core objective of TPA is to provide objective assurance to monitor and assess the conformance by the bidder on various project activities and add value to improve the project operations. It would help GSCL to accomplish the project objective by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of infrastructure, operations service level management and control and governance process.

4.23 Final Acceptance Testing

The final acceptance shall cover overall Supply, implementation, testing and commissioning of the Intelligent City Surveillance System Project, after successful testing by the authority, a Final Acceptance Test Certificate (FAT) shall be issued by the authority to the SI.

Prerequisite for carrying out Final Acceptance testing activity:

- Detailed test plan shall be developed by the SI and approved by authority. This shall be submitted by SI before Final Acceptance Testing activity to be carried out.
- All documentation related to Intelligent City Surveillance System project and relevant acceptance test document (including IT Components, Non-IT Components etc.) should be completed and submitted before the final acceptance test to the Department.
- The training requirements as mentioned should be completed before the final acceptance test.
- Successful hosting of Application.

The Final Acceptance testing shall include the following:

- All hardware and software items must be installed at respective sites as per the specification.
- Availability of all the defined services shall be verified.
- DR Drill to be performed and 100% successful.
- The SI shall be required to demonstrate all the features / facilities / functionalities as mentioned in the RFP.
- The SI shall arrange the test equipment required for performance verification and will also provide documented test results.

4.24 System Documents and User Manuals

- The SI shall provide documentation, which follows the ITIL (Information Technology Infrastructure Library) standards or IEEE/ISO Acceptable Documentation Standards.
- The documentation should be submitted as the project undergoes various stages of implementation and provide all traceability documentation on changes done on the IT components during the course of the implementation.
- Indicative list of documents includes:
    - Site assessment report should provide comprehensive detailing of existing and envisaged infrastructure and requirements in the project.
    - Project Plan should provide micro level activities with milestones and dependencies etc.
    - Original manuals (installation, training etc.) from OEMs.
    - Training Material will be provided which will include the presentations used for trainings and also the required relevant documents for the topics being covered.
    - The SI shall be responsible for preparing detailed process documentation related to the operation and maintenance of each and every component of the Intelligent City Surveillance System Project.
    - The SI shall document all the installation and commissioning procedures and provide the same to the authority within one week of the commissioning of the project.
    - Manuals for configuring of switches, routers, etc. shall be provided by the selected SI.

- Complete inventory list of all the equipment deployed at field level with proper numbering and GIS coordinates.

The SI shall be responsible for documenting configuration of all devices and keeping back up of all configuration files for the complete project tenure, so as to enable quick recovery in case of failure of devices.

4.25 Operations and Maintenance during contract period

Success of the Project would lie on how professionally and methodically the entire project is managed once the implementation is completed. SI is required to depute a dedicated team of professionals to manage the Project and ensure adherence to the required SLAs.

The SI shall provide O&M services for all project related components installed as part of Intelligent City Surveillance System project during the Contract Period, including one (1) year of warranty period after "Go-Live".

The activities to be carried out during the contract period shall include, but not limited, to the following:

- Monitor the operation of Intelligent City Surveillance System and take suitable interventions as required such as change of signal plan, change of signal timing from CCC enabling green corridor etc. Periodic change of signal plans and other configurations parameters on directions of Authority.
- Monitor health of signal and camera equipment and initiate immediate corrective action in any fault.
- Undertake configuration management for all systems.
- Undertake system admin, database admin, back up, archival, network admin activities.
- Comprehensive maintenance of all equipment/sub-system during Contract period.
- Facility Management of Command and Control centre during O&M phase.
- Help Desk Management.

4.26 Project Management and Operation Maintenance

The SI will be required to provide facilities management services to support the authority / Police department officials in performing their day-to-day functions related to this system.SI is required to depute a dedicated, centralized project management and technical team for the overall Project management and interaction with authority and other departments during the time of Implementation. The project management team of SI will work in tandem with the Project PMU/ PMC set up by GSCL during the entire contract duration.

4.27 Indicative resource requirement

Below is the indicative resource requirement for centralized administration of the Project

SI no.	Position	Quantity	Minimum Deployment during Implementation phase	Minimum Deployment during Operation and Maintenance phase
1	Project Manager	1	At least 80%	100%

2	Integrated Commandand Control Centre (ICCC) Expert	1	At least 80%	Onsite Support to Project team on need basis
3	Solution Architect	1	At least 80%	Onsite Support to Project team on need basis
4	Network & Security Infrastructure Expert	1	At least 60%	100%
5	Security & Surveillance Expert	1	At least 80%	100%
6	Server & Storage Expert	1	At least 60%	100%
7	Quality Control Expert	1	At least 80%	Onsite Support to Project team on need basis including quarterly visit and report submission

The above-mentioned manpower requirement is minimum and if the SI believes that to meet the SLAs, additional resources are required, the same may be provided by the SI. GSCL can suggest changes in the aforementioned resource requirement as per the requirement. It is the SI’s responsibility to identify and deploy the resources during the O&M phase.

The Command Centre Operators provided by the SI shall be responsible for verification and generation of the e-challans. They will also be responsible for providing support in terms of monitoring of the data feeds at Command and Control Center and handholding the Officials from Police department required for operationalization of the Intelligent City Surveillance System project.

System Engineer - Hardware shall be responsible for first level of technical support in terms of ICT equipments placed at the Command and Control Centre as well as Help Desk functions.

SI shall deploy adequate site engineers required for smooth operation of the Project components.

SI shall deploy adequate Facility Management staff at Command and Control Centre. Facilities management shall include but not limited to building and grounds maintenance, cleaning, catering and vending, security, space management, utilities management etc. and associated manpower shall also be under the scope of the SI during Operation & Maintenance phase.

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

- All such manpower shall be without any criminal background /record.
- 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.
- SI shall have to replace any person, if not found suitable for the job.
- Operational Manpower shall work in at least 2 shifts, with no person being made to see the feeds for more than 8

hours at a stretch.

- Detail operational guideline document shall be prepared during implementation which shall specify detail responsibilities of these resources and their do’s and don’ts.

4.28 Hand-over of the system before contract expiry

SI will supply the following to the GSCL before the expiry of the contract:

- Information relating to the current services rendered and data relating to the performance of the services;
- Entire documentation relating to various components of the Project, any other data and confidential information related to the Project;
- All other information (including but not limited to documents, records and agreements) relating to the products and services related to the project
- Enable Police Department and its nominated agencies, or its replacing Successful SI to carry out due diligence in order to transition the provision of the Project Services to authority or its nominated agencies, or its replacing Successful SI (as the case may be).
- The SI shall provide GSCL or its nominated agency with a recommended exit management plan ("Exit Management Plan").
- Promptly during exit on reasonable request by GSCL, SI shall provide access to and copies of all information held or controlled by them which they have prepared or maintained in accordance with this agreement relating to any material aspect of the services (whether provided by the SI or subcontractors appointed by the SI).
- GSCL shall be entitled to copy of all such information. Such information shall include details pertaining to the services rendered and other performance data.
- SI to provide appropriate knowledge transfer.

4.29 Other requirements

The SI should ensure the following (not limited to) while implementation of project:

- SI to ensure that for operation and maintenance team has the uniform with the identity card, safety shoes, helmet, Neon Jacket sets.
- SI will have to carry his own four-wheeler and a ladder of 15 feet length to carry out implementation and maintenance work (including transportation of items required for Project) during the Contract Period. All the expenses pertaining to vehicle such as driver’s expenses, fuel, lubricants, maintenance, etc. will have to be borne by the SI.
- SI will pay the charges related to Electric Meter, recurring electricity charges. These charges will be then reimbursed by GSCL. Fuel for DG shall also be provided by authority.
- SI will implement the Biometric attendance system for the attendance of Project member proposed in this document at the command and control center. The SI will share the attendance report with the client at the end of the month. The quarterly payment will be disbursed as per the SLA requirements.

4.30 Video Analytics for the project

- The SI shall have to provide a robust video analytics software under this project. The video analytics should have an AI features and preferably should be on Open-source platform. The detailed specifications are mentioned in subsequent sections of this RFP document.

5 Intelligent City Surveillance System – Functional Requirement & Technical Specifications

The functional requirements and technical specifications provided in the below sections are indicative and carry guiding rule.

Any specified parameters mentioned in the scope/technical requirement in the RFP may be considered if it is required for meeting current & future requirements during the contract period. The SI is fully responsible for the specified outcome to be achieved.

An Architecture diagram shared for better clarity in section 4.5.

5.1 CAMERA SPECIFICATION:

All Cameras to be of Same Make and need to share this specification (Power Consumption, Warranty Period, Field Of View, Firmware update (Auto or manual) spec, Form factor/dimension/weight) along with table mentioned spec.

CCTV		Technical Compliance (Yes/No)	Remark
S.No	**OEM Criteria**		
1	CCTV OEM should be active company and should have direct presence in India from last ten years (not as joint venture, partnership firms or through any other association) & manufacturing in India since last Five years (not as joint venture, partnership firms or through any other association) (3rd Party Manufacturing not allowed) and Foreign CCTV OEM should have manufacturing unit globally from last 10 Years at the time of bidding. Documentary evidence should be submitted.		
2	Bidder shall ensure compliance to the Office Memorandum for insertion of Rule 144 (xi) in the General Finance Rules (GFR)-2017 bearing reference number F.No. 6/18/2019-PPD dated 23 July 2020 or latest, by the Public Procurement Division, Department of Expenditure, Ministry of Finance. Non-compliant bid(s) will be summarily rejected. The OEM should not have any common directors who are also on the board of companies having beneficiaries from land border countries at the time of bidding. The camera OEM must submit declaration regarding their own manufacturing setups and shall not have 3rd party manufacturing from any company blacklisted in India or any company sharing land border with India. The IPR/copyright of source code of firmware/software etc. should not reside in countries sharing land borders with India. OEM should submit supporting document to establish proof of this eligibility criteria.		
3	Bid should be compliant to the Policy and Make in India makes shall be given preference as per Order 2017-Revision vide the Department of Industrial Policy and Promotion (DIPP) Order No. P-45021/2/2017-PP(BE-II) dated 16th September,2020 or latest. OEMs under make in India must submit Undertaking and supporting documents.		
5 MP IP Bullet Camera with in-built 100 Mtr. IR		**Technical Compliance (Yes/No)**	**Remark**

S.No	Features	Required Parameter		
1	Sensor	1/2.7", 5MP Progressive Scan CMOS Sensor		
2	Max resolution	5 MP		
3	Min. illumination	Color: 0.01 Lux @F1.2, B/W: 0.001 Lux@F1.2, 0 Lux at IR ON		
4	Electronic Shutter	Auto, Slow Shutter, (1/1s-1/100,000s Adjustable)		
5	Lens	5-50mm Motorized Lens		
6	IR Range	up to 100Mtr		
7	Camera Feature	WDR (120dB), 3D-DNR, AGC, AWB, Day & Night,		
8	S/N ratio	≥60db		
9	Video Analytics	Line Crossing, Motion Detection, Intrusion Detection, Scene Change, Human Detection		
10	Video & Audio Compression	Video: H.265 & H.264 (H.265/ HEVC and H.264 /AVC Certificate to be submitted at the time of submitting bid) Audio: G.711A		
11	Video & Audio Bit Rate	Video: Constant bit rate, variable bit rate (250kbps-8Mbps)		
12	Video Streams	Mainstream: 5MP (2880X1620)/2MP(1920×1080)@25/30fps Sub Stream: D1 (704x576)/ CIF (352×288) @15FPS Third Stream: VGA (640X480)/CIF (352×288) @15FPS		
13	Security Feature	New Password Policy, ActiveX Remove, Shifting to HTML5, HTTPS, Video Encryption , HTTPS X 509 certificate, syslog, 801.X, Trusted Boot		
14	Protocol	TCP/IP, IPv4,Ipv6, RTCP, NTP, UPnP, SMTP, FTP, ICMP, HTTP, HTTPS, HTTP-Base64, HTTP-Digest, DHCP, DNS, DDNS, RTP, RTSP, IGMP, P2P, IP Filter, SNMP V1 & V2		
15	Alarm In/out	1 Alarm In/1 Alarm Out		
16	Audio In/out	1 Audio In/1 Audio Out		
17	System Compatibility	ONVIF Profile S, G & T . CCTV OEM Should be ONVIF Full Member.		
18	Privacy Mask	Support 4 area privacy mask		
19	Network Port	RJ45 10M,100M adaptive Ethernet interface		
20	SD Card	Support up to 512GB		
21	Operating Conditions	-30°C ~ 60 °C Humidity 95% or less (non-condensing)		
22	Ingress protection	IP66/67 Complaint		
23	Vandalism	IK10 Vandal Proof Complaint		
24	Product Certification	CE, FCC, IS-13252 (Part 1):2010, BIS Registered		
25	OEM should have ISO 9001, 14001, 27001, 45001, ISO/IEC 27032:2012 and CMMI Level 5 Certificate.			
5MP IP PTZ Camera 30x Optical Zoom				

Sl. No.	Parameters	Specifications	Technical Compliance Yes/No	Remark
1	Image Sensor	1/1.9” Progressive Scan CMOS		
2	Min. Illumination	Color: 0.005Lux@F1.2 B/W: 0Lux with IR on		
3	Zoom	Optical Zoom 30X & Digital Zoom 16X		
4	Focal Length	4.7~141mm @F1.5~F4.0 or equivalent to 30x Optical zoom		
5	Video Compression	H.265 & H.264 (H.265/ HEVC and H.264 /AVC Certificate to be submitted at the time of submitting bid)		
6	Field of View	H58°~H3°/D71°~D3°/V44°~V2°		
7	WDR	140dB Super WDR		
8	Shutter Time	1/100000s~1s		
9	Other Feature	Day & Night, 3D positioning, Backlight Compensation, White Balance, Gain Control, Ultra DNR (2D/3D), Electronic Image Stabilization (EIS)		
10	S/N	>65dB		
11	Pan Range/Pan Speed	360° endless/ Pan Manual Speed: 0.1°～400°/s, Pan Preset Speed: 400°/s		
12	Tilt Range/Tilt Speed	0°～90°(Auto Flip)/ Tilt Manual Speed: 0.1°～320°/s, Tilt Preset Speed: 320°/s		
13	Preset	256		
14	Patrol	8 Patrols, up to 48 presets each patrol		
15	Pattern	4 Patterns		
16	IR Distance	Up to 200m		
17	Video Streaming	Main Stream: 30fps@(2592x1944), 60fps@ (1920x1080, 1280x960) Sub Stream: 60fps@(704x576, 640x480, 640x360) Third Stream: 30fps@(1920x1080, 1280x720, 704x576)		
18	**Network**			
19	Ethernet	1*RJ45 10M/100M Ethernet Port		
20	Streaming Method	Unicast / Multicast		
21	Protocol	IPv4/IPv6, SMTP, SNMP, UPnP, SIP, PPPoE, VLAN, 802.1x, QoS, IGMP, ICMP, SSL, TCP, UDP, RTP, RTSP, RTCP, HTTP, HTTPS, DNS, DDNS, DHCP, FTP, NTP		
22	Audio Compression	G.711/AAC/G.722/G.726		
23	Audio I/O	1 IN/1 out		
24	Alarm I/O	4 IN/2 Out		
25	RS485	Support		
26	Edge Storage	Support for micro-SD/SDHC/SDXC (Max 256 GB supported)		
27	Advanced Function	Auto Tracking, IP Address Filtering, AGC, Anti-flicker, Corridor Mode, Deblur		
28	Privacy Masking	Up to 8 areas		
29	Region of Interest	Support		

30	Smart Defogger	Built-In Fan & Heater combined with Software algorithm Provide Fog Free Picture		
31	PTZ Auto Tracking	Support		
32	**Events**			
33	Event Trigger	Motion Detection, Network Disconnection, External Input, IP address conflict, Illegal Access, Storage anomaly etc.		
34	Event Action	FTP Upload, SMTP Upload, SD Card Record		
35	Video Analysis	Region Entrance, Region Exiting, Advanced Motion Detection, Tamper Detection, Line Crossing, Loitering, People Counting, Object Left, Object Removed		
36	System Compatibility	ONVIF Profile S, G & T . CCTV OEM Should be ONVIF Full Member.		
37	**General**			
38	Working Condition	Temperature: -50℃~70℃ / Humidity: 0~95%(Non-condensing)		
39	Power Supply	PoE (802.3at) / AC 24V/3A±10%		
40	Power Consumption	16.5W MAX / 35.5W MAX		
41	Surge Protection	IP67 Compliant, IK10 Certified, Level 2 lightning protection 6000V surge protection		
42	Certification	CE, FCC, IS-13252 (Part 1):2010, BIS Registered		
43	OEM should have ISO 9001, 14001, 27001, 45001, ISO/IEC 27032:2012 and CMMI Level 5 Certificate.			
		5 MP IP BOX Camera		
Sl. No.	**Parameters**	**Specifications**		
1	Sensor	1/2.7”, 5MP Progressive Scan CMOS Sensor		
3	Max resolution	5 MP		
4	Min. illumination	Color: 0.01 Lux @F1.2, B/W: 0.001 Lux@F1.2, 0 Lux at IR ON		
5	Electronic Shutter	Auto, Slow Shutter, (1/1s-1/100,000s Adjustable)		
6	Lens	5-50mm CSMount/M12 Mount Lens/Any Other mount		
7	IR Range	External IR		
8	Camera Feature	WDR (120dB), 3D-DNR, AGC, AWB, Day & Night,		
9	S/N ratio	≥60db		
11	Video & Audio Compression	Video: H.265 & H.264 (H.265/ HEVC and H.264 /AVC Certificate to be submitted at the time of submitting bid) Audio: G.711A		
12	Video & Audio Bit Rate	Video: Constant bit rate, variable bit rate (250kbps-8Mbps)		
13	Video Streams	Mainstream: 5MP (2880X1620)/2MP(1920×1080)@25/30fps Sub Stream: D1 (704x576)/ CIF (352×288) @15FPS Third Stream: VGA (640X480)/CIF (352×288) @15FPS		

14	Security Feature	New Password Policy, ActiveX Remove, Shifting to HTML5, HTTPS, Video Encryption , HTTPS X 509 certificate, syslog, 801.X, Trusted Boot		
15	Protocol	TCP/IP, IPv4,Ipv6, RTCP, NTP, UPnP, SMTP, FTP, ICMP, HTTP, HTTPS, HTTP-Base64, HTTP-Digest, DHCP, DNS, DDNS, RTP, RTSP, IGMP, P2P, IP Filter, SNMP V1 & V2		
16	Alarm In/out	1 Alarm In/1 Alarm Out		
17	Audio In/out	1 Audio In/1 Audio Out		
18	System Compatibility	ONVIF Profile S, G & T . CCTV OEM Should be ONVIF Full Member.		
19	Privacy Mask	Support 4 area privacy mask		
20	Network Port	RJ45 10M,100M adaptive Ethernet interface		
21	SD Card	Support up to 512GB		
22	Operating Conditions	-30°C ~ 60 °C Humidity 95% or less (non-condensing)		
23	Ingress protection	IP66/67 Complaint		
24	Vandalism	IK10 Vandal Proof Complaint		
25	Product Certification	CE, FCC, IS-13252 (Part 1):2010, BIS Registered		
26	OEM should have ISO 9001, 14001, 27001, 45001, ISO/IEC 27032:2012 and CMMI Level 5 Certificate.			

5.2 IP PUBLIC ADDRESS SYSTEM SPECIFICATION:

IP-Public Address System		Technical Compliance (Yes/No)	Remark
Sl. No.	**Parameter**		
1	IP66 Outdoor IP Speaker		
2	Audio streaming: One-way/two-way		
3	G.711 Audio Compression		
4	Max sound pressure level: >121 dB		
5	Frequency response: 250-10000Hz		
6	Coverage pattern: 70° horizontal by 100° vertical (at 2 kHz)		
7	Built-in 30 W amplifier		
8	Security: Password protection, IP address filtering, HTTPS encryption, Digest authentication, User access log		
9	Protocol: TCP/IP, UDP, RTP, RTSP, RTCP, HTTP, HTTPS, DNS, DDNS, DHCP, FTP, NTP, SMTP, UPNP, SMTP, IPv4, IP filter		
10	Power: 12V DC 30W		
11	RJ45 10BASE-T/100BASE-TX PoE		
12	Operating Temperature: 10°C to 60 °C		

IP Speaker Software		Technical Compliance (Yes/No)	Remark
1	Software should have the capability to connect multiple IP speakers		
2	Software should have the capability for one to one and one to many announcement		

3	Software should have the capability to make the group of multiple IP speaker		
4	Software should have the capability to modify the IP speaker configuration like Audio Volume increase & decrease etc.		
5	OEM of software should be CMMI Level 5.		
6	Software should have a multi- level user authentication feature.		

5.3 EMERGENCY CALL BOX SPECIFICATION:

Emergency Call system			
S.No	**Specification**	**Technical Compliance (Yes/No)**	**Remark**
1	ECB Should have SOS button for two way communication		
2	ECB Should have Hands-free Emergency Audio Video calling feature		
3	ECB should have provision to support 3G/4G, Ethernet network and fiber optic connectivity. Any one type of connectivity as defined at design stage should be supplied as per customer requirement.		
4	ECB Should support Video Based call management application with a live site map, the calls for help can be served practically from a remote location.		
5	Video Compression: H.265 & H.264 (H.265/ HEVC and H.264 /AVC Certificate to be submitted at the time of submitting bid)		
6	ECB Should have 2MP (1920 x1080) Camera		
7	Focal Length of Camera 4mm lens		
8	ECB should have 16GB Built-In Memory		
9	ECB Camera Support Triple Stream @25/30 fps in each stream		
10	ECB should have built in Mic and Speaker		
11	Operating Conditions: -30° C ~ +60° C / Less than 95% RH		
12	ECB should be IP66 Compliant. Call Boxes should be built to withstand harsh weather conditions and vandalism, ensuring their functionality in various environmental situations.		
13	ECB operate at DC 12V ± 10%		
14	ECB Camera Support WDR (120dB)		

Emergency Call Box Software		**Technical Compliance (Yes/No)**	**Remark**
1	SOS Emergency Call Box offers hands-free emergency call management service at the time of distress. Such call boxes should be mounted in easily accessible locations. Emergency Call Boxes should be mounted in locations where a CCTV Camera from the proposed bill of material is nearby positioned to capture the overview of the region.		

2	The call-box with Video and all the call boxes are connected to a central server through the bandwidth connectivity envisaged for the project.		
3	Video Based call management application with a live site map, the calls for help can be served practically from a remote location		
4	Software shall be capable to transfer the call to the next Pre-defined Station and ECB Monitoring System at Control Room		
5	Software should be capable to define minimum three pre-define stations to get the alert of each ECB		
6	Software should have the capability to send the alert simultaneously once any Call will be initiated between the ECB and Station, at the same time alert will be sent to VMS and audio/video recording will be started at ECB Recording Server in Control Room		

5.4 Video Monitoring, Recording & Management software

VMS from ONVIF Full Member OEM which should be tested on at least 30 Camera OEMs and 3rd party VA is mandated. The Video Monitoring, Recording & Management software (VMS) should be integrable with in-house apps developed by Indian Government.

Qualification Criteria to be adhered for selection of VMS OEM.	**Technical Compliance Yes/No**	**Remark**
OEM of VMS should be in the manufacturing for minimum 15 years globally. Bidder to submit OEM undertaking with details.		
OEM of VMS should have Service Centre Support in India from minimum last 7 years. OEM Undertaking for same o be submitted. To ensure openness will approximately all camera OEMs, the VMS OEM must have integrated 10000+ camera device at SDK/API level. Documentary evidence need to be submitted.		
OEM of camera and VMS must have supplied and executed min. 1000 IP camera license in any CCTV surveillance system project (Either directly by OEM or SI) to any state / central govt / PSU / Judiciary / or any govt. institution in last 05 years ending on the tender floating date.		
To ensure openness VMS should not be from the same OEM of CCTV camera and OEM of Video Analytics		

Sr. No	**Description**	**Technical Compliance Yes/No**	**Remark**
1	**General**		
	The Video Management System shall be a fully distributed solution, designed for limitless multi-site and multiple server installations requiring 24/7 surveillance with support for devices from different vendors. The Video Management System shall offer centralized management of all devices, servers and users and must empower a flexible rule-based system driven by schedules and events.		

	VMS shall support IP cameras (all the features & functionalities) from at least thirty (50) major camera brands with API level Integration. Documentary evidence having make detail should be mandatorily submitted.		
	The VMS application shall support all the features & functionalities of the offered cameras. Documentary proof should be submitted for same.		
	The offered VMS should have integration with 10000+ camera models at API level. Documentary evidence having camera make and model detail should be mandatorily submitted.		
	VMS shall have API based integration with the major camera vendors in order to support features such as, up to 3 Multi-streams, SD Card storage sync, Camera based Edge Analytics support, Camera I/O support, Camera Audio support		
	To ensure openness, VMS, cameras and VA should not be from the same manufacturer but should be tightly integrated on API level.		
	VMS shall support installation and ability to run on virtualized windows servers		
	VMS manufacturer shall provide their SDK (or any other integration means) libraries and documentation) to ensure a seamless integration with any other system		
	VMS shall be open to any standard storage technologies integration.		
	VMS shall be open to any video wall system integration.		
	VMS OEM should be one of the top 5 OEM from Latest Global IHS World Report for Video Management Software		
	VMS should have the possibility to integrate third party Video Analytics systems.		
	VMS should consist of only Base license and Channel Licenses. VMS should be provided with unlimited number of Failover Servers and Failover Camera Licenses.		
	The system shall act as an SNMP agent which can generate an SNMP trap as a result of rule activation in addition to other existing rule actions.		
	The system shall be able to utilize Microsoft Windows SNMP Service for triggering of SNMP traps		
	The VMS should have the feature to record client workstation screens for monitoring & to provide an account of fraudulent activities by capturing screen recordings of activities/transactions.		
	The VMS should be mandatory provided with 100 number of Client Licenses. In case of additional Licenses required, no extra cost needs to be considered.		
	The VMS should have the feature of privacy masking to conceals certain parts of the image, both in live and playback video and in exported material. It supports permanent masks and liftable masks that can be lifted and managed with user credentials. Masking level is adjustable and ranges between ‘light blur’ to ‘solid grey’		
	The VMS should support video data grooming feature to enables reduction of video recording data size by reducing the frame rate of the video data.		
	VMS should support Scalable Video Quality Recording to record high-quality video to edge storage, while a low-quality reference video stream can be recorded centrally in the recording servers		
	The VMS system shall be a scalable client – server architecture built using well known operating systems		
	The VMS system shall enable recording to be done at the aggregation sites and shall allow the local Control center to import selected video’s on demand.		
	Aggregation site types shall be categorized according to function and size as per		

	the table below.		
	To facilitate the VMS system architecture, the BIDDER shall ensure that sufficient capacity is designed into the data communications & telecommunications infrastructure to deliver the required functionality, along with the ability to allocate and reserve resources (including bandwidth).		
	The Recording server shall have the ability to handle Video Motion detection on Nvidia GPU to optimize the server requirement.		
	The VMS data communications and telecommunications network shall use a suitable transport medium and associated cabling and data transmission infrastructure that will support real-time video display of cameras at the nominated operations centers. The type of transmission network shall be determined by the BIDDER.		
	The VMS system shall be compatible to single and multiple processor servers. The server processor & hardware shall be optimized in all cases.		
	The VMS system shall cluster the processing & memory load across several machines. The failure of any one server in the solution shall not cause a failure in the entire system.		
	The VMS system device drivers shall be stored separately to the central core application to ensure any instability in 3rd party SDKs do not affect the core application.		
	The VMS management server shall be able to intelligently scan an IP network for new devices (cameras or servers) along with automatic model detection.		
	Network infrastructure and installation are the responsibility of the Bidder. Network components both active and required for the successful implementation of the video surveillance detailed in this tender shall be provided by the Bidder. The network infrastructure shall meet the streaming requirement of the project without any bottlenecks. The network infrastructure shall support UDP multicast, UDP unicast and TCP transmission.		
	The VMS system shall provide an integrated secure, scalable and easily accessible software-based solution for the management of the existing & future physical security infrastructure		
	The VMS system shall provide a powerful and efficient management interface for all the security systems across all monitored sites.		
	The Video Management System shall be a fully distributed solution, designed for limitless multi-site and multiple server installations requiring 24/7 surveillance with support for devices from different vendors. The Video Management System shall offer centralized management of all devices, servers and users and must empower a flexible rule-based system driven by schedules and events.		
	The Video Management System shall contain recording servers used for recording video feeds and for communicating with cameras and other devices. The recording servers shall process the recordings and playback the video streams.		
	The Video Management System shall include a federated architecture allowing clients on the host system with the right user rights to view video sources belonging to multiple independent Video Management Systems simultaneously, as if they were on The Video Management System shall contain a management server that shall be the central manager of the system and control recording servers, cameras, devices and users. The management server shall handle the initial client login, system configuration and logging.		
	The management server shall allow access to a system manager from where the		

	administrator can configure and manage all servers, cameras and users.		
	The system shall allow the management server to be installed on multiple servers within a cluster of servers ensuring that another server in the cluster automatically takes over in case the first server fails.		
	VMS should have the capability to integrate with 3rd party Fire alarm, Access Control Systems, BMS systems.		
	The Video Management System shall support installation and ability to run on virtualized Windows servers.		
	The VMS system shall support Device firmware upgrade of single and multiple devices in bulk from within the Management Interface		
	The Video Management System shall allow an unlimited number of cameras to be connected to each recording server and an unlimited number of recording servers to be connected to each management server across multiple sites, if required.		
	The Video Management System shall support high availability of recording servers. A failover option shall provide standby support for recording servers with automatic synchronization to ensure maximum uptime and minimum risk of lost data.		
	The Video Management System shall support a versatile rule system including scheduled or event-driven actions with numerous options including support to time profiles.		
	The Video Management System shall support latest Microsoft windows operation software. The system must use DirectX and .NET Framework.		
	The Video Management System software shall include multicast and multi-streaming support.		
	The Video Management System shall include automatic camera discovery.		
	The Video Management System shall support archiving for optimizing recorded data storage through unique data storage solutions by combining performance and scalability with cost efficient long-term video storage.		
	The Video Management System shall incorporate fully integrated matrix functionality for distributed viewing of any camera in the system from any computer with the client viewer.		
	The Video Management System shall incorporate intuitive map functions allowing for multilayered map environment. The map functionality shall allow for the interactive control of the complete surveillance system, at-a-glance overview of system integrity, and seamless drag-and-drop integration with video wall module option.		
	The VMS software must be possible to integrate customer provided GIS MAP, Google MAP, Open Street MAP only having the MAP credentials.		
	The Video Management System shall support 56-bit encryption of video for export purposes. The 56-bit encryption shall meet the requirements on export limits for encryption.		
	The Video Management System shall support full two-way audio between clients and remote devices. Two-way audio integration shall support the following features and functions:		
	The Video Management System software shall provide fast evidence export by exporting in video to various formats, including video from multiple cameras in encrypted native database format with an included viewer.		

	The Video Management System shall show full awareness of the system through audit logs and shows user activity through comprehensive logs.		
	The Video Management System shall include support for a frame work data module designed to integrate multiple third party Video Content Analysis (VCA) solutions seamlessly into client viewer environments.		
	The Video Management System shall include a Software Development Kit (SDK) that offers important capabilities for integrating the Video Management System with third party software and applications.		
	The Video Management System shall include a stand-alone viewer application to be included with video exported from the client viewer application. The viewer application shall allow recipients of the video to browse and playback the exported video without installing separate software on their computers.		
	The Video Management System shall include support for Active Directory to allow users to be added to the system. Use of Active Directory requires that a server running Active Directory, acting as a domain controller, to be available on the network.		
	The Video Management System shall be designed to support each component on the same computer for efficiency in smaller systems, or each component on separate systems for large system deployments.		
	VMS should support ONVIF S, G, T, Q & M Profile supported by IP Devices		
	VMS should be Full Member of ONVIF or Affiliate to Parent Company or Contributing membership level.		
	Video Recording Server should support Recording at different resolution for the same camera enabling to record one stream at Higher resolution at local station for 30 days and the other at minimum resolution of 800 X 600 which will be archived to central storage for predefined days. Bidder shall have option to consider more than one server per station to achieve the same.		
	Video Recording Server should support archiving minimum resolution of 800 X 600 video to Central Unified storage at scheduled hours. Archiving should resume automatically after any disconnection in the WAN link between station and central location.		
	Archived Recordings for predefined days should be deleted automatically after retention period from the central storage as per FIFO policy.		
	The VMS software must be capable to send events via SMS, email and WhatsApp provided the credentials to the designated client.		
	In case of non-availability of WAN link, Video recording Server shall save minimum resolution of 800 X 600 data internal to server for up to 7 days to avoid data loss, once the link is established the archiving should happen completely.		
	Edge Storage		
	Edge storage shall secure that when a lost or broken connection is back up, the data stored on the camera's internal storage shall be retrieved and stored in the media database. Edge storage shall secure that after recovery from a malfunction it shall be possible to play back and view the video, and audio recorded by the device, while the malfunction persisted		
2	**Bookmarking**		
	A bookmarking feature shall be included in the Video Management System, allowing the client viewer users to mark incidents on live and/or playback video streams.		
3	**Optimized Video Archiving**		

	Administrators shall be able to select a storage container for each device and move a device from one storage container to another or move all recordings inclusive archives to the new storage container, or delete them all.		
	Administrators shall be provided with an overview of the defined storage containers, their archives with path, and free and used space on the drives for each device, including the used storage space in the recording database, and in archives.		
	Video management software shall also have ability to optimize bandwidth requirement on cloud-based storage solution by Recording at local site recording server for at least 24 hours and archive to cloud on schedule basis from different recording servers at different time profile in order to utilize minimum bandwidth		
4	**Failover Support**		
	The system shall support automatic failover for recording servers. This functionality must be accomplished by a failover server that shall work as a standby unit, which takes over in the event that 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.		
	The system shall provide monitoring of all failover servers from the graphical alarm management module.		
	The system shall provide seamless access to recordings on the failover Server for all clients through the same client views once the services are fully started.		
5	**Multicast Support**		
	The system shall support multicasting of video feeds to client workstations in order to conserve network resources. Multicasting should be enabled from the recording servers and not directly from the cameras. Thus the IGMP network would be necessary only for the switches where server and clients are connected.		
	Multicasting shall send a single stream of video to multiple clients, where the stream may be decoded and displayed on all clients simultaneously. This functionality shall support virtual matrix configurations.		
	The infrastructure provided for the system shall support Internet Group Management Protocol (IGMP) for each remote network.		
	The system shall automatically switch to unicast, if the client fails to connect to the multicast stream.		
6	**Multi-streaming Support**		
	The recording server must accept, display and record individual streams of video from each camera that supports it, for example, display a stream in H.264 format and record another stream in MPEG4 format. The intent of this functionality shall be providing independent streams of video from the camera to the server with different resolution, encoding and frame rate.		
	Multi-streaming support shall allow the system to be configured with H.264 with a high frame rate for live viewing and shall allow the system to be configured with high resolution H.264 at low frame rates for recording and playback.		
	The system shall allow recorded video to be recorded at 8fps.		
7	**SNMP Support**		
	The system shall act as an SNMP agent which can generate an SNMP trap as a result of rule activation in addition to other existing rule actions.		
	The system shall be able to utilize Microsoft Windows SNMP Service for		

	triggering of SNMP traps.		
8	**NAT Firewall Support**		
	The system shall support port forwarding, which must allow clients from outside of a Network Address Translation (NAT) firewall to connect to recording servers without using a VPN.		
	Each recording server shall be mapped to a specific port and this port must be forwarded through the firewall to the recording server's internal IP address.		
9	**Management Server Redundancy**		
	The management server shall provide a resilient system solution based on Windows Server Clustering and Native, to secure maximum uptime.		
10	**Centralized Search**		
	The system shall have dedicated tab for searching recording sequences, bookmarks, events, motion, alarms. These Search categories can be combined, also with third party search agent plugins. Save search templates. Visualize location of Search result. Integrates with technology partner solutions		
11	**Motion Detection**		
	The system should have built-in, real-time, camera-independent motion detection with the ability to generate motion metadata for Smart Search.		
	The system should also support motion-based recording feature.		
12	**Alarms Support**		
	The alarm support shall allow for continuous monitoring of the operational status and event-triggered alarms from servers, cameras and other devices.		
	The alarm support shall provide a real-time overview of alarm status, or technical problems, while allowing for immediate visual verification and troubleshooting.		
13	**Matrix Functionality**		
	The system shall include an integrated matrix solution for distributing video to any computer with the client viewer installed. A computer on which the matrix-triggered images can be shown must be known as a matrix recipient.		
	The client viewer shall provide remote users with a comprehensive suite of features:		
	It shall be possible to view live video from cameras on the surveillance system from 1 to 100 per view.		
	It shall be possible to playback recordings from cameras on the surveillance system, with a selection of advanced navigation tools, including an intuitive timeline browser.		
	It shall be possible to create and switch between an unlimited number of views, each able to display video from up to 100 cameras from multiple servers at a time. The system shall allow views to be created which are only accessible to the user, or to groups of users based on 37 different layouts optimized for 4:3, 4:3 Portrait, 16:9 and 16:9 Portrait display ratios.		
	It shall be possible to access views of cameras on any PC with a client viewer application installed.		
	It shall be possible to use multiple screens as well as floating windows for displaying different views simultaneously.		
	It shall be possible to quickly substituting one, or more of a view's cameras with other cameras.		
	It shall be possible to view images from several cameras in sequence in a single camera position in a view – a so called carousel.		
	It shall be possible to view video from selected cameras in greater magnification		

	and/or higher quality in a designated hotspot.		
	It shall be possible to receive and send video through the matrix functionality.		
	The VMS software must have client in English and Hindi language.		
	It shall be possible to include HTML pages and static images (for example, maps, or photos) in views.		
	It shall be possible to control PTZ cameras.		
	It shall be possible to use digital zoom on live as well as recorded video.		
	It shall be possible to activate manually triggered events.		
	It shall be possible to activate external outputs (e. g. lights and sirens).		
	It shall be possible to use sound notifications for attracting attention to detected motion.		
	It shall be possible to get quick overview of sequences with detected motion.		
	It shall be possible to get quick overviews of alerts.		
	It shall be possible to quickly search selected areas of video recording for motion.		
	It shall be possible to skip gaps during playback of recordings.		
	It shall be possible to configure and use several different joysticks.		
	It shall be possible to print images, with optional comments.		
	It shall be possible to copy images for subsequent pasting into word processors, email, etc.		
	It shall be possible to export recording (for example, for use as evidence) in AVI, JPEG and database formats.		
	It shall be possible to use pre-configured as well as customizable keyboard shortcuts to speed up common actions.		
	It shall be possible to insert overlay buttons, for example, for activation of speakers, events, outputs, movement of cameras etc.		
	It shall be possible to use a sequence function that lists thumbnail images representing recorded sequences from an individual camera or all cameras in a view.		
	It shall be possible to use a forced playback mode allowing the user to playback recorded video from inside the ‘live’ mode while viewing ‘live’ video.		
	The client viewer shall support the use of 3-axis USB joysticks for control of pan, tilt, zoom and auxiliary camera functions.		
	The Client should support multiple languages including English & Hindi language		
	The client viewer shall support the use of multimedia control devices, which are capable of emulating keystrokes, for the efficient review of recorded video.		
	The client viewer shall support the use of keyboard shortcuts for control of standard features. It shall allow the user to program numerical keyboard shortcuts for camera views. The shortcut number shall be displayed with the view description in the live and playback displays. The shortcut shall allow the user to change views with 2 to 3 keyboard entries.		
	The client viewer shall support GPU based video decoding to improve video rendering performance and up to 75% reduction in CPU load of the workstation running Client software. The use of GPU based video rendering shall also make client ready for 4K/UHD camera technology.		
	VMS System should Support to Manage device password on one or multiple devices from within the VMS Client		
	The client viewer shall have the capability to receive multicast streams. The client		

	viewer shall have the capability to detect if the network becomes unreliable and to automatically switch to unicast to ensure that the operator is able to receive video.		
	The operator shall have the ability to use digital zoom where the zooming is performed in the image only on any number of cameras simultaneously. This functionality shall be the default for fixed cameras. The use of digital zoom shall have no affect on recording, or other users.		
14	**Map Functions**		
	Built-in map function in the client viewer shall provide an intuitive overview of the system and shall offer integrated access to all system components.		
	Map function shall be able to use standard graphical file formats including: jpg, gif, png, tif, etc.		
	It shall be possible to use any number of layered maps, and it shall be possible to easily drag-and-drop and point-and-click definition of cameras, servers, microphones, speakers, I/O devices, hot-zones, and PTZ camera presets.		
	Hot zones shall be allowed for intuitive navigation between different map levels.		
	Map function shall support instant camera preview when moving the mouse pointer over a specific camera.		
	Map function shall support central overview of the surveillance system via an alarm list containing alarm indicators of high, medium or low prioritized alarms. Furthermore the alarms shall be categorized by the following states; new, in progress, on hold, or closed. Alarms must be possible to acknowledge by right-clicking elements on maps.		
	The VMS software must be integrated with Google MAP, GIS MAP etc.		
	Cameras can be possible to position on the MAP by using latitude and longitude.		
15	**Remote Client Viewer**		
	The web-based remote client viewer shall offer live view of up to 16 cameras, including PTZ control with joystick, fisheye (360 degrees) cameras and event/output activation. The playback function shall give the user concurrent playback of up to 16 recorded videos with date, alert sequence, or time searching.		
	The web-based remote client viewer shall offer quick overviews of sequences with detected motion.		
	The web-based remote client viewer shall be able to generate and export evidence in AVI (movie clip) and JPG (still image) formats.		
	The system shall support the use of separate networks, VLANs, or switches for connecting the cameras to the recording servers providing physical network separation from the clients and facilitate the use of static IP addresses for the devices.		
	The system shall support H.264,H.265, MPEG-4 (Part 2), MPEG-4 ASP, MxPEG, and MJPEG compression formats for all analog cameras connected to encoders, and all IP cameras connected to the system.		
	The system shall support dual-streaming cameras and shall cover the following compression formats: H.264, MPEG-4 (Part 2) and MJPEG.		
	The recording server shall utilize high performance ISCSI, SCSI, SAS and SSD disk drives for online recording storage and shall allow the use of lower cost SATA drives for the RAID arrays for online archive storage. Use of online archiving shall		

	ensure that data always is readily available. Use of tape-backup systems shall not be acceptable.		
	The system shall allow 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.		
	The recording server(s) shall have the ability to support multiple Network Interface Cards (NIC) and shall support connection to the cameras on a network separate from the client viewer, management server and system manager.		
	The recording server shall have the ability to accept the full frame rate supplied by the cameras, while recording a lower frame rate yet still shall make the higher frame rate available to the clients for live viewing.		
	The VMS software must provide minimum 2 technological updates yearly with in the warranty support time of 3/5 years to upgrade the system automatically to accept the new upgraded technology and new devices smoothly into the system.		
	3rd Party System Integration Access Control should be integrated thru VMS Access Control Module or thru SDK/API integration. FAS System to be integrated thru API/SDK or thru Bacnet Over IP Protocol Plugin with VMS BMS System to be integrated thru API/SDK or thru Bacnet Over IP Protocol Plugin with VMS		
	VMS manufacturer shall provide their SDK without any additional charges (or any other integration means) libraries and documentation) to ensure a seamless integration with any other system.		
	The VMS software must have the ability to operate in a FIPS 140-2 compliant mode.		
	The VMS software must ensure compliance with GDPR data privacy law requires careful planning and preparation of the design of your video surveillance system and the policies and procedures regulating how it is used.		
16	**Remote Mobile App**		
	Integrated Mobile Application to monitor overall CCTV system and for required coordination during emergency		
	Mobile Client support Native mobile app for smartphone or tablet users, for easy access to live and playback of cameras, and to activate system events and outputs. Additionally, for use as a remote recording device by using the mobile device's built-in camera, whereby video from the device's camera is streamed back to the VMS and recorded like a standard camera.		
	Support Smart Connect: Easy configuration of internet access to the mobile server by automatic configuration of firewalls and internet routers via UPnP, with verification of configuration and operation of internet connection, with option to email connection details to mobile client users. Includes automatic mobile server on LAN via UPnP.		

	Shall support Android as well as Apple IOS software, with respective smart phones		
	Provide mobile client capability for mobile device users to use their mobile device cameras as cameras in the VMS		

5.5 Technical Specifications of AI Based Video Intelligence Platform

AI based Integrated Security Management			**Technical Compliance (Yes/No)**	**Remark**
Policing Platform				
Sr. No	**Key**	**Description**		
1	**Unified Platform for Deployment, Training, Scaling and Management of all the video AI related application and Hardware provisioning**	**Singular Unified Video AI Platform -** The Platform shall be a singular and unified AI based Video Intelligence platform capable to run all the Surveillance, Women Safety, Citizen safety, encroachment detection and any other Video Analytics use cases on a single platform, namely -		
		Surveillance Related –		
		Facial Detection		
		Advance Intrusion Detection		
		Women Safety		
		Vandalism		
		Crowd Estimation and Management		
		Abandon Object Detection		
		Person Collapsing		
		Encroachment Detection		
		Stray animal Detection		
		People Fighting/Violence		
		Perimeter Detection		
		Camera Health Monitoring		
		Each of the video analytics use case shall be able to run on a unified video intelligence platform. Where the platform shall have the capability to support several multi-vendor/OEM video analytics applications that can be deployed on any camera or video-feed seamlessly.		
		Hardware Provisioning for Surveillance Application -		

		The inferencing hardware provisioned to run the video analytics application should be common to all the applications irrespective of the type of architecture of deployment. Any application including but not limited to surveillance apps like FRS, person attribute etc. should be capable of running on any device be it a central server or an edge based device or LPU .		
2	**Dynamic Deployment**	Each of the video analytics use-case shall be structured as an independent module that can be deployed on any camera using a simple user interface utility, providing a complete visibility of the use cases and which cameras they are running on.		
		The platform should have utility of scheduling each use case on individual camera by minimum of an hourly granularity.		
		The user should be able to easily select the camera by tag, groups or locations and schedule applications on any camera.		
3	**Advanced AI compatible**	The Video Analytics system shall be compatible with the latest technological advancements in the domain of computer vision and AI. Hence, it shall be able to quickly adapt to newer libraries and AI advancements. All the analytics and use-cases shall be based on advanced AI technology and shall not depend on traditional algorithms.		
4	**Libraries and frameworks**	The system shall be fully compatible with popular Computer Vision and Artificial Intelligence frameworks including but not limited to OpenCV, OpenVINO, Tensorflow, CAFFE, Pytorch, MXNet, TensorRT, Keras and Darknet from day one		
5	**Training new models**	The system shall allow seamless training by labelling any objects within the images and providing them suitable attributes of multiple types such as class, subclass, colour, type etc. The system shall allow training to happen continuously, on demand or on periodic intervals, which shall be configurable.		
6	**Annotation Capabilities of the Platform**	The system shall have an inbuilt annotation tool that allows a user to label the images with relevant information using both rectangle and polygon drawing facilities.		

		The annotation should allow labelling of images or drawn objects with different class names. In case of persons, it should also support labelling of various attributes such as color of clothing, type of clothing, age, gender etc as well.		
		The annotation tool should have a comprehensive project management feature, including assigning annotation jobs on a set of images to individual users. The system should also have support for higher privileged users who can approve/disapprove the annotations done by the annotators.		
		The user should be able to train new deep-learning models from the annotated data using the Annotation UI itself. The user-interface should allow to plug-in the trained model in any of the relevant Video Analytics use-cases dynamically at each camera.		
		The system should allow the user to plug newly trained AI models at runtime by simply selecting the models in the per-camera configuration page		
		SI to consider sufficient hardware and sizing as required for optimal running of proposed software during design phase.		
7	**Model Comparison**	The System shall have a library (This library has to be regularly updated over the time) of standardized AI models developed by the OEM of the Video Analytics System, academic institutions and members of the developer community. These models shall be used for comparing and benchmarking the performance of newly developed models. The system shall allow for both qualitative and quantitative comparison of models, i.e. it shall allow the end user to compare individual parameters of the model (such as learning rate) as well as the overall performance of the model on any given dataset when compared to a standardized model.		

8	**Monitoring and analytics**	Autonomously objective metrics shall be available to be evaluated and Insights into the performance of each algorithm, model and their versions shall be made available to key stakeholders or users as defined. Visual map of composition, workflow, usage analytics, resource utilization, failure points etc. would be made available to provide complete control of A.I. workload.		
9	**Key UI View and operational functionalities of the Video Intelligence Platform**	**The System shall provide the following key results from the use case**		
		Event Notifications: The result of each of the use case shall be in the form of events that contain the screenshot with other metadata describing the event, such as detected objects, timestamp, camera/video that generated the event and all other metadata representing the event from different use cases. The User Interface shall have a grid and list view with all the events from different use cases, cameras etc. These features should be also supported through a mobile application to may be utilized by various users in future.		
		There should be option to export data (video, insights, analysis, etc. files) to a suitable file format		
		The system should support customization of alerts, video feeds, and priority-based alerts for individual users from day one.		
		Resource Management View: The User interface shall provide a list of all the resources available in the system such as computing servers and cameras. The status of each of the devices, whether they are online/offline shall also be available at all times.		
		AI Training Tool: The User interface shall have a training tool to annotate and label images from the events to train new AI models and update the existing ones. The training tools shall also contain a list of all the models available in the system, which can be plugged into any AI use case easily.		

		Use case deployment matrix: The user interface shall have a matrix to assign, start, stop and schedule any use case on any camera. The status of active and non-active use cases shall be clearly visible with colour coded information.		
		There will be 2 video analytics use cases deployed per fixed camera on an average.		
		Video Synopsys UI- The Video Intelligence shall provide an intuitive UI for Vide Synopsys. Able to analyze all the recorded video files and provide the operator with synopsis video for quick review and investigation thereby reducing viewing time considerably. The video files from all the 3rd Party Video Management Software (VMS) shall be supported.		
		Data Analytics Dashboard: The user interface shall also have an analytics dashboard listing all the patterns of events from different cameras with a heat-map of number of events on an hourly basis.		
10	**Common UI for all the use-cases**	The user interface shall be a unified dashboard that shows events from all the Video Analytics use-cases and all the cameras in a common UI, and which gets populated in real time from event notifications.		
11	**Web based Interface**	The User based access and interface of the system 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.		
		The alerts and notifications should be based upon the user profile.		
		The user can log in from any device and yet should be able to access the system according to his/ her profile .		

12	**Live Video Interface**	The User interface shall allow a user to view the live video stream from any camera with overlaid information of regions, objects, people and vehicles based on each of the use-case		
13	**Configuration per-use-case per-camera level**	The system shall allow each use-case to be uniquely configured for every individual camera stream, with parameters for camera calibration, image quality improvement, night/day settings etc. .		
		Each use-case shall be able to run on different cameras with different settings (e.g., different Zones for Intrusion, different lines for line crossing detection, etc.) at different hours of the day.		
		The configuration page shall allow a user to choose any of the available AI models to detect and classify objects within the image. The description of the models shall clearly specify performance and hardware requirements of each of the model.		
14	**Camera Calibration Tool**	The Video Analytics system UI should have an in-built 3D camera-calibration tool that can take user inputs such as reference-heights, reference depths and floor landmarks to calibrate the camera. The calibration tool should have an option to use the GPS coordinates of the camera location.		
		Once the camera is calibrated, each detected object should also be assigned real-world coordinates with respect to the Camera GPS coordinates.		
		This functionality should be available for each camera added in the VA system		
		The OEM should ensure that there should not be any geometric distortions on the deployed cameras.		
15	**Key configuration parameters**	The use case on each camera shall allow setting up configuration of multiple detections zones such as lines and regions that can be used to define perimeters, regions of interest.		
		The configuration user interface shall allow adjusting various sensitivity and confidence parameters to adjust each video-analytics use-case’s performance with respect to the physical deployment of the camera.		

16	**Filtering and Retrieval**	The system shall allow a user to filter and retrieve all the events based on any combination of the following parameters:		
		- Time of the event		
		- Objects in the event		
		- Type of the use-case		
		- Camera Location etc.		
17	**Transparent and Open Architecture**	The architecture shall clearly demonstrate the technology stack with layers of the core platform, data governance and interface to different software application		
18	**Highly parallel and distributed**	The algorithms powering the video intelligence system shall possess capability to operate parallel and distributed manner across a cluster of machines. Both training of AI algorithms and inference shall be distributed.		
19	**User Management**	The system shall support user with a hierarchical access level, with different access level for different users demarcated with respect to cameras, locations and the data. The user access control system shall allow setting of SOP's like CRUD (Create, Read, Update and Delete) operations for each user.		
20	**Deployment of use-case across any camera**	The system shall allow deployment of any use case on any camera without any MAC level or IP level locking. Ideally any use case shall be deployable and redeploy able on any camera or video source as far as the camera view supports such use cases to be deployed.		
21	**Video Compatibility**	The System shall be a real-time video analytics engine that utilizes advanced image processing algorithms to turn video into actionable intelligence. The AI based Video Analytics system shall consist of video-processing & analytics engine that works seamlessly both on saved videos or camera streams in real-time and provide events to the user based on the use-case basis. The system shall be compatible with all ONVIF compliant IP cameras with H.264/H.265 video decoding.		

22	**Centralized Deployment Support**	All the video streams shall be processed centrally at the Data Center with one or more servers for video processing. The user shall be able to log in to the system through the central dashboard to access all the data from all the servers. The processing of videos as well as alert generation shall be done on premise. At no point in time shall the data from the site be shared over the internet or sent over to the cloud. The System UI shall only be accessible using workstations and terminals available on premises.		
23	**Support for third-party use-cases**	The AI system shall also support third-party developed algorithms and use-cases that can provide the user with a large base of use-cases to choose from.		
		If a new use-case needs to be developed based on Video Intelligence, the system shall provide a developer Software Development Kit (SDK) for this purpose. The SDK shall be provided along with detailed documentation for building end-to-end use-cases on the system.		
		The system shall also allow the user to plug different AI models in the individual running of the video analytics use-case.		
24	**Flexible Technology Stack**	The technology stack shall be modular and scalable based on containerized micro services. Each use-case shall be orchestrated as a stand-alone micro service, which communicates with a central server for exchanging of the data.		
		A.I. micro services components shall be agnostic to language used in technology stack. It shall work with any language, framework, and library of choice without any impact on the rest of the architecture. This type of flexibility will ensure lower friction for collaboration and deployment of AI.		

		Algorithms being containerized shall ensure both interoperability and portability, allowing for code to be written in any programming language or any version of library and framework but then seamlessly exposes a single API to be integrated and ported with multiple modules/AI components of diverse stack. It shall seamlessly integrate with other components and shall be portable/ replicable easily across the machines automatically.		
		High Availability and Virtualization Support - The Video Intelligence platform should support HA and Virtualization from Day 1.		
25	**General VA specifications**	The Video Analytics shall be based upon Machine Learning and Deep Learning framework.		
		To save the duplication of the video storage, the analytics should flag the video for the configurable duration of time pre and post event in the Video Management System. It should be possible for the operator to jump to the alert flag in the archived video for detailed investigation of the event.		
		It shall be possible to run the analytic as per hourly/daily/weekly schedule. There should be a provision to define multiple such schedules. It should be possible to set the schedule to any analytic use case. It should be possible to assign multiple analytics on the same camera.		
		It is possible to generate email or a text message to the designated recipients in case critical alerts are generated. The application shall escalate the alert to the designated users through email or a text message in case the alert is not acknowledged by the operator in a specified period of time.		
		It shall enable common configuration settings in a batch mode on multiple cameras.		
		The application shall allow searching the analytics events based on priority, date and time (from and to) and camera. It should be possible to generate statistical analysis of various use cases across the time of the day.		

		The analytics shall enable the operator to define an unlimited number of detection regions per camera. The system shall allow setting each region independently to be 'Active for Analytics' for any given period of time of the day.		
		The analytics events shall be stored in the database. In case the events are purged, the purged events stored to external files for later reference.		
		For Vehicular Analytics, it is possible to deploy the analytics in centralized architecture where all the feeds from the cameras are available in the Data Center and analyzed centrally.		
		The system shall have a single client application for setting analytics, live viewing, archived viewing, and the administrator functions.		
26	***Video Summarization System Functional Requirements & KPIs:***	The proposed solution should help in making Video Searchable, Quantifiable and Actionable, reviewing long duration of video in short time; quantitatively analyze video to derive actionable insights for data driven safety, security and operational decision making. The proposed system should be state of the art image processing technology essentially creating condensed summaries of original, full length video recordings, while preserving all objects and events of interest. These should be presented either simultaneously or in rapid succession, regardless of the time point and sequence in which they occurred, effectively providing operators with a clear view of activities and enabling them to rapidly review and home in on events of interest.		
		The system should provide operators, what they need to quickly scan through video data to find suspicious, out of the ordinary or potentially criminal aspects. After detecting an object of interest, the user shall be able to select to see the object in its original form in the original video which can then be exported.		

		Video Summarization tool based on attributes and meta data field will facilitate to reach to relevant and meaningful content for the defined search meeting the requirements for effective post investigation analyses within shorter time span.		
		System shall be able to analyze all the recorded video files and provide the operator with Summarization video for quick review and investigation thereby reducing viewing time considerably.		
		a. The video files from all the 3rd Party Video Management Software (VMS) shall be supported.		
		System shall support: -		
		· Shall support Video File exports from all kind of 3rd Party VMS and even the video files recorded from a Mobile Or any other kind of Analog Camera.		
		· System shall be able to enhance safety and security with quick rapid human response to critical events recorded on video		
		· Shall support Video File exports from all kind of 3rd Party VMS and even the video files recorded from a Mobile Or any other kind of other video sources.		
		· Shall automatically extracts objects from the original video and efficiently reconstructs and superimposes them back in the original scene, simultaneously displaying events that have occurred at different times.		
		· System shall rapidly pinpoint people and vehicles of interest, using an extensive range of appearance and movement filters, across multiple video sources from different cameras installed in the premises.		
		· Shall Instantly locate people, vehicles, and items of interest by searching for similar looking objects.		
		· System shall display time-stamps for various objects in the video continuously, while the summarization is played.		
		· Shall provide a web interface to upload the video files, generate the Summarization & for the management of multiple investigation cases		

		· System shall provide density control while replaying the Summarization video. Density refers to the number of events shown concurrently when playing a Summarization.		
		· The density control shall increase or decrease the number of events shown at once also changing the event density shall alter the run time duration of the video Summarization thereby enabling quick review time.		
		· Time Range - Limit the search criteria to specific time ranges		
		· Source - Limit objects to specific cameras or files		
		· Class – Video Summarization shall be shown based on People, Two-Wheeled Vehicles, Other Vehicles and Animals		
		- People Class: Man, Woman and child.		
		- Two-Wheeled Vehicle Class: Bicycle and Motorcycle		
		- Other Vehicles Class: Car, Pickup, Van, Truck, Bus		
		- Bags: Backpacks, Hand-held Bags		
		- Hats: Hats, No Hats		
		- Upper Wear: Short/No Sleeves, Long Sleeves		
		- Lower Wear: Long, Short		
		· Colour - Identify objects according to any combination of Brown, Red, Orange, Yellow, Green, Lime, Cyan, Purple, Pink, White, Grey and Black		
		· Size - Select objects based on their actual (real-life) size from a histogram of sizes relevant to a specific case		
		· Speed - Select objects based on their actual speed from a histogram of speeds relevant to a specific case		
		· Dwell - Select objects dwelling for longer than a certain period in a scene		
		· Area - Identify objects included or excluded within one or more user-defined 3- or 4-sided polygon areas. The user shall be able to set the minimum duration the object spends inside the area.		
		· Path - Identify objects traveling along one or more user-defined paths. The user shall be able to set the minimum duration the object spends inside the area.		

		· Appearance similarity – System shall be able to do filter and display only the objects matching similar-looking people (People Similarity) or Vehicles (Vehicle Similarity).		
App Specification – Abandon Object detection				
S. No.	**Key**	**Description**		
1	**App detection**	The app should be able to detect Left and Unattended baggage in a camera view.		
2	**App Reporting**	The app should report the incident with an image marked with the region / area where unattended baggage is detected.		
App Specification – Person Collapsing				
S. No.	**Key**	**Description**		
1	**App detection**	The app should detect if a person walking upright has collapsed or fallen on the ground.		
2	**Configurable parameters**	The user should be able to configure the amount of time beyond which if the person is on the ground, the system should raise an alert.		
3	**App Reporting**	This app should raise an alert if any pedestrian is Jay walking.		
		The app should provide zone wise data of both the pedestrian movements at zebra crossings and jay walking with a minimum of hourly granularity.		
App Specification – AI Based Advance Intrusion Detection				
S. No.	**Key**	**Description**		
1	**App detection**	The app should be able to detect an act of intrusion. Intrusion herein refers to the instance of an individual crossing a pre-defined virtual fence defined by the user.		
2	**Configurable parameters**	The user should be able to configure the length and orientation of the virtual fence. She should also be able to define the direction in which crossing the line would be considered as intrusion. App shall have intelligence of identifying intrusion done by Human , vehicle or Animal		
AI based Crowd Estimation and Management				
S. No.	**Key**	**Description**		

1	**Introduction**	Crowd Estimation and Management (CEM) Video Intelligence system shall allow estimation of crowd density within the camera view. This is an important tool for understanding the crowd movement and management for the security and facilities management agencies. System shall raise an alert if the crowd density within a camera view is above a certain threshold.		
2	**Deployment**	The CEM System shall be a purely computer vision and artificial intelligence-based system that be deployed on all the existing and new CCTV cameras, including box cameras and PTZ cameras.		
3	**Camera compatibility**	The system shall be completely independent of the make/model of the cameras and be compatible with ONVIF compliant cameras. The CEM system shall support H264, H264+, H265 and MJPEG video streaming from cameras.		
4	**Accuracy on datasets**	The CEM system shall have 85% average accuracy in estimation of crowd on public databases and/or real time situation to be given during proof of concept time/need to submit the test report. The accuracy should be estimated in a test dataset following standard train/validation/test split methods-during detailed engineering and design phase.		
5	**Ability to define regions**	The CEM system shall have an ability to annotate multiple regions within the camera view and the user shall be able to specify crowd thresholds for each of the regions separately. If within any region the crowd density estimation if above the user defined threshold, the system shall raise an alert.		
6	**Alerts**	The system shall raise alerts in case of the following:		
		- The CEM system shall raise an alert if the density of crowd is above a user-defined threshold.		
		- The system shall raise an alert in case of erratic movement detected within the crowd		
		- The system shall raise an alert if there is any chance of stampede or overcrowding due to increase in flow rate and erratic movement		
		- The system shall trigger alarm if more than desired density is observed near specified regions of interest.		

7	**Crowd flow estimation data**	The CEM system shall also provide a data of crowd flow from one user-defined region to the other, in case of two regions selected by the user.		
8	**Data representation**	The CEM system shall have an MIS system with a detailed report and dashboard on crowding events and data at a minimum of hourly granularity.		
		- The system shall report Crowd Density and direction to load-balance various gates.		
		- The system shall provide detailed counts of total visitors in hourly/daily/weekly/monthly and overall.		
		- The system shall also provide IN and OUT counters for all the visitors		
9	**Heat Maps**	The CEM system shall have an option of generating real time heat maps of crowd density.		
AI Based Camera Health Monitoring				
S. No.	**Key**	**Description**		
1	**Camera Status**	The Camera Health Monitoring app should be able to monitor the status of the camera and report an alert in case the camera is not functional or tampered with intentionally or unintentionally.		
2	**View Obstruction**	It should detect and raise an alert if the camera view is obstructed by any foreign object. The user should be able to adjust the threshold parameters of extent of obstruction in terms of percentage of camera view		
3	**Bright Light Shown**	The app should be able to detect and raise an alert if the camera view is tampered with bright lights. The system should specifically identify it as a camera tampering event with light shining.		
4	**Camera View Changed**	It should raise an alert if the camera view is changed/moved suddenly.		
5	**Illumination Too Low**	It should raise an alert if the camera scenes gets too dark below a threshold.		
6	**Camera Connectivity**	It should raise an alert if the camera is turned off or connectivity is lost.		
7	**Notification with Health Type**	The health monitoring app should notify the user with the type of camera health issue, namely: View Obstruction, Bright Light Shown, Camera View Changed, Low Illumination and loss of connectivity		
8	**Sensitivity Management**	It should have provision to adjust the sensitivity of detection on each camera		

Facial Detection System				
S. No.	**Key**	**Description**		
1.	**Detection**	Face Recognition System shall work on real time and offline mode for identifying or verifying a person from various kinds of inputs from digital **image file** and **live video source** from any IP video streaming sensor like IP Camera, Body Worn Cameras, Mobile handset cameras, UAV/Drones etc.		
2.	**Live and Offline Mode**	FDS shall be able to capture face images from live & pre-recorded CCTV feeds received		
3.	**Detections in crowd**	The system shall be able work to detect more **than 20 faces** in crowd on moderate face rotation either horizontal or vertical. It should support a yaw angle of **-40 to +40 degrees**, a pitch angle of -30 to +30 degrees and a roll angle of -30 to +30 degrees.		
4.	**Detection of partial faces**	The FDS shall recognize partial faces with varying angles from multiple videos simultaneously from Video clips, Group Photographs and VMS Playback directly from FRS Client Interface. FRS shall be able to process uploaded pre-recorded video feeds with a speed of up to X20, depending on the proposed hosting hardware and the video quality		
5.	**Ability to add reference Images**	The system shall be able to add photographs obtained from law enforcement agencies to the criminals' repositories tagged for sex, age, scars, tattoos etc. for future searches.		
6.	**Support for cameras/video formats**	The system shall support diverse graphic & video formats as well as live cameras. FRS shall support day/night operation with ability to detect faces both in colour and in black/white mode by using any H.264, H.265 Fixed IP and PTZ Cameras with IR Illuminators without any special configurations required		
7.	**User-management**	FRS must support a user management module that enables different user level groups to support various permission levels.		
		FRS client shall have ability to share recognition data like images & videos with multiple users and operators for better reference, alarm & incident management.		

8.	**Image Enhancement Capabilities**	FRS system must have capability to enroll whatever images fed in the system with image enhancement and ability to verify the quality of the enrolled images with different colour indicator for low quality images enrolled in watch list/database.		
9.	**Image Format support**	The system shall be able to utilize any of the file formats like JPEG, PNG, BMP, TIFF etc. format for enrolment.		
10.	**De-duplication**	FRS shall be able to check if new enrolled face is already enrolled in the database before registering the new enrolled face in the system. Also, the system shall be able to find a previous detection of a POI (person of interest) upon enrolment to watch list (retrospective search) in less than 2 sec.		
11.	**Enrolment of faces**	The system shall have option to automatically enroll face images from CCTV cameras/video source. This functionality should also be provided through the Video Intelligence platform in addition to the FRS application.		
		The system should also have an option for Bulk Enrollment either from file system or a 3rd party databases such as UID, SAARTHI, IT, NCRB, EPIC etc.		
12.	**Categories of database faces**	The system shall have capacity to create different categories of people with option to customize the matching threshold for different categories.		
13.	**Full HD Support**	The system shall be able to work on full HD Camera video with maximum performance.		
14.	**Implementation**	The system shall be able to be implemented on IT hardware like Server or Workstation.		
15.	**OS Support**	The FRS algorithm should be able to use proven open source tools and technologies like Linux to bring down the total cost of ownership of the solution. FRS running on any other OS should be supplied with Pre-Licensed Server based latest version OS like Microsoft Server 2016 and Microsoft SQL as needed by the application		

16.	**Database Support**	The system shall employ database system like MS SQL/ MYQL/ Leading Open Source Database/Sybase/ Mongo DB/ Postgres/Oracle etc. The FRS system should natively integrate with Video Intelligence platform and use a common database of the platform, so that common queries can be made on the common database for faces detection and other events.		
17.	**Algorithm Benchmarking**	The Vendor should have any performance benchmarking certificate. NIST certificate will be preferred.		
18.	**Performance**	The system must perform a full 1: N search of the probe image in under 5 seconds against a database of up to 50 mn face records.		
19.	**Mobile Application Support**	FRS Software vendor shall have mobile application of the same FRS software to support iOS and android based smart field devices. Mobile application shall be capturing the face of suspect in field and sending back to the FRS server for matching. Matching result shall be shown on the mobile application screen with matching score. There shall be provision in mobile application to stream mobile device camera as video streamer.		
20.	**Detection robustness**	System shall be able to detect the faces across the multiple CCTV video sources for online (real-time) and offline modes regardless of following conditions:		
		a. Changes in Facial expression		
		b. Changes in facial hair or hairstyle		
		c. Changes by moderate aging (up to 15 years)		
		d. Partially hidden faces or occluded faces like wearing dark glasses mask etc.		
		e. Changes in lighting conditions		
21.	**Search Capabilities**	Simple Search UI that facilitates quick and easy access to the collection of events recorded by the system without the constant monitoring by operators and must perform a full 1: N search of the probe image in under 2 seconds against a database of up to 5-8 Million POIs. It shall support following		
		a. Search previous events by images from previous detections		
		b. Search previous events by images uploaded by operator		

		c. Search previous events by enrolled names		
		d. Search previous events by date and time		
		e. Search previous events by watch list group		
		f. Search in Watch list by image		
22.	**Retrospective Search**	FRS shall have capability of Search backwards for previous detections and/or recognitions (events) of the detected person without enrolment from live CCTV & other forensic videos / offline videos		
23.	**Up to 5 nearest matches support**	FRS shall have ranking features to show next 5 closest & similar subjects in the Watch list with nearest score to the detection. This option enables you to review POIs that are potential matches for this detection for efficient system performance.		
24.	**OEM owned algorithm**	The FRS OEM should have ownership of Face Recognition Engine /Algorithm for any custom specific development as required by client		
25.	**Map feature**	FRS must allow tracking of person on maps to be uploaded in the system for cameras connected to FRS and shall highlight the camera location on the map for each detection/alert.		
26.	**SDK/API for integration**	FRS shall provide an SDK/API for integration with any third-party software like C4I (Command, Control Communication & Compute Center). API must be available with a full set of documentation of each method with accompanying sample code. All FRS function shall be fully accessible via API.		
27.	**Video Alert**	FRS shall be able to play a short video clip of the moment of face detection without dependency on VMS which can be downloaded/exported/saved for evidence proof		
28.	**Timeline of detections**	FRS shall provide timeline sequence of all detections of subject with date, time & location.		

29.	**Email Integration**	FRS shall support email Alerts via Gmail, Outlook or via an Exchange SMTP service. Different recipients can be defined for different Camera Groups. User shall be able to define how frequently recognition/detection emails are sent, the email subject and the email sender (among other things). The email itself includes the timestamp of the detection, the score, the description, the reference image (defined in the Watch list) and the detected image.		
30.	**Minimum hardware support**	FRS Application Engine must be able to run a minimum of 20 FRS Camera Channels per Server. (Server with 128 GB RAM, 3 NVIDIA Tesla T4 card with 40 cores.) Other optimized and better sizing shall be accepted.		
31.	**Use of AI accelerator hardware**	FRS shall use extensive AI Technology and perform video processing on GPUs like NVIDIA; INTEL or similar as per design & sizing vetted by AI FRS Algorithm OEM. The number of servers to be supplied, shall be based on the number of camera channels on which the FRS needs to be performed.		

5.6 VMD (Variable Messaging Display)

Technical Specification	**Compliance (Yes / No)**	**Remarks**
· LED Pixel Pitch is 4mm or better.		
· Colour of LED: Full Colour, class designation C2 as per IRC/EN 12966 standard		
· LED Pixel Configuration: SMD		
· Certifications:		
o ISO 9001:2015		
o ISO14001:2015		
o OHSAS18001:2007		
o EN12966		
o BIS		
· LED package vendor acceptable makes (certificate from the LED package vendor to be provided during the supply certifying the same)		
· Cree /Nichia/Nationstar or Equivalent		
· LED Display Size in mm is 3000 (H) x 1500 (L) X 200 (W)		
· LED Active area in mm is 2880 (H) x 1248 (L)		
· LED Display Brightness is 6000 cd/m2		
· System Contrast Ratio is 5000:01:00 /		

· LED Display Brightness Control: Manual / Auto / Scheduled		
· System Viewing Angle: 140° / 140°		
· System Luminance Class/Ratio: L3 as per IRC/EN 12966 standards.		
· System Grey Bit is 16Bit.		
· LED Modules should have Anti-UV mask, black matt without any reflection, and Fire retardant.		
Ø Installations by OEM:		
· OEM should have at least 80 Nos installations of outdoor LED wall in a single network with content being published centrally and control also being done centrally. Proof of this should be submitted. Size of these installs should be similar or bigger and should be in India running for at least 1 year successfully.		
· OEM should have a registered office in India for minimum 4 years from this tender.		
Ø Cabinet Specification		
· IP Class of LED Display Front: IP65 / Back: IP54		
· LED Display Maintenance: Back Service		
· Material for VMS frame: at least 2mm aluminum or Non-corrosive, water resistant or better. Frame of the VMS is Matte black & Powder coated.		
Ø Operating Temperature		
· Operating Temperature of LED Display is -20° C ~ 60° C		
· Storage Temperature of LED Display is -40° C ~ 60° C		
Ø Others		
· LED Display Communication: Ethernet, Wifi, GSM.		
· Nominal Work Life of LED Display is 50000 Hours		
Ø Picture Display		
· System's Picture Display is At least 300mm as per IRC /EN 12966 standards		
· Full Matrix of LED Display and It is capable of displaying real time message generated by CCCC.		
· System has special frontal design to avoid reflection and UV resistant		
· Beam Width of LED Display is B6 as per IRC/EN12966 standards.		
· System's Standard- viewing angle both horizontal and vertical is 160 / 160 degree		
· System's Viewing Distance is Suitable for readability from 150 Mtrs. or more at the character size of 240mm, from moving vehicles		
Ø Alarms		
· System's Refresh Frequency should not be less 90 Hz. No visible flicker to naked eye.		
· System's Communication (connectivity) is Wired & GPRS based wireless technology with 3G upgradable to 4G capability.		
· Display's Ambient Operating Temperature is capable of working in ambient temperature range of T1 (- 15oC to +60oC.)		
· System is capable to protect against Pollution/dust/water		
Ø Power		
· 230V AC (more than 90% power factor) or DC as per equipment requirement.		
· Protection for overvoltage/ fluctuation/drop of the nominal voltage (50%) incorporated.		
· power supply is with PFC, thus screen's actual power consumption is less and heat less, which are good for long-time usage;		

· The enclosure shall contain at least two 15 Amp VAC (industrial grade) outlet socket for maintenance purpose.		
Ø Luminance Control & auto Diming		
· It automatically provides different luminance levels but shall also be controllable from ICCC using software.		
· System has Auto dimming capability to adjust to ambient light level (sensor base		
· System has Photoelectric sensor shall be positioned at the sign front and sign rear to measure ambient light.		
· It is Capable of being continually exposed to direct sunlight without impairment of performance.		
· Messages are readable even in broad daylight without any shade & displayed image shall not appear to flicker to the normal human eye (>5500 cd/m2).		
Ø Self-Test		
· All periodic self-test results are relayed to the CCCC in real time to update the status of the VMS		
Ø Mounting, Installation and finishes		
· Mounting structure: Use minimum 6 Mtrs. High Cylindrical GI Pole (Class B) or suitable structure with 5.5 mtr. Minimum vertical clearance under the VMS sign from the Road surface.		
· The mounting is capable of withstanding road side vibrations at site of installation.		
· It is provided with suitable walkway for maintenance access.		
· The side interior and rear of enclosures are provided in maintenance free natural aluminium finish. All enclosure are flat and wipe clean.		
· Rugged locking mechanism is provided for the onsite enclosures and cabinets		
· For Structural safety, we provide structural safety certificate from qualified structural engineers approved/ certified by Govt. Agency.		
· Wind Load: WL9 as per EN12966 to withstand high wind speeds and its own load.		
Ø Local Storage in VMS		
· Embedded VMS controller is be capable to store at-least 100 messages and symbols/pictograms to allow display to run in isolated mode on a predefined structures/timings, in case of connectivity failure.		
· The MTBF of DDS shall not be less than 100,000 hours.		
Ø Functional Requirements:		
· Central Control Software allows controlling multiple VMAS from one console.		
· System is Capable of programming to display all types of Message having alphanumeric character in English and Hindi and combination of text with pictograms signs. The system has feature to manage video / still content for VMAS display.		
· The system has capability to divide VMAS screen into multi parts to display diverse form of information like video, text, still images, advertisements, weather info, city info etc.		
· It is Capable of controlling and displaying multiple font types with flexible size and picture sizes suitable as per the size of the VMAS.		
· It is Capable of controlling brightness & contrast through software.		
· It is Capable to continuously monitor the operation of the Variable Message sign board, implemented control commands and communicate information to the Traffic Monitoring Centre via communication network		
· Real time log facility – log file documenting the actual sequence of display to be available at central control system.		

· Multilevel event log with time & date stamp.		
· Access to system only after the authentication and acceptance of authentication based on hardware dongle with its log.		
· Report generation facility for individual/group/all VMASs 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.		
· Configurable scheduler on date/day of week basis for transmitting pre-programmed message to any VMAS unit.		
· Various users can access the system using single sign on and shall be role based. Different roles which could be defined (to be finalized at the stage of SRS) could be Administrator, Supervisor, Officer, Operator, etc.		
· Apart from role based access, the system shall also be able to define access based on location.		
· Rights to different modules / Sub-Modules / Functionalities shall be role based and proper log report should be maintained by the system for such access		
· Components of the architecture must provide redundancy and ensure that there are no single points of failure in the key project components. To take care of remote failure, the systems need to be configured to mask and recover with minimum outage.		
· The architecture must adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft, natural disasters etc. provisions for security of field equipment as well as protection of the software system from hackers and other threats shall be a part of the proposed system. Using Firewalls and Intrusion detection systems such attacks and theft shall be controlled and well supported (and implemented) with the security policy. The virus and worm's attacks shall be well defended with Gateway level Anti-virus system, along with workstation level Antivirus mechanism. There shall also be an endeavour to make use of the SSL/VPN technologies to have secured communication between Applications and its end users. Furthermore, all the system logs shall be properly stored & archived for future analysis and forensics whenever desired.		
· Ease of configuration, ongoing health monitoring, and failure detection are vital to the goals of scalability, availability, and security and must be able to match the growth of the environment.		
· System use open standards and protocols to the extent possible		
· System has Facility to export reports to excel and PDF formats.		
Ø Remote Monitoring		
· All VMAS are connected/configured to Traffic Monitoring system for remote monitoring through network for two-way communication between VMAS and control Room to check system failure, power failure & link breakage.		
· Remote Diagnostics to allow identifying reason of failure up to the level of failed individual LED.		
· The system is capable to display warnings, traffic advice, route guidance and emergency messages to motorists from the ICCC in real time.		
· The system is also be capable to display warnings, traffic advice, route guidance and emergency messages to motorist by using local PC/Laptops. The system shall display graphical representation of the lanes with directional arrows and colour such as green, yellow, red for depicting density of traffic		
· The VMAS can display text and graphic messages using Light Emitting Diode (LED) arrays		
· The System is able to display failure status of any LED at ICCC.		
· The System supports Display characters in true type fonts and adjustable based on the Operating system requirement.		

· The ICCC workstation can communicate with the VMAS controller through the network. It shall send out command data to the variable message sign controller and to confirm normal operation of the signboard. In return, the ICCC workstation shall receive status data from the VMAS controller.		
· VMAS controllers continuously monitor the operation of the VMAS via the provided communication network.		
· Operating status of the variable message sign shall be checked periodically from the ICCC.		
· It is capable of setting an individual VMAS or group of VMAS'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.		
· It is capable of being programmed to display an individual message to a VMAS or a group of VMAS's at a pre-set date and time.		
· A sequence of a minimum of 10 messages/pictures/ pre-decided sign or group of signs shall be possible to assign for individual VMAS or group of VMAS's.		

5.7 Environmental Monitoring Sensors

Functional Requirement				
Sl. No.	**Parameter**	**Description**	**Technical Compliance (Yes/ No)**	**Remark**
1		The environmental sensors housed in the Sensor station shall monitor following parameters and include the following integrated sensors inside one station a. Carbon Monoxide (CO) sensor b. Ozone (O3) sensor c. Nitrogen Dioxide (NO2) sensor d. Sulphur Dioxide (SO2) sensor e. Carbon Dioxide (CO2) sensor f. Particulate/SPM Profile (PM10 and PM2.5) sensor g. Temperature sensor h. Relative Humidity sensor i. Wind Speed sensor and direction sensor j. Rainfall sensor k. Barometric Pressure sensor l. Noise sensor All Air Sensors should be as per the Air Act and any modifications to it.		
2		The sensors shall be able to communicate its data using both wired and wireless technology.		
3		Apart from information provision, the sensors must ensure data is transmitted securely and have security measures from sensors to the software platform		
4		The environmental sensors location shall be visible as a layer in GIS Maps as dashboard		

5		Environmental Sensor station shall be housed in a compact environmentally rated outdoor enclosure. It shall be an integrated module which shall monitor overall ambient air and noise quality among other parameters as detailed above		
6		Environmental sensor station shall be ruggedized enough to be deployed in open air areas such as streets and parks		
7		Software shall display real time and historical data in chart and table views for dashboard view of the Client		
8		Software shall display trends of environmental parameters based on user specific time periods.		
9		It shall be possible to configure and calibrate the sensors through the software from a remote location		
10		Alarms shall be generated for events where the environmental parameters breach the safe or normal levels.		
11		Data of all the environmental sensor shall be available on the same software interface		
12		It shall be integrated at the ICCC for the purposes of monitoring, display of information and control of the system		
13		Ensure compliance of published Environmental standards/benchmarks and parameters set by: a. National Air Quality Index (NAQI) b. Central Pollution Control Board(CPCB) or State pollution control board(SPCB) c. Meteorological department. d. Health department /Public health		
14		The environmental monitoring system should be capable of integration from the ICCC in real time.		
15		The environmental systems should have a functionality to display units levels in real time sensors.		
16		The System should be able to display failure status of any sensors at ICCC.		
17		Environmental application in ICCC should continuously monitor the pollution levels and AQI index operation of the Sensors locations via the provided communication network.		
18		Operating status of the environmental sensors levels should be checked periodically from the ICCC.		
19		MSI shall also ensure store Environment related Data & information in real time status of all the monitoring of Environmental sensors displayed/installed in the smart city locations .		
20		The AQI index and pollutant Levels/benchmarking shall be viewable and readable from a distance upto 150 meter. And various angles on the junctions installed or road as decided by the Authority		
21		MSI shall ensure the Environment monitoring systems devices/sensors shall be connected/configured to ICCC platform/dashboard for remote monitoring by establishing a communication network between Environmental sensors and Environmental monitoring platform at ICCC to check system failure, power failure & link breakage.		
22		Remote Diagnostics on real time basis of Environmental sensors and devices should allow identifying failure up to the level of failed individual display segment.		

2.14 Technical Requirement: Environmental Sensors				
Sl. No.	**Parameter**	**Description**	**Compliance**	
1	Carbon Monoxide (CO) Sensor	Range of CO sensor shall be between 0 to 1000 PPM		
2		Resolution of CO sensor shall be 0.01 PPM or better.		
3		Lower detectable limit of CO sensor shall be 0.040 PPM or better		
4		Precision of CO sensor shall be less than 3% of reading or better		
5		Linearity of CO sensor shall be less than 1% of full scale or better		
6		Response time of CO sensor shall be less than 60 seconds.		
7		Operating temperature of CO sensor shall be as per City requirement		
8	Ozone (O3) Sensor	O3 Sensor shall have a range of at least 0-1000 PPB.		
9		Resolution of O3 sensor shall be 10 PPB or better.		
10		Lower detectable limit of O3 sensor shall be 10 PPB or better		
11		Precision of O3 sensor shall be less than 3% of reading or better		
12		Linearity of O3 sensor shall be less than 1% of full scale.		
13		Response time of O3 sensor shall be less than 60 seconds		
14		Operating temperature of O3 sensor shall be as per City requirement		
15	Nitrogen Dioxide (NO2) Sensor	NO2 Sensor shall have a range of at least 0-10 PPM.		
16		Resolution of NO2 sensor shall be 0.001 PPM or better.		
17		Lower detectable limit of NO2 sensor shall be 0.001 PPM or better.		
18		Precision of NO2 sensor shall be less than 3% of reading or better.		
19		Linearity of NO2 sensor shall be less than 1% of full scale		
20		Response time of NO2 sensor shall be less than 60 seconds.		
21		Operating temperature of NO2 sensor shall be as per City requirement		
22	Sulphur Dioxide (SO2) Sensor	SO2 Sensor shall have a range of at least 0-20 PPM.		
23		Resolution of SO2 sensor shall be 0.001 PPM or better.		
24		Lower detectable limit of SO2 sensor shall be 0.009 PPM or better.		
25		Precision of SO2 sensor shall be less than 3% of reading or better.		
26		Linearity of SO2 sensor shall be less than 1% of full scale.		
27		Response time of SO2 sensor shall be less than 60 seconds		
28		Operating temperature of SO2 sensor shall be as per City requirement		
29	Carbon Dioxide (CO2) Sensor	CO2 Sensor shall have a range of at least 0-5000 PPM		
30		Resolution of CO2 sensor shall be 1 PPM or better		
31		Lower detectable limit of CO2 sensor shall be 10 PPM or better		
32		Precision of CO2 sensor shall be less than 3% of reading or better.		
33		Linearity of CO2 sensor shall be less than 2% of full scale.		
34		Response time of CO2 sensor shall be less than 60 seconds		
35		Operating temperature of CO2sensor shall be as per City requirement		
36	Particulate/SPM Profile (PM10 and PM2.5) sensor	Particulate profile sensor shall provide simultaneous and continuous measurement of PM10, PM2.5, SPM and TSP (measurement of nuisance dust) in ambient air.		
37		Range of PM2.5 shall be 0 to 230 micro gms / cu.m or better.		
38		Range of PM10 shall be 0 to 450 micro gms / cu.m or better		
39		Lower detectable limit of particulate profile sensor shall be less than 1 µg/m3.		

40		Accuracy of particulate profile sensor shall be <± (5 µg/m3 + 15% of reading)		
41		Flow rate shall be 1.0 LPM or better.		
42		Operating temperature of the sensor shall be as per City requirement		
43	Temperature Sensor	Temperature sensor shall have the capability to display temperature in °Celsius.		
44		Temperature range shall be -10° to +100°C.		
45		Sensor accuracy shall be ±0.3°C (±0.5°F) or better.		
46		Update interval shall be 10 to 12 seconds		
47	Relative Humidity sensor	Range of relative humidity sensor shall be 1 to 100% RH.		
48		Resolution and units of relative humidity sensor shall be 1% or better.		
49		Accuracy of the sensor shall be ±2% or better.		
50		Update interval shall be less than 60 seconds		
51		Drift shall be less than 0.25% per year.		
52	Wind Speed Sensor and direction sensor	Wind speed sensor shall display wind speed in km/h		
53		Range of sensor shall be 0-60 m/s.		
54		Accuracy of wind speed sensor shall be ±5% or better.		
55		Update interval shall be less than 60 seconds		
56		Range of the wind direction sensor shall be 0° to 360°.		
57		Display resolution shall be 16 points (22.5°) on compass rose, 1° in numeric display		
58		Accuracy shall be ±3% or better.		
59		Update interval shall be 10 seconds		
60	Rainfall Sensor	Rainfall sensor shall the capability of displaying level of rainfall in inches and millimetre		
61		Daily Rainfall range shall be 0 to 99.99” (0 to 999.8 mm).		
62		Accuracy for rain rates shall be up to 4”/hr (100 mm/hr) or ±4% of total		
63		Update interval shall be less than 60 seconds.		
64	Barometric Pressure Sensor	Barometric pressure sensor shall have the capability of displaying barometric pressure in Hg, mm Hg and hPa/mb.		
65		Range of barometric pressure sensor shall be 540 hPa/mb to 1100 hPa/mb		
66		Uncorrected reading accuracy shall be ±1.0 hPa/mb at room temperature or better		
67		Elevation range of the barometric pressure sensor shall be - 600 m to 4570 m.		
68		Elevation accuracy shall be ±10’ (3m) to meet equation accuracy specification or better		
69		Overall accuracy shall be ±0.03" Hg (±0.8 mm Hg, ±1.0 hPa/mb) or better		
70		Update interval shall be less than 60 seconds		
71	Noise Sensor	Noise Sensors shall be installed for the outdoor applications.		
72		Noise sensor shall detect the intensity of the ambient sound in a particular area.		
73		Noise sensor shall be able to identify the areas of high sound intensity ranging from 30 dBA to 120 dBA.		
74		Noise sensor shall have resolution of 0.1 dBA.		

5.8 UNITERRUPTED POWER SUPLY (UPS)

1 KVA TRUE ONLINE UPS WITH 60 MINUTES BACK-UP- will be used for all location except ICCC and VC's.
1 KVA TRUE ONLINE UPS WITH 30 MINUTES BACK-UP- will be used for VC's
100 KVA MODULAR ONLINE UPS WITH 60 MINUTES BACK-UP- will be used for ICCC and On-premise DC

5.8.1 1 KVA TRUE ONLINE UPS WITH 60 MINUTES BACK-UP

Warranty period should be Go-live+ 5 year, Power factor, Efficiency, Transfer time (should be 4 to 8 ms for online to battery /battery to online mode) need to share.

Since there may be unseen situations when the power outage in some locations is more than 60 minutes, it should be ensured that all data from various equipment like camera, sensors, etc. are backed up to avoid loss of data and Its SI responsibility to maintain it. Proper civil infrastructure for housing the UPS must be ensured at each location during design and detail engineering phase.

Minimum Technical Specification

Sl. No.	Parameter	Description	Technical Compliance (Yes/ No)	Remark
1	**Configuration**	**1 KVA** IGBT based On-Line UPS with inbuilt Isolation Transformer for Galvanic Isolation.		
2	**Capacity**	**1 KVA / 900 Watts**		
3	**AC Input Voltage Range**	160-280 V AC, 1 Phase @100% load		
4	**Input Frequency**	50Hz ± 10% (Suitable for Generators)		
5	**AC Output Voltage**	230 V AC, 1-phase ± 1% (Sine Wave Output)		
6	**Output Frequency**	50 Hz ± 0.5 Hz		
7	**Overload Capacity**	Overload – 110%: UPS shuts down after 05 minutes or transfers to AC supply when it is normal. Overload – 125%: UPS shuts down after 1 minutes or transfers to AC supply when it is normal.		
8	**Harmonic Distortion**	<2% for Linear Loads and <5% for non-linear loads		
9	**Isolation Transformer**	UPS output should be fully isolated by double conversion and inbuilt isolation transformer within the UPS cabinet itself. External transformer shall not be considered.		
10	**Indications & Audible Alarms**	Mains On, Inverter On, Overload, Battery Low		
11	**Digital Metering**	LCD display for measurement of AC Voltage, Battery voltage, Battery Current, Load Current, Output frequency.		
12	**Battery Charger**	Offered UPS must have inbuilt 10 Amps Charging Current for proper charging of Battery Bank.		
13	**UPS Remote Monitoring through Mobile App**	UPS should have Cloud based Monitoring & Management platform with necessary hardware and below features: ● UPS monitoring system should be plug and play easy installation that allows the user to manage and monitor the UPS status remotely via an ANDROID and iOS mobile phone application in addition to browser based platform		

		• SNMP having both Wi-Fi antenna and RJ45 port with QR Code ID • Clear interface to view instant status • Real Time alert and notification • Logs for troubleshooting • Secure Web and APP portal to access and monitor UPS from any connected device • Shutdown remote server without any software installation Datasheet to be provided for the above		
14	**Battery Back-up & Other Details**	The system must be capable of providing requisite battery back-up time of **60 Minutes** using 12V, VRLA Sealed Maintenance Free Batteries with each UPS. Required VAH: **1500 VAH for 60 minutes with required battery bank.** Offered VRLA SMF batteries should comply with below: • Long Design Float life of at least 10 years • Made of Lead-Calcium-Tin alloy composition for long float service life • Manufactured in India (class 1 MII Product) • Made of UL94 V0 class fire retardant container and cover • Operating Temperature Range of 0°C - 45°C • ISO 9001, ISO 14001 for manufacturing plant in India • Brochure of Battery indicating above specifications with Make & Model to be specified		
15	**Certification**	• ISO 9001, ISO 14001, ISO 45001, ISO 50001 certified. • E-Waste (EPR authorization from CPCB, Govt. of India) • BIS/CE Certificate		
16	**Installation & Commissioning**	Bidder/OEM should install, commission and maintain the UPS system as per Govt Electrical standard practices. Bidder/OEM's Valid Govt electrical license to be enclosed with Bid		
17	**After Sales Support & Manufacturer's Credibility**	• UPS OEM should have its registered office in Assam for ≥10 years and company owned 8~10 service centres across Assam with adequate technical manpower and spares for ensuring 24 x 7 x 365 support as per contract SLA. Contact numbers and addresses to be provided for support centers • UPS OEM should have ongoing service & maintenance contracts for ≥1000 nos. On-Line UPS Systems to Govt./PSU organizations in Assam & NE as proof of having 24 x 7 x 365 service support capabilities and competency along with their Client references. • UPS OEM should not have past history of blacklisting or breach of contract from any government/PSU organization. • UPS OEM should have past experience for deploying minimum 2000 nos. of ≥1 KVA UPS Systems in any Govt/PSU project in Assam & NE in a single order		

5.8.2 1 KVA TRUE ONLINE UPS WITH 30 MINUTES BACK-UP

Warranty period should be Go-live+ 5 year, Power factor, Efficiency, Transfer time (should be 4 to 8 ms for online to battery /battery to online mode) need to share.

Proper civil infrastructure for housing the UPS must be ensured at each location during design and detail engineering phase..

Minimum Technical Specification

Sl. No.	Parameter	Description	Technical Compliance (Yes/ No)	Remark
1	**Configuration**	**1 KVA** IGBT based On-Line UPS with inbuilt Isolation Transformer for Galvanic Isolation.		
2	**Capacity**	**1 KVA / 900 Watts**		
3	**AC Input Voltage Range**	160-280 V AC, 1 Phase @100% load		
4	**Input Frequency**	50Hz ± 10% (Suitable for Generators)		
5	**AC Output Voltage**	230 V AC, 1-phase ± 1% (Sine Wave Output)		
6	**Output Frequency**	50 Hz ± 0.5 Hz		
7	**Overload Capacity**	Overload – 110%: UPS shuts down after 05 minutes or transfers to AC supply when it is normal. Overload – 125%: UPS shuts down after 1 minutes or transfers to AC supply when it is normal.		
8	**Harmonic Distortion**	<2% for Linear Loads and <5% for non-linear loads		
9	**Isolation Transformer**	UPS output should be fully isolated by double conversion and inbuilt isolation transformer within the UPS cabinet itself. External transformer shall not be considered.		
10	**Indications & Audible Alarms**	Mains On, Inverter On, Overload, Battery Low		
11	**Digital Metering**	LCD display for measurement of AC Voltage, Battery voltage, Battery Current, Load Current, Output frequency.		
12	**Battery Charger**	Offered UPS must have inbuilt 10 Amps Charging Current for proper charging of Battery Bank.		
13	**UPS Remote Monitoring through Mobile App**	UPS should have Cloud based Monitoring & Management platform with necessary hardware and below features: • UPS monitoring system should be plug and play easy installation that allows the user to manage and monitor the UPS status remotely via an ANDROID and iOS mobile phone application in addition to browser based platform • SNMP having both Wi-Fi antenna and RJ45 port with QR Code ID • Clear interface to view instant status • Real Time alert and notification • Logs for troubleshooting • Secure Web and APP portal to access and monitor UPS from any connected device • Shutdown remote server without any software installation Datasheet to be provided for the above		
14	**Battery Back-up & Other Details**	The system must be capable of providing requisite battery back-up time of **30 Minutes** using 12V, VRLA Sealed Maintenance Free Batteries with each UPS. Required VAH: **900 VAH for 30 minutes with required battery bank.**		

		Offered VRLA SMF batteries should comply with below: • Long Design Float life of at least 10 years • Made of Lead-Calcium-Tin alloy composition for long float service life • Manufactured in India (class 1 MII Product) • Made of UL94 V0 class fire retardant container and cover • Operating Temperature Range of 0°C - 45°C • ISO 9001, ISO 14001 for manufacturing plant in India • Brochure of Battery indicating above specifications with Make & Model to be specified		
15	**Certification**	• ISO 9001, ISO 14001, ISO 45001, ISO 50001 certified. • E-Waste (EPR authorization from CPCB, Govt. of India) • BIS/CE Certificate		
16	**Installation & Commissioning**	Bidder/OEM should install, commission and maintain the UPS system as per Govt Electrical standard practices. Bidder/OEM's Valid Govt electrical license to be enclosed with Bid		
17	**After Sales Support & Manufacturer's Credibility**	• UPS OEM should have its registered office in Assam for ≥10 years and company owned 8~10 service centres across Assam with adequate technical manpower and spares for ensuring 24 x 7 x 365 support as per contract SLA. Contact numbers and addresses to be provided for support centers • UPS OEM should have ongoing service & maintenance contracts for ≥1000 nos. On-Line UPS Systems to Govt./PSU organizations in Assam & NE as proof of having 24 x 7 x 365 service support capabilities and competency along with their Client references. • UPS OEM should not have past history of blacklisting or breach of contract from any government/PSU organization. • UPS OEM should have past experience for deploying minimum 2000 nos. of ≥1 KVA UPS Systems in any Govt/PSU project in Assam & NE in a single order		

5.8.3 100 KVA MODULAR ONLINE UPS WITH 60 MINUTES BACK-UP

Warranty period should be Go-live+ 5 year, Power factor, Efficiency, Transfer time (should be 4 to 8 ms for online to battery /battery to online mode) need to share.

Since there may be unseen situations when the power outage in some locations is more than 60 minutes, it should be ensured that all data from various equipment like camera, sensors, etc. are backed up to avoid loss of data and Its SI responsibility to maintain it.

Proper civil infrastructure for housing the UPS must be ensured at each location during design and detail engineering phase.

S. No.	TECHNICAL SPECIFICATIONS FOR 100 KW N+1 MODULAR ON-LINE UPS	Technical Compliance (Yes/No)	Remark
	GENERAL FEATURES:		
1	Supply, installation and commissioning of 100 KW N+1 True On-Line Double Conversion, modular type UPS. The UPS shall be DSP controlled with front end IGBT rectifier. Inverter shall be 3 Level IGBT based for highest efficiency. The 100 KW N+1 KW UPS system should have provision to operate in parallel redundant		

	mode, with similar UPS to provide redundancy in future (at least 3 nos. UPS frames/cabinets in parallel).		
2	Each 100 KW N+1 KW UPS shall be with modular architecture with suitable nos of 25KW~50KW Hot Swappable Power Modules of double conversion configuration, especially designed for mission critical applications, i.e. 5 nos x 25 KW or 4 nos x 40KW or 3 nos x 50KW Modules, such that 01 module shall be redundant. Individual Module size >50 KW and <25 KW shall not be accepted. There shall be provision to scale up the UPS to minimum 200 KW through vertical expansion simply by inserting additional 25KW/50KW hot swappable power modules as and when necessary. Further, UPS should also be scalable upto 600 KW through horizontal expansion		
3	The frame for Each 100 KW N+1 UPS shall be in a space saving design, with standard IT 42U frame		
4	Each hot swappable UPM power module shall include a rectifier, battery converter, inverter and independent logic circuitry. There should be no common controller (either single or redundant) outside the modules		
5	Each hot-swappable power module should have isolated air flow design, such that the PCB boards and heat-sinks are in two completely different sections, which should allow the UPS to run in dusty environments, significantly improving its stability and environmental adaptability.		
6	Each UPS frame shall also have an STS Module comprising of a fully rated, continuous duty static bypass switch for high-speed transfers along with RS232 port, USB port, SNMP Slot, Dry contact ports.		
7	The control panel comprising of a Colour graphical LCD DISPLAY, touch screen based, with LED status indicators for monitoring of all measured parameters, UPS and battery status and alarms along with facility for displaying the waveform of the output voltage and current, and the bypass voltage. There shall be provision for Recording/Storing of waveforms of critical elements during fault conditions for rapid maintenance service diagnosis.		
8	UPS should have inbuilt facility for Life cycle monitoring of critical components like fan, capacitors, battery which helps the UPS to predict the life of these components.		
9	The UPS shall have inbuilt 35 Amperes Charging Current to adequately charge the battery bank. The vendor has to supply the necessary battery rack and interconnecting cables (nyvin fire retardant type). There shall be provision for adding extra rack mounted charger module (3U) of 30 Amperes in order to allow proper charging of batteries in case extended autonomies are required. Technical Datasheet verifying this feature should be provided.		
10	**BATTERIES:** Each 100 KW N+1 KW UPS shall have battery bank comprising of 158,000 VAH using 12V, VRLA Sealed Maintenance Free Batteries for 60 minutes backup time. Offered VRLA SMF batteries should comply with below: Long Design Float life of at least 10 years Made of Lead-Calcium-Tin alloy composition for long float service life Battery should be Manufactured in India (class 1 MII Product with >50% local content) Made of UL94 V0 class fire retardant container and cover Operating Temperature Range of 0°C - 45°C Self-discharge per month <3% of rated capacity at 25°C ISO 9001, ISO 14001 for manufacturing plant in India Brochure of Battery indicating above specifications with Make & Model to be		

	specified			
11	**Energy Saver Smart sleep function:** System should have capability to intelligently shutdown inactive power modules to increase energy savings and achieve higher efficiency			
12	**Self-Test mode:** System can perform a full load test without the connection of a load bank, processing power in a re-circulating fashion, using its own rectifiers and inverters as an internal load bank, generating significant savings in cost, time, coordination and power.			
13	**Isolation Transformer** of 200 KVA should be provided with each UPS for providing galvanic isolation between input & output. Isolation Transformer should be external to the UPS and placed inside a suitable enclosure with powder coated paint and provided with cast iron wheels at bottom and hooks for lifting the unit.			
14	**DETAILED SPECIFICATION SHEET**			
	MODEL RATING (1.0 p.f.)	100 KW N+1 KVA/KW Modular On-Line UPS		
	Make & Model	To be Specified		
	ELECTRICAL CHARACTERISTICS INPUT			
	Rated input voltage	380 V; 400 V; 415 V, 3 Phase		
	Voltage tolerance	310~475 VAC @100% load 220~475 VAC @50% load		
	Rated input frequency Frequency tolerance	50 or 60 Hz, user configurable 40 to 70 Hz		
	Input power factor, double conversion @100% load	> 0.99		
	Input current distortion at rated input current	< 3%, 100% load		
	ELECTRICAL CHARACTERISTICS OUTPUT			
	Crest factor	3:1		
	Rated output voltage	380 V; 400 V; 415 V, 3 Phase		
	Output voltage variation, steady state	± 1% (balanced load); ± 2% (unbalanced load)		
	Total voltage harmonic distortion 100% linear load 100% non-linear load	 < 1% < 5%		
	Rated output frequency Output frequency variation	50 or 60 Hz, configurable ± 0.1 Hz		
	Overload capability	1 hour: 110%, 10 mins: 125%, 1 min:150%		
	Efficiency in double-conversion, rated linear load	≥95%		
	BYPASS			
	Type of bypass	Static		
	Bypass rating	200 KW		
	Bypass voltage range	380 V; 400 V; 415 V		
	BATTERY CHARACTERISTICS			
	Battery technology	12V, VRLA SMF Batteries		
	Nominal VAH capacity	158000 VAH for 60 minutes Back-up		
	Battery start option	Yes		
	COMMUNICATION CIRCUITS			
	Standard connectivity ports	USB/RS-232, BMS/SNMP card		

	System Display	Touch based graphical LCD display		
	UPS Remote Monitoring through Mobile App	UPS should have Cloud based Monitoring & Management platform with necessary hardware and below features: • UPS monitoring system should be plug and play easy installation that allows the user to manage and monitor the UPS status remotely via an ANDROID and iOS mobile phone application in addition to browser based platform • SNMP having both Wi-Fi antenna and RJ45 port with QR Code ID • Clear interface to view instant status • Real Time alert and notification • Logs for troubleshooting • Secure Web and APP portal to access and monitor UPS from any connected device • Shutdown remote server without any software installation Datasheet to be provided for the above		
	ENVIRONMENTAL			
	Acoustic noise at 1 m, in 25 °C ambient temperature	< 65 dBA		
	Ambient service temperature range	0°C to + 40°C without output power derating		
	COMPLIANCE WITH STANDARDS			
	Quality	ISO 9001, ISO 14001, ISO 45001, ISO 50001		
	Safety	IEC 62040-1		
	EMC	IEC 62040-2		
	E-Waste	EPR authorisation from CPCB, Govt of India		
15	**Installation & Commissioning**	Bidder should install, commission and maintain the UPS system as per Govt Electrical standard practices. Bidder’s Valid Govt electrical license to be enclosed with Bid		
16	**After Sales Support & Manufacturer’s Credibility**	• UPS OEM should have its registered office in Assam for ≥10 years and company owned 8~10		

		service centres across Assam with adequate technical manpower and spares for ensuring 24 x 7 x 365 support as per contract SLA. Contact numbers and addresses to be provided for support centers ● UPS OEM should have ongoing service & maintenance contracts for ≥1000 nos. On-Line UPS Systems to Govt./PSU organizations in Assam & NE as proof of having 24 x 7 x 365 service support capabilities and competency along with their Client references. ● UPS OEM should not have past history of blacklisting or breach of contract from any government/PSU organization. ● UPS OEM should have past experience for supply & installation of at least 10 units of ≥100 KW Modular UPS System in any Govt. or PSU Data Centre/Server Room/Computer Centre Site		
	The bidder should submit documentary evidence in support of 100% compliance to the tender specifications. The bidder should submit the Datasheet and user/operation manual of the UPS system offered.			

5.9 DG-180 KVA Silent DG SET WITH AMF PANEL

The sound level of the DG must be in accordance with the latest CPCB norms

Specification	**Specification Name**	**Bid Requirement (Allowed Values)**	**Technical Compliance (Yes/No)**	**Remark**
Power Generator INSTALLATION CONFIGURATIONS	Power Generator installation configurations as defined in CPWD General Specifications for Electrical works - Part VII (DG Set)	Fixed (Power Generators are permanently installed)"		
OUTPUT CAPACITY RATING / PHASE	Nominal Rated Capacity (kVA)	180		

	No of Phase	Three Phase		
ENGINE	Rated Engine Power (kWm)	100% of the required powered at STP (Standard Temperature Pressure) i.e., equal to (Nominal Rated Capacity (KVA) of power generator + Any Auxiliary power Consumption by the Power generator) x Power factor (0.8) / Alternator efficiency, 110 % of the required powered at STP (Standard Temperature Pressure) Le equal to (Nominal Rated Capacity (KVA) of power generator Any Auxiliary power Consumption by the Power generator) x Power factor (0.8) /Alternator efficiency OR higher		
	Type of Engine cool i n g	Liquid Cooled		
	Type of governor	Electronic Or higher (G2 or G3)		
	Number of cylinders (nos)	Greater than or equal to 4		
	Rated RPM of Engine [RPM)	1500		
	Fuel	High Speed Diesel (HSD)		
	Starting voltage (volt)	12 / 24		
	Salient Features of Engine	Turbo Charged Engine, Direct injection Fuel System		
ALTERNATOR	Alternator Voltage Rating	415.0		
	Conformity to Indian Standard (for Alternator)	Generally conforming to IS:13364 (Part-2) latest (Above 20 KVA)		
	Voltage Regulation Grade	VG 3 Or higher		
CONTROL PANEL	Control Panel	AMF Control Panel		
	Control Panel Location	Inside the canopy		
	Display meters in the control panel (with appropriate rating and accuracy class) - inclusive in the scope of supply	Multifunctional Digital display meter (displaying Voltage, Current, Frequency, Power Factor)		
	Other devices in the control panel (with appropriate rating) - inclusive in the scope of supply	Required switches and cut-out, MCB, MCCB, Contactor, Circuit breaker, Battery charger		
	Displayed parameters / Features	Engine Speed, Lube oil pressure, Coolant/cylinder head Temperature, Engine running hours, Engine battery voltage, Engine Running status, Generator Voltage (Ph-Ph), Generator Voltage (Ph -N), Generator Current (R, Y, B), Generator apparent Power (kVA), Generator active Power (kW), Power factor, Frequency, Fuel level, Event log, Control supply Voltage		
	Indicators	Low Lube oil pressure, High water / coolant / cylinder head temperature, Low fuel		

		level, Over speed		
	Audio Alarm	Low Lube oil pressure, High water / coolant / cylinder head temperature, Low fuel level, Over speed		
BATTERY	Battery Type & Specification	Low Maintenance free to IS: 14257 for high cranking performance"		
	No of batteries	½		
SALIENT FEATURES	Salient Features of Power Generator	Glass window on Acoustic Enclosure in front of the Control Panel, Emergency Stop outside the Acoustic Enclosure		
SCOPE OF INSTALLATION	Installation	with installation - inclusive in the scope of supply any anything extra if required		
WARRANTY /SERVICE	Warranty on Complete power generator/DG Set	5 years support after successful commissioning. Bidder should quote for 02 years comprehensive warranty (including cost of all spares and consumable for routine preventive and corrective maintenance) followed by CAMC (including all spares and consumables for routine preventive and corrective maintenance) for 03 years, i.e., 3rd, 4th and 5th year after 02 years warranty period. **GSCL will not pay any additional cost for maintenance or repairs during breakdown, during these 05 years, except cost of fuel. This shall be subject to force majeure conditions.**		
MAINTENANCE SERVICES	Number of preventive maintenance visits offered in an year during warranty period (Supply of all consumable and spares is the seller's responsibility)	No of Visits shall be as per DG OEM standard policy. Declaration of the OEM is required from the bidder during submission of bid.		
	While providing preventive and corrective Maintenance Services within the warranty and CAMC period, the bidder will not be allowed to charge anything for consumables and spares (except fuel). All packaging, forwarding freight and Service charges shall be under bidder’s scope	Declaration of the bidder is required from the bidder during submission of bid		
TEST REPORT /DOCU MENT	Agree to provide all relevant documents Test Report / supporting document / Reports etc to the buyer	Declaration of the bidder is required from the bidder during submission of bid (ARAI certificate/Alternator test Certificate/AMF panel test certificate with drawing)		

	at the time of bidding or on demand			
Remote Access	Mandatory	The bidder should provide remote access provision to the Gen Set operational investigation.		
Breakdown Call	Should be attended within 24-48 hours	Declaration of the bidder is required from the bidder during submission of bid		

Scope of installation for Diesel Generating Set when offered by the vendor - inclusive in the scope of supply

S. No.	Technical Specification	Technical Compliance (Yes/No)	Remark
1	Installation of Power Generator when offered by the vendor is inclusive in the scope of supply and shall be done by the seller. The installation work of Power Generator and its constituent parts shall be generally conforming to CPWD General Specification for Electrical Works, Part - VII - latest.		
2	Foundation shall be constructed by the Selected bidder. Foundation shall be of PCC type with the ratio of 4:2: 1. The length and breadth of the foundation shall be 300 mm more from the respective length and breadth of the Power Generator. The height of the foundation shall be 400 mm, i.e., 200 mm below and 200 mm above the ground level. All the materials / labour required for foundation work shall be supplied by the selected bidder.		
3	Supply, laying and termination of exhaust Pipe Line, interconnecting power and control cable, changeover switch etc. shall be done by the seller. The cable supplied shall be ISI marked heavy duty PVC insulated, armoured cable, with PVC outer Sheath of Type ST- 2 (FR Grade, Category Cl), with aluminium conductor having insulation of PVC compound type -C, suitable for rated voltage up to and including 1100 volts and conforming to IS: 1554 (Part-1) latest. For 3-Phase Power Generators, 3.5 core or higher core (150 sq mm) cables shall be used. Total length of the cable supplied by the seller may be within 70 meters for each Power Generator with AMF control panel. (4 turns)		
4	Construction of suitable earthing station and necessary connections shall be done by the Selected bidder. All the materials / labour required for construction of earthing station shall be supplied by the Selected bidder. The total number of earthing pits/stations shall be 4, i.e., 2 for neutral and 2 for body-earthing. Neutral earthing shall be done with copper Plate and Body earthing shall be done with G.I. plate / Copper. The consignee should choose installation site in such a way that the earthing stations can be made within 10 metres of the Power Generator. Earthing station shall be typically constructed as per prevalent standard practices and shall be generally conforming to CPWD General specification for Electrical Works, Part - VII & Part - I - latest.		

5.10 Integrated Command and Control Centre(ICCC)

S.no	Description	Compliance (Yes / No)	Remarks
1	The Smart City Software Suite should serve as a foundation for building the technology base of the smart city and should harness advances in digital technologies in IoT, Big Data, BI, AI, Mobile and GIS. The Software Suite should cover a Digital platform to integrate the various urban systems and Pre -integrated Application software covering Integrated Command and Control Center, Mobile workforce Management, It should also act as a central system through which the city administrators can monitor and operate the various city services intelligently and efficiently.		
2	The Smart City software suite should be standard Commercial-of-the-shelf (COTS) product, and should adhere to the industry standards for interoperability, data representation & exchange, aggregation, processing, and storage management. It should Aggregate, Process, Store, Analyse and Act based on the streaming data from sensor networks, data from application subsystems and provide a centralized common platform for services to be used by various applications.		
3	Proposed ICCC Platform should have been deployed in at least 5 smart cities in India / Global. Minimum 3 City implantations must be in India among the 5 implementations. All these implementations should be successfully operational for least 3 years with Integration to minimum 10 different sub systems /applications.Document Proof: OEM Shall submit P.O and Completion Certificate/ Installation Notes/UAT Certificates from MSI as documentary proof.		
4	ICCC Platform OEM should have ISO 9001:2015 & ISO 27001:2013.		
5	ICCC platform should be “make in India”		
6	The proposed Smart City Software Suite should at the minimum support the following services and capabilities.		
7	Seamlessly connect & monitor urban systems		
8	1. It should be able to connect, collect and process data from various urban systems and detect anomalies.		
9	2. It should provide an easy-to-use interface to onboard and provision sensor data and data from various applications systems		
10	Analyse data in real time and automate core processes		
11	. It should enable Intelligent automation of the workflows based on anomalies detected including actuating devices/systems and work with AI/ML system for predictive actions.		
12	2. It should enable the operator to configure various types of SOPs and automate the processes		
13	Drive in-line departments operational efficiency through AI		
14	1.It should support ready to deploy Smart Cities AI/ML applications for various domains to drive efficiency across various in-line departments.		
15	2.It should be integrated with a tool to support composing the data, building ML models and deploy them as APIs to be used by various AI/ML applications.		
16	Build 360º situational awareness for operations		

17	It should enable effective management of City Operations through a Integrated Command and Control Center Application System.		
18	Empower city workforce with insights to respond faster		
19	1. It should be integrated with Unified Workforce management Application system so that City Workforce across all departments can be integrated and equipped with Mobile App to efficiently run their day to day activities.		
20	2. It should provide complete visibility to the events and real time insight to take action faster by the workforce.		
21	Smart City Software Suite should be in compliance with the Smart City Standards of a layered architecture and should be able to integrate the various layers to provide a unified system capability. The Software Suite should at the minimum cover the following layers.		
22	IoT & AI Platform		
23	A central IoT & AI Platform for integrating the Sensor Data and Application Data from the various city-wide urban systems. It should be pre-integrated with various sub systems like – IoT, Complex Event processing. Big Data, BI and AI Advanced Data Analytics, API/ESB, BPM, GIS, Security and Logging & Monitoring. Also, it should support rich pre-integrated tools for Provisioning and Administration, Building Dashboards and Deploying and Building ML Models and deploying.		
24	The Smart City Software Suite should be integrated and support all the core applications that will enable the Digital Transformation of the city. The Applications should cover –		
25	· Integrated Command and Control Center System for City Operations		
26	· Mobile Workforce Management System for integrating the city workforce through a City Workforce App.		
27	· Business Intelligence based real time dashboards for various domains.		
28	The Smart City Software Suite should comprise of various client applications for the stakeholders to use and consume the services. Wide range of personas covering – City Authorities, City Operator and Managers, City Workforce and Managers across the various departments, Community should be able to access the system securely through Web Application, Dashboards, Portals and Mobile Apps.		
29	Smart City Platform : The functional specifications provided in the below sections are critical functionalities to be adhered by the proposed Smart City Platform.		
30	Smart City Platform should serve as a City-Wide IoT & AI Platform that can integrate data from any urban system, detect anomalies and take action in real-time so that the urban system operations can be remotely managed through a common city command and control centre.(Urban System – Municipality, Health, Education, Transport, Utility, Power/Electricity, Disaster mgmt.,Law and order, etc).		
31	It should be a system of systems platform pre-integrated with advanced digital technologies to collect, process, store and analyse the data. The system of systems approach supports the sub systems to be pre-integrated to the platform to deliver the total value of IoT and AI.		
32	The Platform should support Microservices and each of the Service components should be loosely coupled to support scale. The sub systems of Smart City Platform should be able to provide the services as listed below		

33	Data Integration: Should integrate data from sensors and external applications from the city-wide urban systems		
34	Data Processing: Should process the data in real time and create alarms based on data anomalies and geo-events		
35	Data Management & Analytics System: 1.Big Data based Storage System to store the structured, semi-structured and unstructured data		
36	2.Platform should have pre-integrated analytics engine covering BI services to build and deploy Dashboard for monitoring operational KPIs and gain insights to city civic services delivery		
37	3. Platform should also have a pre-integrated AI engine with Ready to use ML Pipeline for prediction, recommendation, optimization, forecasting, Natural Language Processing, and anomaly detection to provide advanced analytics based on AI/ML.		
38	Common Enabling System: Platform should be enabled with the following common services delivery-		
39	1. Mobile Enablement – Integrate with mobile applications and enable service		
40	2. GIS Integration Engine to work with various Map and Map Services – Custom Map, ESRI (offline) and Google (online). GIS integration may also be made with indigenous GIS system (https://stategisportal.nic.in/stategisportal).		
41	3. Inbuilt, pre-integrated security system for Device, User and Data Security		
42	4. Logging and Monitoring for platform and application services uptime		
43	5. BPM Engine to create Dynamic Workflows and Automate SOP execution		
44	Out-of-the-Box Tools: The Platform should have built-in tool capabilities to support easy provisioning and management of the platform, build and deploy -ML models, configurable dashboards, and reports		
45	1. Platform Administration tool- Tool which shall act a central hub for Smart City platform administration and monitoring		
46	2. Machine Learning Composer – Visual programming-based environment for building Machine Learning Models and deploying the same		
47	3. Configurable Dashboard- Enable customer to personalize their dashboards and deploy faster		
48	The Platform should be integrated and work with unified communication and Contact Center System for Call handling, routing, and recording. Standard APIs should be available for quick and easy deployment.		
49	The Platform should be integrated with Building Management System to integrate various building systems through BACNET and Modbus network protocols.		
50	The Platform should be integrated with SCADA System to integrate various SCADA Sub-systems through OPC UA		
51	The Platform should be integrated with Advanced Metering System for Meter Data Management and Insights.		
52	Data Integration Subsystem- Data Acquisition from Sensors/Devices : The digital platform should be a pre-integrated with IoT and AI capabilities, thus enabling the city with actionable intelligence.		

53	The platform should be able to integrate with any type of sensor platform being used for the urban services irrespective of the technology used. The Platform shall be agnostic to communication channels such as LoRA, ZigBee, GPRS, Wi-Fi, IP Camera		
54	It supports a secured multitenant layer to acquire and validate data collected (push/pull) from the sensor and transform rough data into valid, verified, possibly corrected data.		
55	Edge Analytics: It should pre-process the data in real-time from the sensors using Edge computing capability.		
56	The Platform should provide SDK support which have low code, highly secured and low footprint model runtime that can be embedded in IoT gateways and small footprint edge devices.		
57	Network Protocol Adoption: It should support bi-directional communication between platform and the sensor system.		
58	It should be network and protocol agnostic.		
59	Identity Store: The Platform shall provide a centralized identity registry for device management and provisioning operations. The inbuilt registry will establish an identity for devices and track metadata such as the devices' attributes and capabilities.		
60	The Identity Registry shall use a hardware fingerprint to authenticate IoT device with its Physical Unclonable Functions		
61	Backbone Messaging System: The Platform should have a Backbone Messaging System like Kafka for building horizontally scalable real-time data pipelines to receive, store, route and deliver messages.		
62	Data Normalization : The Platform shall automate the steps required to analyse data from IoT devices. It should transform and enrich IoT data before using it for real-time analytics and time-series data storage for analysis.		
63	It should support transformation of messages from native protocol of devices to a common format and should have data transformation adaptors to perform better analytics on runtime.		
64	It should be agnostic to sensor technologies and integrate with various types of sensor platform.		
65	The Platform should allow normalization of all the in-coming data from different devices of various OEMs.		
66	API Management System : The Smart City digital platform should be pre-integrated with API & ESB Integration System that enables various smart city applications to be integrated covering existing and proposed new applications in a seamless manner and provide service automation.		
67	The API & ESB subsystem shall cover - API gateway, Key Manager, API Portal, ESB and Analytics & Monitoring.		
68	API Management System shall be capable of supporting policy enforcement for API subscriptions, application creation, etc. with the help of customizable workflows.		
69	Normalized APIs for the City Application domains should be available (Parking, Outdoor Lighting, Traffic, Environment, Urban mobility etc.) to monitor, control sensor and/or actuators functionality to enable app developers to develop apps on the platform. For example, Lighting APIs: Vendor agnostic APIs to control Lighting functionality		

70	API Management System should possess Cross collaboration APIs: Enabling contextual information and correlation across domains and verticals (Multiple vendor and Multi-sensor in future)		
71	API Gateway: The platform should enable decentralized API management policies		
72	Key Manager: The platform should authenticate and authorize API requests from any client or device types that requests the resource servers which are operating on traditional and microservice architectures.		
73	API Portal: The API portal shall be the repository of standard APIs for consumption by any third-party applications/ sub-systems		
74	Normalized APIs should be available to carry out integration with other platforms/applications		
75	Enables City and/or its partners to write software adaptors based on the API(s) provided by device vendors and have the ability to control, monitor and collect the data from these street devices		
76	Services and Protocol Support: API Management System should possess integrated ESB solution capable of ensuring pluggable approach to Smart City Application		
77	Route, Mediate and Transform Data: API Management System should possess following routing capabilities such as header based, content based, rule-based and priority-based routing		
78	API Management System should possess mediation capability to support all Enterprise Integration Patterns (EIPs), database integration, event publishing, logging & auditing and validation		
79	API Management System should possess payload transformation capability to support XSLT 1.0/2.0, XPath, XQuery and Smooks		
80	API & Interface Security: API Management System should support security standards: OAuth 2.0, HTTPS over SSL, and key management help protect the data across all domains.		
81	API Management System should support security features built for many of its components by using HTTPS, TLS for all its public facing API implementations. For deployment where CCC Software API(s) exposed to application eco system, API Management, API security features and API Key management functions are required.		
82	Control Access and Enforce Security : API Management System should be capable of configured Single Sign-On (SSO) using SAML 2.0 for easy integration with existing web apps		
83	ESB System: The ESB System shall be highly available (Active / Active, Failover, Load Balancing, etc.)		
84	The ESB System shall support common publish-subscribe architecture		
85	The ESB System shall be capable of vertically and horizontally scalable		
86	The ESB System shall support synchronous and asynchronous transactions		
87	The ESB System shall support service orchestration, business process management, and complex event processing		
88	The ESB System shall provide common management capabilities (monitoring, auditing, and logging.)		
89	The ESB System shall support general use of XML as the messaging language		

90	The ESB System must enable the management and control of APIs exposed to third parties by identifying authorized access, time of access, SLA and number of allowed requests etc.		
91	The ESB System must support real-time monitoring and management of APIs at runtime		
92	The ESB System must enable appropriate and authorized users to easily create and edit new workflow processes through a graphical user interface that will specify the steps of the workflow, business rules around each step, authorized users, and control points that require manual authorization		
93	The ESB System design shall incorporate a multi-bus approach supporting micro-services architecture and differentiation between internal and external integrations		
94	The ESB System shall be Service Oriented Architecture (SOA) capable and support SOA standards.		
95	Data Processing sub-system - Complex Event Processing System		
96	The Smart City digital platform should be pre-integrated with Complex Event Processing System with BPM enabling the configuration of the Policy, alarm management and execution of SOPs. The system shall provide extensive capabilities in detecting anomalies and also correlating anomalies across various city domains.		
97	The Complex Event Processing sub-system shall allow the city to create complex analytics on sensor data with Adaptive Intelligence		
98	The Complex Event Processing sub-system shall have a drag and drop functionality using which rules can be applied to a single stream of data or multiple streams from interconnected sensor systems.		
99	The Complex Event Processing sub-system shall process and integrate millions of events per second in real time with <10ms latency.		
100	The Complex Event Processing sub-system shall support streaming and complex event processing types such as filters, streaming aggregations, patterns, non-occurrence, anomaly detection, Aggregative Functions (window based, or Start Based, Group based), Joins (works with Windows) Pattern, Sequence, Geo Spatial and etc.		
101	The Complex Event Processing sub-system should allow Application to		
102	- Generate alerts based on thresholds		
103	IF, Then Else analysis - Based on input		
104	The Complex Event Processing sub-system should calculate aggregations over a short window (time, length, session, unique, etc) or a long time period		
105	- Average, Sum etc		
106	The Complex Event Processing sub-system should perform Analytics based on geo spatial data which includes		
107	1. Alert based on geo boundaries - Geo Fencing		
108	2. Distance Travelled		
109	3. Speed		
110	The Complex Event Processing sub-system should calculate aggregations over long time periods with seconds, minutes, hours, days, months & years granularity		
111	- Correlate data while finding missing and incorrect events		

112	- Detect temporal event patterns		
113	- Analyse trends (rise, fall, turn, tipple bottom)		
114	- Run pre-treated machine learning models (PMML, TensorFlow)		
115	- Learn and predict at runtime using online machine learning models		
116	It should support Static rule processing, Context specific rule processing, Dynamic rule processing, Decision making through synchronous stream processing, Query tables, Windows and Aggregation.		
117	It should serve the following value propositions,		
118	- Ability to respond to real-time data with intelligent & automated decisions		
119	- Should provide an environment for designing, developing, and deploying business rule & event applications		
120	- Should provide an integrated development environment to develop Object Model (OM) which defines the elements and the relationships		
121	- Should be able to deal with the change in operational systems based on the operator's decision		
122	Data Management System- Big Data System		
123	The Smart City digital platform should be pre-integrated with Big Data based Data Management platform based on Hadoop.		
124	The Platform shall support Big Data Lake for storing all the data and supports various data stores - Key Value Store, Time Series and Documents based.		
125	The Big Data System should be highly scalable in terms of storing large volumes of structure and unstructured data.		
126	The Big Data System should support various engines for ingestion - IoT, ETL based services, APIs based Services and Connectors		
127	The Big Data System should be pre-integrated with BI and AI/ML engines for Business Intelligence and Predictions.		
128	The Big Data System governance framework should cover administration, security, configuration, and reporting.		
129	The Big Data System should be able to consume raw data feeds from different data sources and ability to prepare information for downstream uses. E.g., Ability to process data coming through online systems, mobile apps, social media, edge sensors, third party applications and tools, data files (EXCEL, GIS etc.) and different data bases for effective interpretation.		
130	The Big Data System should support the latest open-source projects of Apache Hadoop and Spark ecosystems. Should stay up to date with the newest releases of open-source frameworks, including Kafka, HBase and Hive LLAP etc.		
131	The Big Data System should be designed to avoid storing and processing of duplicate data		
132	The Big Data System should support System Integration (E.g., Web services) and Data integration (E.g., ETL / ELT) functionality out of the box with capabilities for data transfer to Big Data Platform to support Analytics Use cases with different latencies.		
133	The Big Data System should be capable of using connections to perform all the tasks and to implement the following Integration Services features:		

134	The Big Data System should have connection with source and destination data stores such as text, XML, Excel workbooks, relational databases and bigdata to extract and load data		
135	The Big Data System should have connection with relational databases that contain reference data to perform exact or fuzzy lookups		
136	The Big Data System should have connection with relational databases to run stored procedures and SQL commands such as SELECT, DELETE, and INSERT		
137	The Big Data System should have connection with SQL Server to perform maintenance and transfer tasks such as database backup and login transfer		
138	The Big Data System should have connection with Analysis Services projects and databases to access data mining models, process cubes & dimensions and to run DDL code		
139	The Big Data System shall specify existing or create new files and folders to use with Foreach Loop enumerators and tasks		
140	The Big Data System should have connection with message queues, windows management instrumentation (WMI), SQL Server Management Objects (SMO), Web, and mail servers.		
141	The Big Data System must provide the ability to make OLAP and OLTP transactions in the same time		
142	The Big Data System must support both Column-based and Row-based in-memory data structure		
143	The Big Data System should have Schema flexibility and ability to add columns on real time		
144	The Big Data System should have security mechanism for metadata access by enabling controls on access to entity instances and operations like add/update/remove classifications		
145	The Big Data System should be Integrated with centralized RBAC store to enable authorization/data-masking on data access based on classifications associated with entities. The authorized access would be classified as Personally identifiable information (PII) and SENSITIVE		
146	Data as Service Server should be capable of enabling API access to the Sensor/ Event data through Interactive querying. It shall also have pluggable approach that would allow the system to extend the API requirement using the standards		
147	The Integrated data access system should have APIs including Real Time Data, Latest data, Time series data and Search data		
148	It should aggregate time-series data from sensor/device-based system and event series data through ETL process to get insights of operational view and KPIs.		
149	The stored data shall be leveraged using Machine Learning and Analytics engine to enable Real time interactive querying, enable intelligence by KPI based reports and Analytics.		
150	Data Analytics sub-system		
151	The Smart City digital platform OEM should be pre-integrated with analytics engine to enable necessary insights and analytics.		
152	The Analytics sub-system should be an AI-based smart city analytics platform module to maximize business value through advanced machine learning capabilities. The		

	machine learning capabilities aid in automating policies that result in better asset and infrastructure management.		
153	The platform shall be pre-integrated with analytics to perform multi-dimensional analysis on incidents data supporting business intelligence and machine learning capabilities that enable delivery of pre-packaged analytics applications like dashboard, reports, advanced analytics - disaster management, social analytics, etc.		
154	The Platform shall be integrated with analytics engine, and which shall support following capability.		
155	The Analytics sub-system should support multiple Data Sources. Min below standard data sources should be supported from day 1 – CSV, TSV, MS Excel, NoSQL, RDBMS		
156	The Analytics sub-system should be able to discover, compare, and correlate data across heterogeneous data sources to unravel the patterns that are previously hidden. At a broader level system shall support following tasks:		
157	• Connect to a variety of data sources		
158	• Analyze the result set		
159	• Visualize the results		
160	• Predict outcomes		
161	The Analytics sub-system should be capable of performing descriptive, predictive, and also prescriptive analytics wherever applicable.		
162	The Analytics sub-system should have capability to analyse data in motion to display the alerts in real-time and store the data in centralized database for future trend analysis.		
163	The Analytics sub-system should be capable of developing predictive analytics based on the requirements of the city. Domains can range from Solid Waste, Transport etc.		
164	The Analytics sub-system should provide with end user access ranging from ETL, integration of data from structured & unstructured data sources, intelligence with simulation and modelling and interactive dashboards with ad-hoc query, integration with spreadsheets, proactive alerting, Scorecards and so on.		
165	The Analytics sub-system should provide capabilities to create KPIs to measure progress and performance over time and graphically communicate strategy & strategic dynamics using Strategy maps, Cause and Effect diagrams, and Custom views. Intuitive and dense visualizations must be available.		
166	The Analytics sub-system should help simulate what if scenarios. It should help visualize assets/resources at risk due to the pending/ongoing incident, should render impacted region on a GIS/3D map. The solution should help build the list of assets, their properties, location and their interdependence through an easy-to-use Graphical User Interface. Solution should highlight not only the primary asset impacted but also highlight the linked assets which will be impacted.		
167	The subsystem should be capable of providing time-shifted or offline analytics on the archived data.		
168	It should provide capabilities for the analysis to run autonomously, refreshing data and re-analyse the situation continuously across a complex set of variables.		

169	Analytics Engine Visualizations		
170	Analytics sub-system should provide visualizations dashboard.		
171	In the visualization workspace, it should allow to change visual attributes of a graph.		
172	User should not be allowed to alter the graph/visualization definition.		
173	In the visualization workspace, user should be able to do the following operations:		
174	- Change the graph/visualization type		
175	- Print the graph		
176	- Export the graph		
177	- Narrow down on the value ranges		
178	- Toggle the axis labels		
179	- Integrate with other 3rd party applications seamlessly		
180	Sentiment Analytics		
181	The Analytics sub-system shall have the capability to provide sentiment analytics of configured key words/accounts through internet crawling through the platform. Ability to categorize key issues/topics/words in real time on social media platform (Twitter, Facebook, Website Discussion Forums, News Papers) which are contributing to negative/positive perception among citizens.		
182	Business Intelligence		
183	The BI subsystem should be capable of providing vertical specific models and report repository.		
184	It should support tabular models at all compatibility levels, multidimensional models, and data mining service.		
185	It should be built considering scale from ground up and should have single source of analytical data to ensure discrepancies at minimum.		
186	The Analytics sub-system shall be capable of carrying out business intelligence as well as real time analytics for city systems where it shall develop insight into possible future conditions or events. Analytics shall measure the efficacy of services delivered and help operators and city personnel to test scenarios.		
187	The Analytics sub-system shall make use of cross-system data analytics from historian and real-time information received from independent systems through smart city platform to aid in the operations and management of city services.		
188	The system shall have ability to synthesize, analyse and integrate data from all City systems and should provide analytical insights to city integrated operation Centre for running real time sensors and to decision makers for policy making and optimizing decisions.		
189	Platform should provide a user friendly; web based, drag and drop interface for data processing		
190	Platform should be capable of summarizing and presenting the data using a variety of highly customizable charts		
191	Platform should be capable of displaying and tracking of metrics with the support visual features like Metric Dials and Graphs etc.		
192	Platform should be scalable to incorporate any additional functional requirements (Low Code Tools-like IOTops, ML Composer, Configurable Dashboard)and analysis capabilities.		

193	Platform should be capable of displaying the dashboards on third-party tools/applications		
194	Platform shall allow generation of dashboard using ad-hoc queries by the user		
195	The reporting solution should be web-enabled		
196	Platform should enable different types of users to conduct effective explorations on all available data without the need of subset, sample, and multiple views of data with minimal training for users		
197	Platform should have self service capability in importing and integrating local text/csv/xls files with the data warehouse and be able to generate reports		
198	Platform should assist the user with explanation on forecast results by providing “What does it mean” capabilities		
199	Platform should provide geographical map views to provide a quick understanding of geospatial data		
200	Platform should provide capabilities to subset data independently without any technology intervention		
201	Platform should allow ad-hoc hierarchy creations for traversing till intricate information to execute root cause analysis		
202	Platform should provide the capability to export data in Excel and CSV/TSV document formats		
203	Platform should provide the ability for user to view interactive reports using iOS & Android devices using a native application. It should provide rich user experience with capabilities such as gesture control, zoom and swipe etc.		
204	Platform should provide the capability to the user to save and share the analysis as exploration, report, or PDF		
205	Platform should directly extract information from transactional systems without depending on data warehouse or data marts		
206	Platform should be capable of scheduling data updates and report refresh		
207	Platform shall have capability to generate MIS reports		
208	Platform should enable the user with an interface to design reports and dashboards with automatic refresh capability on changes in underlying data		
209	Platform should allow the user to drill down the reports to the granular level of details		
210	Platform should be able to populate/ filter output with interactive filtering of reports from existing selection		
211	Platform should be capable of passing parameters among reports to retrieve details and investigate specific entity		
212	Platform should enable the user to execute pre-defined procedures using the interface to visualize reports		
213	Platform should support configurable report generation based on ad-hoc querying across multiple fields of entity-wise information		
214	AI Data Pre-Processing		
215	Platform should enable machine learning with big data, providing the ability to obtain valuable insight from large amounts of structured, unstructured and fast-moving data		

216	Platform should enable organization and labelling of data by the intelligent methods of alignment and indexing		
217	Platform should be capable of handling missing data		
218	Platform should support data cleaning operations.		
219	ML Libraries Notebook		
220	Platform should be capable of native support for asynchronous execution of collective operations and peer-to-peer communication		
221	Platform should allow user to export models in the standard file formats(Pickle, H5, ONNX)		
222	Platform should enable fast, flexible experimentation and efficient production through a hybrid front-end, distributed training and ecosystem of tools & libraries		
223	Platform should have a web-based notebook that would enable data-driven, interactive data analytics and collaborative documents		
224	The notebook should possess a console-based approach to interactive computing, providing a web-based application suitable for capturing the whole computation process: developing, documenting, and executing code and communicating the results.		
225	Model Store and Service		
226	Platform should allow the user to convert ML model to a bitstream, store it in disk and reloaded at any point of time.		
227	Platform should allow the user to do real time and batch predictions using the models		
228	Platform should create an API wrapper around the predicted model and should be capable of deploying it as a web-service		
229	Common Enabling System : The Smart city platform should be pre-integrated with Common Enabling System that will extend the capabilities of the platform to configure and automate the workflows, build location intelligence, provide mobile enablement of the services, provide security system for Identity and authentication of devices, users & data and support Logging & Monitoring for Application working and performance.		
230	Business Process Management		
231	The Smart City digital platform should be pre-integrated with Business Process Management (BPM) sub-system that would enable the process automation, delegation, parallel workflows, etc.		
232	It should be capable of handling parallel process flows, that would carry out all possible combinations including split, merge and cross reference of processes. It		
233	It should also enable the user to delegate or assign an activity to individuals or teams.		
234	GIS Map Support		
235	Platform must provide ability to configure various geo-spatial data from different providers including but not limited to City GIS systems		
236	Platform must provide ability to support different geo spatial formats from commercial and open geospatial standards.		
237	System should support integration with any Map API services like Google, Esri, Open Street, etc. It should be possible to visualize all the Assets (Sensor, Devices, Vehicles, Cameras, other city resources) on map.		

238	It should be possible to visualize all the Assets (Sensor, Devices, Vehicles, Cameras, other city resources) on map.		
239	The Assets must be provided as layers with ability to switch these layers and visualize the assets of only selected layers.		
240	The GIS Maps should provide interactive visualization of travel time and traffic based on the sensor data and data ingested from 3rd party sources.		
241	It should allow the operator to execute dynamic messaging across the city through the sign boards to inform the citizens in real time.		
242	GIS Platform shall support GIS Maps in following file format PDF, JPG, PNG, Vector PDF Map, Web Map Service (WMS) defined by the Open Geospatial Consortium (OGC), Google Map-aerial; terrain, Bing Map, aerial, satellite, hybrid, ArcGIS/ESRI and Open Platform GIS Applications		
243	GIS platform should provide a picture-in-picture map view capability,		
244	- Upon the availability of GPS positioning of a file, the user should be able to quickly alternate between the video and map view within the video player		
245	- The application must be able to ingest and present either a static location (e.g., for a fixed camera) or dynamic location (e.g., for mobile cameras) that allows users to validate the location where the video was recorded at the time of the event		
246	Location engine		
247	a. Map services and geospatial coordinates: Shall provide the geographical coordinates of specific facilities, roads, and city infrastructure assets, as well as unmapped facilities		
248	b. Geospatial calculation: Shall calculate distance between two, or more, locations on the map		
249	c. Location-based tracking locates and traces devices on the map		
250	IoT Security		
251	The Platform should set up individual identities and credentials for each of the connected devices and help retain the confidentiality		
252	The Platform should provide mutual authentication and support encryption at all points of connection, so that data is never exchanged between devices and IoT Platform without a proven identity.		
253	To maintain the integrity of the system, the Platform shall allow the user to selectively revoke access rights for specific devices as needed.		
254	To ensure the flexibility for the device vendor, the platform should allow the user to create Authentication and Authorization policies based on device profile level, it shall also support the below policies:		
255	1. Standard Authentication		
256	2. Custom Authentication		
257	3. x.509 Certificate based Authentication		
258	Standard Authentication should comprise of Time-based password for the device to ensure that in case the device gets compromised, it can only utilize the token for the defined time.		
259	Security - IoT Device Identity Registry		

260	All IoT Device connecting to the IoT Platform shall be secured through strict device Identity Policies and token-based authentication		
261	The Platform shall Support AES 128, 256 Based Payload Encryption.		
262	The Platform shall have Per device authorization policies to ensure zero data leak tolerance.		
263	Security - User Identity and Access Management		
264	Role based access shall be enforced for all application activities.		
265	The Platform should support LDAP to be used as an additional data store for user management and authentication.		
266	Shall have Single Sign on and Multi factor authentication for secure user access to application services		
267	Data Security & Integrity		
268	Data Governance / RBAC: The Platform should support data governance & stewardship model, in which roles, responsibilities are clearly defined, assigned, implemented, documented and communicated		
269	Data Protection / Production Data integrity: The Platform should support procedure in place to ensure production data shall not be replicated or used in non-production environment		
270	Data Protection / Data at rest: The Platform should support encryption for tenant data at rest (on disk/storage)		
271	Data Retention: The Platform should support capabilities to enforce tenant data retention policies		
272	Data recover & restore: The Platform should support capability to recover and restore data in case of a failure or data loss.		
273	Data disclosure & privacy: The Platform should disclose data attributes, elements collected from source. All the attributes should be disclosed & appraised to data owner. With appropriate approval from City authority, Platform should have ability to encrypt sensitive data element at rest.		
274	Configuration of Data Security Features		
275	The Platform shall have the ability to configure user access and authorization control to provide specific set of information/data/application control to designated or authorized set of users. For E.g.: Ability to restrict water department operation team to view water billing data (if not authorized).		
276	Cybersecurity framework and security		
277	A Cybersecurity framework should be developed aimed at building a secure and resilient application for citizens and stakeholders of Smart City. The framework comprising of policy, procedures, and guidelines should be designed to protect the application and information; build capabilities to prevent and respond to cyber-attacks; and minimize damages through cyber-attacks.		
278	Data Governance		
279	The Platform shall be Integrated with data governance to ensure only authorized owner have permission to read / write data into the system.		

280	The Platform shall allow storage encryption to prevent illegal data and behavioural tracking activities		
281	The Platform shall assure data quality in terms of accuracy, accessibility, consistency, completeness and updating.		
282	The Platform shall Govern all aspects of API Access services including data service descriptions, data consumption, service usage, service discovery, service lifecycle management and service policy		
283	Monitoring - all the data access from the application shall be logged and monitored		
284	Centralized Logging & Monitoring Platform		
285	The Platform shall consist of a centralized logging and Monitoring platform which integrates with all part of platform services for Audit and performance monitoring.		
286	The Centralized Logging and Monitoring sub-system should be integrated with all smart city application and the IoT platform to give the user an operational view		
287	The system should be able monitor the application/platform infrastructure for performance with time series view of:		
288	- Up time		
289	- CPU Utilization		
290	- Network Utilization (Bytes received per second, Bytes sent per second, Packet drops and Timed out connection)		
291	- User connection count		
292	- Disk connection count		
293	- Process Count		
294	- Total threshold count		
295	Platform should keep track of sensor last seen date and time and be able to detect disconnected sensors & raise alarms		
296	The Platform shall allow time shifted analytics with the log data.		
297	The user should be enabled to control all the platform service from a single system, the control operation includes		
298	1. Service Restart		
299	2. Update Configuration		
300	The system should allow user to get detailed SLA monitoring along with SLA report		
301	Out of the Box Support for Tools: The Smart City Platform should support pre-integrated Tools for Provisioning and Administration, Composing and Building ML models and support Configuration of dashboards.		
302	Provisioning & Service Management		
303	The Smart City digital platform OEM shall provide solution for enabling end to end Platform Administration which includes Asset Management, Rule Configuration & Workflow Management.		
304	The solution shall have a view of all the sensors connected to the platform with their health status for real time monitoring.		
305	The solution shall support secure device onboarding process with bulk uploading options.		

306	The solution shall be capable of sensor health abnormality detection and automated workflow execution with integrated workforce app.		
307	The solution should provide icon-based user interface on the GIS map to report non-functional assets.		
308	The solution should also provide a single tabular view to list all assets along with their availability status in real time.		
309	Machine Learning Builder		
310	ML Composer should provide an environment to build machine learning models through low-code/no-code visual toolkit for developing, deploying, and operating enterprise AI ML driven applications.		
311	The system also supports traditional ML models, time series forecasting, and deep learning.		
312	There shall be a tool for the city administrators to create analytics / predict outcomes, when necessary, the tool provided shall allow the user to develop models for analytics using the necessary data available to the user.		
313	The Machine Learning Tool should have an easy-to-use, visual interface that gives users the access to data exploration.		
314	The Machine Learning Tool shall support data input from multiple data Sources for data accumulation.		
315	The Machine Learning Tool supports ready to use ML Pipeline for prediction, recommendation, optimization, forecasting, Natural Language Processing, Anomaly detection.		
316	The Machine Learning Tool should support users to choose from multiple Machine Learning Model types like (Not limited to:)		
317	1. Auto ML: Users can select this option and the system automatically selects the Algorithm based on best accuracy		
318	2. Manual ML: Users can select Algorithms manually and provide parameters based on the selected Algorithm		
319	3. Geo ML: Users can select ML Algorithms especially built for Geospatial Data.		
320	Users can Export files in multiple data formats (CSV, PDF, Excel etc.)		
321	The Machine Learning Tool shall allow the users to load disparate data sources and join, filter, and wrangle data, all without having to write queries.		
322	Configurable Dashboard		
323	Configurable Dashboard should help in reducing the customization time for building the dashboard.		
324	Configurable Dashboard should provide a single web interface for configuring the data source to visualize the data using various visuals available		
325	Application should allow to connect various data sources for fetching the data. The Configurable Dashboard shall provide the user to connect with any data source provided in the application for fetching the data and later can be configured in the widgets Standard Dashboard templates should be available for various Smart City Domains- Surveillance, Traffic, Environment, Parking, Waste Management, Energy, Buildings		

326	The application should provide GIS based visuals for geospatial analysis.		
327	The application should allow user to configure the basic settings, colour theme, etc. which need to get updated throughout all the widgets built		
328	The application will allow user to create widgets which can be used for building the dashboard. Once the widget configuration is done, the same widget can be used in multiple dashboards without the need to create multiple times		
329	The user should be able to fetch the data from the saved data source and configure the dataset for the selected widget.		
330	The user should be able to view the configured widgets which user can bring a common place and create the layout as per the need.		
331	The user should be able to save the dashboard and can get shareable link which can be used to embed the dashboard in any application		
332	The user should be able to create a KPI defined on top the connected data source. If the KPI has been met, a pre-defined process should be executed.		
333	The Smart City Software Suite should support pre-integrated applications software that enable the digital transformation of cities. The applications should be fully integrated with the City Platform and can be modularly deployed in a phased manner.		
334	Command & Control Centre: Integrated Command & Control Center System to build a unified city operations centre for Major Incidents and Events.		
335	Advanced Analytics covering Business Intelligence (BI) and AI/ML.: Advanced Analytics Applications to derive intelligence and drive efficiencies in operations of the various in-line departments. Standard BI Dashboard templates for various smart city domains.		
336	Mobile Workforce Management System to unify the city workforce across departments through a common App: Mobile Workforce Management System to unify the city workforce across departments through a common Workforce app and empower them with real-time intelligence and mobility		
337	Smart City Solutions. Optionally it should be possible to extend the Smart City Platform services and build various in-line department specific solutions for use the by the various departments. The various applications can cover.		
338	Solid Waste Management System for garbage collection and disposal.		
339	Parking Management System for booking and availing parking services.		
340	Intelligent Transport System for public transit and passenger information.		
341	Intelligent Street Light System for optimising the use of the Street Lights		
342	Command-and-Control Centre		
343	The Command-and-Control Centre should be pre-integrated with the platform and shall act as the central hub for integration of the various systems and form the foundation for the city administrator to manage the city operations. The Integrated Command and Control Center Software should support Incident Management and provide a 360-degree situational awareness of the city operations with real-time KPI based operational dashboard.		

344	Incident Management - General Capabilities. Incidents are verified and converted from alerts (Like Camera based Alerts, Bin Fill Alert, Environmental alerts etc) generated by various sensors/systems. The each type of alarms are configured based on the rules defined. This will consider during detailed engineering and design phase.		
345	The application should:		
346	help the city operators to run the city efficiently by integrating all the alarms and provides an easy-to-use GUI interface (web & client server)		
347	help manage: alarms, map-based visualization of the city assets and events, execute SOPs and coordinate the operations;		
348	provide 360-degree situational awareness and insights across urban functions to city administrators.		
349	SOP Execution:		
350	Based on the incident type, system shall open the activities that need to be carried out for the incident. The SOP shall provide the actions like notification, correlate, dispatch, and close incident. This activity should be defined in the administrator system for each type of incident. This activity will be either manual or automated. SOP's will be configured based on the concerned department's usage through administrative module as well as will consider during design and detailed engineering phase.		
351	It should be integrated with a real-time KPI dashboard that will provide 360-degree situational awareness of the various urban system operations and efficiency.		
352	The alarm management module should:		
353	enable the City Operations Center (CoC) to service all alarms generated automatically by the city digital platform for operators to visualize the alarms, create incidents and dispatch city workforce for action.		
354	Provide the details about each alarm received from the various sub-systems integrated.		
355	provide the operator details regarding the source of the alarm, type of alarm, generated time, priority, and elapsed time to take appropriate action.		
356	provide advanced map & video visualization for situation awareness.		
357	provide an easy use GUI that is simple to operate.		
358	operator to view various types of alerts in a single place and validate the alerts for further processing.		
359	GIS Visualization		
360	The application shall provide map-based visualization for all the details of the alarms and enable the operator in decision making.		
361	Application enables visualization of all the assets (camera, access control, lighting) on the GIS map as a layer.		
362	Unique identification (icon /symbol) should be provided for each of the asset types.		
363	The application shall allow health status (functional /non-functional) of assets to be identified using colour code.		
364	All field resources (vehicles /field workforce) should be location enabled and mapped to the GIS with unique identification (icon /symbol).		

365	Each of the asset shall be created as a layer on the map and can be turned ON /OFF by the operator depending upon the alarm type and incident use case.		
366	The application shall enable operator to search assets based on the type and jurisdiction and enables operator to object based interactive building floor plan, parking lot layouts, bus inside, etc.		
367	Video Visualization		
368	The application shall provide video-based visualization of all the associated cameras for the alarms in matrix view and enables the operator in decision making.		
369	Selection of cameras can be based on the following:		
370	I. Map based selection		
371	II. Jurisdiction/ camera selection from the camera list alert the details of the alerts		
372	AI and BI Applications		
373	It should support AI applications to solve narrow problems covering the various urban systems and build applications to deliver actionable insights and optimise the operations.it should also support standard BI dashboard templates for various smart city domains so that it can be configured and deployed readily.		
374	Social Analytics / Citizen Sentiment Analytics		
375	The Application should predict, analyse and report the activity’s happenings in social media through automated intelligent applications		
376	The application should evaluate newly launched programmes and policies through a continuous feedback loop		
377	The application should pave the way for better governance by keeping a tab on the pulse of citizens through real-time analysis of feeds from social websites		
378	The application should provide various analytics trends, heatmap for geo-tagged data, word cloud based on posts received from various social media platforms		
379	The application should analyse the sentiment of posts and categorized into positive, negative and neutral in dashboard view.		
380	The application should recognize the named entity for creating word cloud to give an overview of the words which is used most by the people.		
381	BI Dashboard Templates		
382	The Dashboard Templates must cover various smart city domains – Surveillance, Environment, Transport, Parking, Traffic, Waste, Buildings, and related components such as HVAC, Elevators, UPS/DG Set, Fire Alarm, Security etc.		
383	Mobile Workforce Management Application System		
384	It should support Mobile Application to unify the city workforce and enable the day-to-day activities thus driving efficiency and speed of operations. It should be pre-integrated with the platform data and services and should support various types of user roles across the departments of the city.		
385	Workforce Mobile App		
386	The application should provide intelligence and insight for city workforce to stay connected and act on real time.		

387	It should be based on user roles and support workforce across various departments		
388	Workforce app should be able to visualize all the events with the status		
389	App should have provision to filter the events based the activity status (All, Pending, In Progress and Completed) and criticality (Low, Medium and High)		
390	App should provision to view event details like Event Name, Location, Source, Time		
391	Provision to navigate to the event location		
392	Provision to attach image, video, audio as action taken report		
393	Provision to chat with control room operator		
394	Provision to view lists of jobs and events based on day wise view, week wise view and month wise view on a calendar		
395	Provision to access the map-based view of current location		
396	Provision to share location, identify nearby workforce		
397	Provision to report any incident from the field to the command centre operator/ department operator.		
398	There should be a provision to track the location of the workforce by the Command Center/department operator		
399	App should be available for Android and iOS		
400	Workforce Management Web Portal		
401	The portal should allow for easy configuration of User Roles, e-Form and enablement of various user services based on department requirements. Various user services to be enabled for workforce are: 1) My Events 2) My Schedules 3) Communicate- Chat, Video and Audio 4) Nearby workforce, events, departments 5) Report Incident 6) E-forms 7) Attendance 8) Chat		
402	It should provide a dashboard covering total running and closed schedules, online and offline users, Pending and closed incidents.		
403	Provision to add new events based on the Event code, Event Name, Time to Complete (Target time to complete - in Minutes), Priority (Drop down - High, Medium, and Low), Assign Form		
404	Provision to edit & delete event details and search for events from the event list		
405	Provision to view the workforce user list, add, edit, reset & delete user		
406	Provision to add group based on group name and group code		
407	Provision to create, edit and delete a new e-form		
408	Provision to search, view add, delete department		

S.No	Parameter	Application Use Cases	Dashboard Use Cases	Compliance (Yes / No)	Remarks
1	ITMS (Intelligent Traffic Management System - RLVD, ANPR, SVD,NHDS,TRDS,DOP,NSB)	Asset Synchronization	Live view of traffic density based on area and status		
		Geo Visualization	violation (Traffic)		
		Automated Number Plate Recognition (ANPR) Alert	Live view of traffic density by location		
		Red Light Violation Detection (RLVD) Alert	Alarm trend		

		Speed Violation Detection (SVD) Alert	Hourly/average and traffic speed		
		Unauthorized vehicle movement	Type of violation based on categories		
		Vehicle without valid permit	Type of violation based on alarm status		
		Vehicle without/expired insurance			
		Stolen vehicle as well as report vehicles by police department			
		Vehicles without valid PUC certificate			
2	Adaptive Traffic Control System (ATCS)	Synchronization & Geo Visualization of Traffic Signals	Total ATCS controllers		
		Real time monitoring of traffic Signals	Active ATCS controllers		
		Blinker mode activate and deactivate functionality	Inactive ATCS controllers		
		Signals running status (Auto/Manual)	Energy consumption per day		
		Traffic Signals health status (On/Off) as well alert	Percentage change (previous 24h)"		
		Congestion Alert (Over Saturated & Under Saturation)	Grievance statistics		
		Controller Fault Alert	Highest traffic density location		
		Blinker Mode Alert	Average traffic density in 24h		
		4D Radar failure alert	Realtime view of traffic sensors		
		Hurry Call/Green corridor SOP	Total Signals		
		Adaptive camera will provide the real time Vehicle count	ATCS Health Status		
3	City Surveillance System (VMS & VA)	Synchronization & Geo Visualization of surveillance Camera's	Live view of all the cameras within the city		
		City Surveillance Camera live feed for situational awareness	Total, Active, Inactive Camera's		
		Detection/Recognize the pattern of Demonstration & Conflicts in Crowd	Region wise Alarm Type		
		Detection of loitering person	Top 10 Crime Region		
		Tampering alert	Violation (Surveillance)		
		Wrong way or Illegal turn detection	violation (Traffic)		
		Speeding Vehicle			
		Accident Detection			
		Person Climbing Barricade			

		Person Collapsing			
		Vehicle of Interest tracking by speed, colour, and number plate			
		No Helmet Detection			
		Unwanted/			
		Banned vehicle detection			
4	Environmental Sensor	Synchronization & Geo Visualization of Environment sensor locations	Synchronization & Geo Visualization of Environment sensor locations		
		Environment sensor health alert status (On/Off)	· Total Environmental sensors		
			· Active environmental sensors		
			· Inactive environmental sensors		
		AQI alert through Environment sensor:	· Air quality trend based for 24hr based on time and date		
		1. Air Quality alerts will be generated based on standard threshold limits for CO, NO2, SO2,O3,CO2,PM2.5,PM10 like Good, Normal, Satisfactory, Moderately polluted, poor, very poor & Severe	· Real time air quality index		
		2. Alerts will be generated based on temperature, Humidity, Pressure & Noise	· Realtime temperature reading		
			· Realtime value of light intensity		
			· Realtime reading for noise level		
			· Air Quality trend based on day, Month, Year		
			· Real time Air quality analysis based on areas		
			· Air quality index for peak hours		
			· AQI Actual vs Forecast		
			· Pollutant Actual vs Forecast		
			Status of all alarms in the city (Total, received, closed)		
		Air quality Index Visualisation by hovering on Individual Sensor			
		Integration with GIS map with analytic layer			
5		VMD Synchronization & Geo Visualization			

	Variable Message Signboard		Realtime view of sensors on maps		
		VMD Operational Status (ON/OFF)	· Total VMD sensors		
			· Active VMD sensors		
			· Inactive VMD sensors		
			· VMD Alert status		
			· Energy consumption per day		
			· percentage change (previous 24h)"		
			· VMD Asset status		
		Pre-defined general information messages to Public (e.g., Traffic Congestion, Advertisement, Other relevant information provided by ASCL)			
		Specific Message (Manually defined message) to individual/selected			
		VMD's Regular health check-up (fault detection) of VMD device			
		Specific Image to individual/selected VMD's			
		Publish predefined data from Environment Sensor to the Nearest VMD Device			
		Device Health Status Alert in case of Ambient Light Sensor Off and in case of VMD Panel door open.			
6	Public Address System	PA Operational Status (ON/OFF)	Realtime view of PA systems on maps		
		Pre-recorded general information messages to Public (e.g., Traffic Congestion, Advertisement, Other relevant information provided by department)	Total PA sensors		
		Specific Message (Manual announcement) to selected PA's	Active PA sensors		
		Specific Message (Manual announcement) to selected PAs in multiple Zone's /Area	Inactive PA sensors		
		Regular health check-up (fault detection) of PA device	PA loudness		
		Play pre-recorded Audio Message individually or change the schedule of existing queue	PA Asset status		
7	ECB	ECB operational health alert status (On/Off)	· Incident Statistics		
			· Realtime view of sensors on maps		
			· Total ECB sensors		
			· Active ECB sensors		

			· Inactive ECB sensors		
			· ECB Call count ECB Asset status		
		Emergency alert through ECB with details (Caller Image, Caller Clip, Caller Voice & date, and time)			
		Show location of ECB systems on map with its current working status red & green along with issue in case of offline			
		Receive Emergency calls and showcases the location on GIS map & play nearest cameras for situational awareness			
8	GIS	ICCC Should integrate with the GIS MAP and support the MAP based visualization	Asset visualization on the MAP Screen		
		ICCC Should support marking of the event on the MAP Screen			
	Should Support Integration with future Applications.		Dashboard Use Cases		
9	Intelligent Transport System	Real-time fleet tracking and Management	Vehicle Dashboard		
		MAP Based visualization of the vehicle list, route list, Bus stop List,	View the map with the point of interests, live spot for buses, Bus stops.		
		View a list of vehicles on routes for ETA	Visualize the count of citizen grievances		
		Vehicle Scheduling - Time Table	Visualize the Fleet statistics		
		View the Device Alerts, Citizen Complaints			
10	Solid Waste Management System,	MAP based visualization of the assets like Vehicle Type, Bin Type, Vehicle Status, Citizen Grievance, Cameras	Visualize total Vehicles		
		view the tracking details of the vehicle such as Vehicle Number, Vehicle Type, Position, Speed, Location, Time on the map.	Visualize total Bins		
		Scheduling and trip playback	Visualize total Distance		
		Bin locations on the MAP Screen	Visualize total complaints		
		View list of households with details such as Bin Name, Householder, House Number, Zone, Ward, Road Name, Status.	Visualize total trips		
		Creation of POI's by providing details such as Zone, Ward, POI Name, POI Type, POI Long/Lat, POI Radius, POI Address.	Visualize staff attendance		
		Creation of Primary and Secondary Route	Visualize bin status (Primary/Secondary Collection status)		

		Staff Attendance			
11	Grievance Redressal System, and other e-Governance & Citizen services	Incident Creation	· Grievances Trend,		
		Search Grievances	· Total Number of cases		
		Filter Grievances based on the different sources such as (Citizen App	· Pending cases,		
		Chat, Voice Call, Twitter, SMS, WhatsApp, Email, City Chatbot, E- Governance, Citizen Portal, Facebook			
		Social Intelligence			
		Dispatch Workforce to attain the incident created	· In progress cases,		
		View the Logs of incident/non incident/calls	· Completed cases		
		Collect the feedback from citizen	· Citizen feedback		
		Chat with Citizens	· Chanel wise distribution of grievances		
		Visualize similar events	· Grievances Trend,		
		Visualize nearby incidents	· Total Number of cases		
		Visualization of the incidents and caller location on the MAP Screen	· Pending cases		
12	Street Lighting	Smart Light (Smart Pole) Synchronization & Geo Visualization with Branding	· Smart Light (Smart Pole) Synchronization & Geo Visualization with Branding		
		Smart Light (Smart Pole) Auto Switch ON/OFF and diming, based on Schedule	· Smart Light (Smart Pole) Health Alert (Fault detection)		
		Smart Light (Smart Pole) Health Alert (Fault detection)	· Single Light Failure Detection in a Smart Pole		
		Single Light Failure Detection in a Smart Pole	· Energy Consumption Monitoring and Visualization		
		Energy Consumption Monitoring and Visualization			
13	Drone Surveillance System	ICCC will be required to integrate with Drone Surveillance System (Through Drone OEM Video Management System or Server based connectivity) using open API Standards.			
		ICCC Should be able to showcase the live video feed of Drones.			

*** Few Important definitions/detailing of key words-**

1. **Urban System-**

The term any urban system used here to define the capability of integrating with any city urban systems over OPEN API's which includes (Existing/ Proposed/New Systems) which are required to be communicated with the ICCC Platform.

Urban System Integrations listed below are qualified based on the initial assessment of Guwahati Requirements. However we can update this based on your inputs.

1. ITMS (Intelligent Traffic Management System-RLVD, ANPR, SVD, existing ITMS feature)
2. ATCS
3. City Surveillance System
4. Smart Parking Application
5. Smart Pole and Smart Street Light
6. Public Address System
7. ECB
8. Environmental Sensor
9. Environment Sensor (Flood)
10. Variable Message Signboard
11. Smart Kiosks
12. Drone(UAV)

2. **Social Media Analyzing** -

- Social Analytics Application enables City Administrators and Safety agencies to listen to the various social media networks and websites and enable correlation of the data into sentiment analytics which can be mapped to various type of public safety incidents.
- The Platform enables the social listening of various social media channels through location, keywords, hash tags and users in near real-time. This transforms location-based social data to intelligence to understand what's happening in the specific jurisdiction zones. The Platform enhances situational awareness through social monitoring. It will allow hyper-local social search to monitor events, assess crisis areas and coordinate with field team. This allows the regulators to analyze the archived social data to identify keyword trends, time-based activity, influential contents, social sentiments etc. The reports are generated from the system by extracting social data and allows to share with rest of the organization in PDF/CSV formats.

3. **Sentiment Analytics**-

- Sentiment refers to the emotion behind the social media content and used to measure the tone of the conversation - is Positive (happy), Negative (annoyed/angry) or neutral. Text analysis which part of main module awards sentiment value to each tweet or any text comes it's away. It is powered by ML algorithms which is again trained on well-prepared data set to ensure high accuracy. It will classify and indicate the sentiment count as chart/graph per the topic of search. Trending hashtags are shown as part of analytics in the dashboard.
- The scope is to provide sentiment analytics of configured key words/accounts through internet crawling through the platform. Ability to categorize key issues/topics/words in real time on social media platforms (Twitter, Facebook, Website Discussion Forums, News Papers) which are contributing to negative/positive perception among citizens.

4. **Contextual Search**-

To engage immediate search on various social websites, this module will be used. These search results can be used for taking actions by the operator following the SOP's

5. **Overall Analytics View-**

This view presents overall spatial analytics on map as heat map to show active regions from where the feeds are coming, it also gives a line graph to show engagement of people over prescribed time. Overall sentiment can be understood through pie charts as shown in the screenshot below; Having analyzed the data we have we give list of top influences as well as recent twitter users with their profile description.

6. **Social Publish Module-**

This module gives the platform to the authorities to notify the citizens on any important news or announcements and keep citizens informed/ updated.

7. **Geo-Spatial Analysis -**

To analyze the social feeds on the map, we use this module which helps to locate the exact location from where the event is happening and action can be taken based on this. Operator can further filter the data by platform, sentiment, username, etc.

5.11 ENTERPRISE MANAGEMENT SYSTEM

Enterprise Management System - Technical Specifications			
Sr No	**Description**	**Compliance YES/NO**	**Remark**
Enterprise Management System (EMS) :			
	General		
1	For effective operations and management of IT Operations , there is a need for an industry-standard Enterprise Management System (EMS). Given the expanse and scope of the project, EMS becomes very critical for IT Operations and SLA Measurement. Some of the critical aspects that need to be considered for operations of IT setup of are: a) Network Fault Management b) Network Performance Management c) Network Configuration Management d) Server Performance Monitoring e) Network Traffic Analysis f) Centralized Log management g) Centralized and unified Dashboard h) Centralized and customizable service level reporting i) Helpdesk for Incident management j) Asset Management j) Project Management		
2	The Monitoring Solution should provide Unified Architectural design offering seamless common functions including but not limited to: Event and Alarm management, Auto-discovery of the Network environment, Correlation and root cause analysis, Reporting and analytics		
3	EMS/ NMS OEM must be an industry standard solution and shall be present in Network Automation and Orchestration Tools report. Documentary proof must be submitted at the time of submission.		
4	There should be a tight integration between infrastructure metrics and logs to have the single consolidated console of Infrastructure & security events.		
5	Consolidate IT event management activities into a single operations bridge that allows operator quickly identify the cause of the IT incident, reduces duplication of effort and decreases the time it takes to rectify IT issues.		
6	The Operator should be able to pull up security events related to a given Configuration Item, from a single console which also has NOC events, and use the security events to triage the problem. This way the Operator gets consolidated system/network event details and security events (current and historical) from the same console and save time in troubleshooting / isolating the issue.		
7	The solution should have capability to perform cross domain correlation with alarm correlation built-in algorithms from Network , Systems and other domain events as well as KPI patterns, also correlation should not be limited to only parent-child or service mapping relationships		
8	The operator should be able to build correlation rules in a simple GUI based environment where the Operator should be able to correlate cross domain events		
9	Scalability – The system should be capable of supporting at least 15 thousand network flow per second on single server with capability to capture each unique traffic conversations		
10	The solution shall provide future scalability of the whole system without major architectural changes.		
11	The Solution shall be distributed, scalable, and multi-platform and open to third party integration such as Cloud, Virtualization, Database, Web Server, Application Server platforms etc.		

12	The monitoring module of proposed solution must not use any third party database (including RDBMS and open source) to store data in order to provide full flexibility and control on collected data as well as avoiding tempering with SLA calculations		
13	All the required modules should be from same OEM and should be tightly integrated for single pane of glass view of enterprise monitoring		
14	The OEM of the proposed EMS solution should be a "Make In India" company with 100% local content.		
15	The OEM of the proposed EMS solution should have presence of min. 10 years in the market and the solution should be deployed in min. 5 smart city projects in India. The documentary proof should be submitted at time of the bid submission.		
16	The solution and it's data store should be virtual appliance and deployable on Linux operating systems to reduce the overall TCO.		
DETAILED SPECIFICATIONS: EMS			
	Consolidated Dashboard		
1	The platform must provide complete cross-domain visibility of IT infrastructure issues		
2	The platform must consolidate monitoring events from across layers such as Network, Server, Application, Database etc		
3	The solution should support single console for automated discovery of enterprise network components e.g. network device, servers, virtualization, cloud, application and databases		
4	The solution must support custom dashboards for different role users such as Management, admin and report users		
5	The solution must allow creating custom data widget to visualize data with user preferences eg. Refresh time, time span, background colour, unit conversion		
6	The solution must support custom query based widget with multiple visualization methods including Chart, Guage, Grid, Top N list etc. to visualize and represent collected data with ease.		
7	The solution must provide compehensive query language to pull and plot complex visualization with multiple arithmatic operator such as top, sum, min, max etc.		
8	The solution must support out of the box data widgets for Metric, Log and network flow data with multiple visualization methods such as gauge, grid, charts, Top N etc.		
9	The solution should provide superior view of infrastructure health across system, networks, application and other IT Infrastructure components into a consolidated, central console		
10	There should be only one dashboard/interface to collected network/server/application/log data after correlation and consolidation across the IT landscape to reduce/correlate number of metrics/alarms		
Network Performance Management			
1	The solution must provide discovery & inventory of heterogeneous physical network devices like Layer-2 & Layer-3 switches, Routers and other IP devices and do mapping of LAN & WAN connectivity with granular visibility up to individual ports level.		
2	The solution must support custom device template to support Generic SNMP devices as well as exptensive support on traffic encryption including SNMP v3 with AES-256 encryption		
3	The NMS should provide very powerful event correlation platform/engine and thus must filter, correlate & process, the events that are created daily from network devices. It should assist in root cause determination and help prevent flooding of non-relevant console messages.		

4	It shall provide Real time network monitoring and Measurement offend-to-end Network performance & availability to define service levels and further improve upon them.		
5	The Network performance operator console should provide operators with seamless transitions from fault data to performance data. For example - select a NMS fault event and fault drill down must also provide historical, near real time and correlated data without switching the page		
6	The solution should have the ability to do "baseline" performance metrics and determine normal operating values and patterns by self-learning algorithms on a day, week, month, etc. and ability to configure threshold on these values. The solution should also have built in algorithms to start the monitoring with zero threshold configurations		
7	The proposed system should be able to auto-calculate resource utilization baselines for the entire managed systems and networks and allow user choose algorithms that is more relevant to specific KPI in case of false positive		
8	The agents should be extensible and customizable allowing incorporation of any required monitoring source not included in the out-of-the-box monitoring policies. With capabilities to collect and analyze performance data from the operating system and installed applications and use historical patterns to establish performance baselines.		
9	All baseline thresholds should have lower bound, higher bound, polarity, deviation set point and reset point for ease of use.		
10	System should have anomalies detection, outlier detection and stop alarm flooding with these dynamic thresholds.		
11	The solution should be capable of performing prediction- based anomaly detection to identify unusual or unexpected events and measurements within the monitored environment.		
12	The Solution should provide AI and ML capabilities to help in preventing of Network problems before they occur The Solution should include unsupervised learning module to gather realtime network data and which learns the behavior of devices, applications, and users on the network It should be capable to bring together and correlate network and application data to predict anomaly and performance issues		
13	The solution must provide agentless and agent based method for managing the nodes and have the capability of storing events / data locally if communication to the management server is not possible due to some problem. This capability will help to avoid losing critical events.		
14	The NMS admin consol must provide the ability to start, stop and restart the agent on target server infrastructure and the agent should provide collection capabilities not limited to just KPIs but also support collecting raw logs as well as packets.		
15	The proposed EMS solution must provide agentless as well as agent based monitoring for server infrastructure. The agents should be able to set polling interval as low as 1 second with low overhead on target server infrastructure.		
16	The proposed solution should include a distributed search engine data-store to ingest various types of textual, numerical, geospatial, structured and unstructured data.		
17	The NMS admin console must provide operators with seamless automation to extract fields from collected logs via drag and drop functionality to avoid log parsing complexity of collected logs from various syslog/ windows/ application sources.		
18	It shall provide Real time network monitoring and Measurement offend-to-end Network performance & availability to define service levels and further improve upon them.		

19	The EMS solution shall keep historical rate and protocol data for a minimum of 30 days (most recent) in its short term operating database. All data in that database shall have a maximum 1- minute window granularity. User shall be able to select any 1-minute window over the last 30 days and display unique utilization and protocol data for every monitored interface		
20	The proposed solution should be able to take back up of running and startup configuration of network devices. It should also provide versioning for backup to track changes.		
Fault Management			
1	The proposed solution must should provide out of the box root cause analysis with multiple root cause algorithms inbuilt for root cause analysis. It should also have a strong event correlation engine which can correlate the events on the basis of event pairing, event sequencing etc.		
2	The Platform must include an event correlation automatically fed with events originating from managed elements, monitoring tools or data sources external to the platform. This correlation must perform event filtering, event suppression, event aggregation and event annotation		
3	The proposed solution should provide alert console with alert summary such as no. of correlated alert, network alert, server alert, virtualization alert, cloud alert, applcation alert etc.		
4	The system must have provistion to overlay alert on reported metric to understand alert triggering behaviour across mutiple drill down pages		
5	The proposed solution should have drill-down and correlation page to correlate cross domain historical data points and result should be exported as image and tabular format.		
6	The proposed solution should provide out of the box root cause analysis with multiple root cause algorithms inbuilt for root cause analysis. It should also have a strong event correlation engine which can correlate the events on the basis of event pairing, event sequencing etc.		
7	Powerful correlation capabilities to reduce number of actionable events. Topology based and event stream based correlation should be made available.		
8	The solution must offer relevant remedy tools, graphs in context of a selected fault alarm/event		
9	The proposed monitoring solution should have capability to configure actions based rules for set of pre-defined alarms/alerts enabling automation of set tasks.		
10	The Platform must support Event or Alarm Correlation integrations with service desk to trigger automated creation of incidents, problems management		
11	The solution should classify events based on business impact and also allow defining custom severity levels and priority metrics such as Ok, Critical, Major, Down, Info etc with color codes		
12	The solution should allow creation of correlation or analytics rules for administrators		
13	The proposed solution must provide default event dashboard to identify, accept and assign generated alarms		
Log Management			
1	The proposed solution must provide a common classification of event irrespective of the log format		
2	The proposed solution must provide the ability to store/ retain both normalized and the original raw format of the event log as for forensic purposes for the period of 3 months and allow to extend it to further with additional hardware without any disruption to the ongoing data collection		

3	The proposed solution should provide a minimum log compression of 8:1 for ensuring log compression to reduce overall log index storage space for the raw log format		
4	The log data generated should be stored in a centralized server. The period upto which the data must be available should be customizable.		
5	The proposed solution must support logs collected from commercial and proprietary applications. For assets not natively supported, the solution should provide the collection of events through customization of connectors or similar integration		
6	The proposed solution must support log collection for Directories (i.e. AD, LDAP), hosted applications such as database, web server, file integrity logs etc. using agents		
7	The Log receiver or log collection component must store the data locally if communication with centralized collector/receiver is unavailable.		
8	The proposed solution must support log collection from Network infrastructure (i.e. switches, routers, etc.). Please describe the level of support for this type of product.		
9	The system shall support the following log formats for log collection: Windows Event Log, Syslog, Access Log Data, Application Log data, Any Custom Log data, Text Log (flat file), JSON Data		
10	The collection devices should support collection of logs through Syslog, syslogNG and also provide native Windows Agents as well as Agentless(PowerShell) connectors		
11	The proposed solution must provide alerting based upon established policy		
12	The proposed solution must provide SDK and Rest API to write custom connectors and collectors to pull log and monitoring data from third party system		
13	The proposed solution must provide UI based wizard and capabilities to minimize false positives and deliver accurate results.		
14	The proposed solution must collect, index the log messages and support full-text searching for forensic investigation		
15	The proposed solution must support the ability to take action upon receiving an alert. For example, the solution should support the ability to initiate a script or send an email message.		
16	The solution must provide pre-defined log correlation rules to detect suspicious behavior		
17	The solution must support real-time and scheduled alerting time-line while creating a log policy to catch specific log pattern		
18	The solution should support applying regex pattern in real-time to extract vendor specific log data for reporting and alerting purpose		
19	The system shall have the capability to drag and drop building of custom search queries & reports		
20	The system shall be capable of operating at a sustained 5000 EPS per collection instance. The system shall provide the ability to scale to higher event rates by adding multiple collection instance		
Network Flow-based Traffic Analysis			
1	The proposed traffic monitoring system must be able to track all network flow (including netflow v1-v9, Jflow, Sflow and IPFix) of traffic on the network and identify malicious behavior with all IP conversations.		
2	The proposed system must provide details of applications, hosts, and conversations consuming WAN bandwidth to isolate and resolve problems.		
3	The proposed system must provide baseline network flow policy to detect anomaly in traffic usage behaviour		

4	The solution must provide flow data expolrer with capability to analyze extacted data using multiple columns , chart type, group by operators and filters. System must also provide dashboard to flow data explorer drill down capability.		
5	The proposed solution must be able to monitor and report on a variety of unique protocols (used in the overall deployed solutions) per day and display utilization data for each protocol individually. This capability must be available for each monitored interface uniquely.		
6	The proposed solution must keep historical rate and ip to ip, ip to protocol, protocol to protocol conversation data for a minimum of 3 months (most recent) in its current long term operating database. All data in that database must have a maximum 15 minute window granularity.		
7	The proposed solution should include a distributed search engine data-store to ingest various types of textual, numerical, geospatial, structured and unstructured data.		
8	Should support use of policies that can detect violations based on blacklist/whitelist matches.		
9	The proposed solution must keep historical rate and protocol data for a minimum of 60 days (most recent) in its short term operating database. All data in that database must have a maximum 1 minute window granularity with option change retention period		
10	The system must support the ability to create reports that allow the user to search all IP traffic over a specified historical period, for a variety of conditions. o Search for any traffic using a specific configurable destination port, or port range. o Search for any protocol in use by a specific host, interface or list of hosts or interfaces.		
Service Desk - Incident Management			
1	The proposed helpdesk system shall provide flexibility of logging, viewing, updating and closing incident manually via web interface		
2	The proposed helpdesk solution should have achieved PinkVERIFY certification on at least 6 available ITIL processes such as Incident Management, Request Management, Problem Management, Change Management, Availability Management and Event Management (Documentary proof should be provided at the time of bidding).		
3	Each incident shall be able to associate multiple activity logs entries via manual update or automatic update from other enterprise management tools.		
4	The proposed helpdesk system shall be able to provide flexibility of incident assignment based on the workload, category, location etc.		
5	The proposed solution should automatically provide suggested knowledge base articles based on Incident properties with no programming		
6	The proposed solution should automatically suggest available technicians based on workload, average ticket closure time assigning tickets with no programming		
7	The proposed solution should tightly integrate with monitoring system to provide two way integration - E.g. when system down alarm created, it should automatically create ticket and assign it to technician, in case system comes up before ticket is resolved by technician, it should automatically close the ticket to minimize human efforts		
8	The proposed system must not create more than one ticket for same recurring alarm to avoid ticket flooding from Monitoring system		
9	The proposed solution should allow administrator to define ticket dispatcher workflow which automatically assign incoming tickets based on rules defined in workflow. E.g. Network fault keyword tickets gets assigned to network technician automatically within NOC team		

10	The proposed helpdesk system shall provide grouping access on different security knowledge articles for different group of users.		
11	The proposed helpdesk system shall have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues		
12	The proposed solution should allow Technician to relate Incidents to Problem, Change and vice versa to have better context while working on any of ticket type		
13	The proposed helpdesk system shall support tracking of SLA (service level agreements) for call requests within the help desk through service types.		
14	The proposed helpdesk system shall integrate tightly with the Knowledge tools and CMDB and shall be accessible from the same login window		
15	The proposed helpdesk solution should be equipped with chatbot functionality for identifying the intent of the query and provide an accurate answer and suggest options to confirm or resolve the issue.		
16	The chatbot should have NLP functions (Natural Language Processing) to analyze the context of the query.		
17	Proposed solution should not be dependent on any third party NLP algorithm. It should be inbuilt in the product.		
18	Proposed helpdesk should have support of inbuilt conversational AI.		
19	Proposed helpdesk should support custom theme option including color scheme of GUI, Fonts and custom logo placement.		
Asset Inventory Management			
1	A configuration management database shall be established which stores unique information about each type Configuration Item CI or group of CI.		
2	The proposed solution allow scheduling periodic report to check current software and hardware inventory		
3	The proposed solution must allow attaching CI record to generated service tickets		
4	The Proposed solution should provide end to end Asset Life Cycle Management: Makes it easier to handle the complete life cycle of an asset, that is, all stages/modules from procurement to disposal		
5	The Proposed solution should support maintaining AMC/Warranty Information with Alerting when about to expire also provide Asset Deletion capabilities enabled with workflow engine		
6	The Proposed solution should support Software License Metering: Helps to understand the software license compliance and the use of unauthorized software in the organization and helps to act proactively to curb illegal usage and problems associated with it.		
7	The proposed solution should provide Asset Dashboards/Reporting: Graphical representation all the assets based on Category, location, aging of the asset, customer, which can be further level down to the incident record ID		
8	The proposed solution should provide out of the box purchase and contract management modules to support end to end asset life cycle		
9	The proposed solution must provide asset baselining to manage and track asset effectively.		
Project Management			
1	A project management tool should have a clean, intuitive, and user-friendly interface that allows users to easily navigate the software and access the features they need.		
2	The tool should allow for easy creation and management of project plans, including tasks, timelines, milestones, and dependencies. It should also allow for real-time tracking of progress against the project plan.		

3	The tool should enable team members to communicate, collaborate, and share project information in real-time.		
4	The tool should allow users to create, assign, and track tasks, as well as set deadlines, priorities, and reminders.		
5	Project scheduling: The tool should provide the ability to create and manage project schedules, including milestones, deadlines, and dependencies.		
6	Resource management: The tool should enable users to allocate and manage resources, including people, materials, and equipment.		
7	Budget tracking: The tool should enable users to create and manage project budgets, track expenses, and monitor financial performance.		
8	Reporting and analytics: The tool should provide users with reports and analytics that enable them to monitor progress, identify bottlenecks, and make informed decisions.		
9	The tool should have robust security features and access controls that protect project data and ensure that only authorized users can access sensitive information.		
10	Integration with other software: The tool should integrate seamlessly with other software, such as accounting or CRM systems, to streamline workflows and improve efficiency.		
11	The tool should be scalable and flexible to accommodate the needs of small or large teams, and customizable to fit the specific requirements of different projects and industries.		
12	The proposed solution must allow attaching CI record to generated service tickets		
13	The Proposed solution should provide end to end Asset Life Cycle Management: Makes it easier to handle the complete life cycle of an asset, that is, all stages/modules from procurement to disposal		
14	The Proposed solution should support maintaining AMC/Warranty Information with Alerting when about to expire also provide Asset Deletion capabilities enabled with workflow engine		
15	The Proposed solution should support Software License Metering: Helps to understand the software license compliance and the use of unauthorized software in the organization and helps to act proactively to curb illegal usage and problems associated with it.		
16	The proposed solution should provide Asset Dashboards/Reporting: Graphical representation all the assets based on Category, location, aging of the asset, customer, which can be further level down to the incident record ID		
18	The proposed solution should provide out of the box purchase and contract management modules to support end to end asset life cycle		
	Service Level Reporting:		
1	The solution should provide reports that can prove IT service quality levels, such as application response times and server resource consumption		
2	The system reports should be accessible via web browser and Reports can be published in PDF and csv format		
3	The solution most have an integrated dashboard, view of Contract Parties & current SLA delivery levels and view of Services & current SLA performance		
4	The solution must provide Reports that can be scheduled to publish automatically, or they can be produced on demand		
5	The solution should be able to report in the context of the business services that the infrastructure elements support— clearly showing how the infrastructure impacts business service levels		

6	The solution should provide Business Service Management functionality to track Service quality by logically grouping Network, Server, and Application components. The solution should provide correlation between Network, Server, and Application to identify the business impact from the specific event or alarm		
7	The solution must provide way to define key performance indicators (KPIs) within the Service Quality report.		
8	The solution must provide SLA measurement to track service quality from both Availability and Performance perspective.		
	EMS Other Key Requirements:-		
1	Proposed NMS solution must have deployment reference in Smart city for monitoring & managing network nodes in at least 5 Smart City Projects.		
2	The Solution should provide all the modules as a single monitoring engine to correlate events in real-time from Networks, Servers, and Applications		
3	The solution should be virtual appliance and deployable on Linux operating systems to reduce the overall TCO		
4	The proposed OEM should possess ISO 27034 Certification for Application Security Management. Documentary proof must be provided at the time of submission.		
5	The proposed Network Monitoring Solution, Help Desk and Asset Management module should be from a single OEM.		

5.12 VIDEOWALL

Command Centre - Video Wall – Techno-Functional Spec				
Sl. No.	**Parameters**	**Minimum Specifications**	**Technical Compliance (Yes/No)**	**Remark**
1	Configuration	Video Wall cubes of 70"(± 5 %) diagonal in a 5(C) x 2(R) configuration complete with base stand with Unique cooling system ensures longer LED/ LASER lifetime		
2	Cube &Controller	Cube & controller, Software should be from the Same OEM		
3	Native Resolution	Full HD (1920x 1080) DLP Single chip/DLP LED/ LASER Technology or higher		
4	Technology	LED/ LASER Lit DLP Rear Projection Technology without any colour wheel		
5	Light Source	LED/ LASER light source with a minimum life time of 1,00,000 hrs. in Normal Mode; Individual cube should be equipped with multiple LED/ LASER banks and each LED/ LASER bank should have an array of diodes. Single or multiple diode failure should not impact image display on the screen		
6	Display Technology	DLP Rear Projection with 4K@60Hz minimum resolution supported		

7	Brightness on Screen	Minimum 500 cd/m2 and should be adjustable for lower or even higher brightness requirements		
8	Brightness Uniformity	>95% (ANSI 9points) complete separation of image signal processing versus color and brightness uniformity correction		
9	**Color**	Should provide auto color adjustment function and should be sensor based,		
		automatic calibration system which works with an advanced color sensor. The sensor continuously measures the primary levels of the entire wall and adjusts white point and color when needed.		
		Color and brightness sensor should be in- built inside the projector only Placing sensors outside the projector and projector body is not acceptable		
10	Screen	180° viewing angle		
11	Dynamic Contrast	500000:1 or more		
		System must be modular in installation; Dark box type stacking model is not acceptable		
12	Heat dissipation	Less than 650 BTU / h, with noise < 20 dB(A) one module at 5m distance in front		
13	Control	IP Based control ; old IR based control should not be acceptable		
14	Remote	IP based control should also be provided for quick access; old IR based control should not be acceptable		
15	Screen to Screen Gap	Less than 0.5 mm Gap between 2 screens		
16	Terminal in each Cube	2x Input (DP1.2) 2x Input (HDMI2.0) 2x LAN 2x USB 1x Output (DP1.2)		
17	Power Consumption in Full Bright	Power Consumption for each VDU/Rear		
		Projection Modules should be less than 180 Watts		
18	Power Supply	100 – 240 VAC, 50-60Hz; Option to have Redundant Power Supply in each cube		
19	Input Frequency	24 – 62 Hz		
20	Genlock	49 – 61 Hz		
21	Cooling Inside Cube	Any advanced cooling mechanism		

22	Light Source	Individual cube should be equipped with multiple LED/ LASER diodes. Lifetime of Light source in Eco Mode: 1,00,000 Hrs. Lifetime of Light source in Normal Mode: 1,00,000 Hrs Light source should redundant for each of 3x LED Banks / LASER Banks		
23	Maintenance Access	Cube should be accessible from the rear side for maintenance only		
24	Cube control & Monitoring	Video wall should be equipped with a cube control & monitoring system. It should provide options to view control layouts on remote devices such as tab, laptop, etc through web browsers		
		Should be able to control & monitor individual cube, multiple cubes and multiple video walls		
		Should provide a virtual remote GUI over the IP to control the video wall		
		Status log file should be downloadable as per user convenience		
		System should be AI (Artificial Intelligence) and non-AI based advance proactive with Advance Pro-active real- time Monitoring and Diagnosis of hardware over cloud for predictive failure to have maximum uptime.		
25	Sharing & Collaboration	It should be possible to share the layouts over LAN/WAN Network with Display in Meeting room or on Remote Workstations connected on LAN/WAN Network		
26	Processor	Octa Core, 2.1 GHz or higher end processor, RAM- Minimum 32 GB expandable to 64 GB		

5.13 IP PBX System

Technical Specifications for IP PBX System (Latest Server - Media Gateway Architecture) System				
Sl. No.	**Technical Parameters**	**Technical Description**	**Technical Compliance (Yes/No)**	**Remark**
1	**Configuration & Architecture:**			

	IP Telephony System Architecture	The IP telephony system must be based on a pure IP technology that is a software-only solution.		
		The IP telephony system must support unified communication (UC) server & gateways architecture for SIP, Digital and Analog trunks connectivity.		
		The system must be capable of supporting Analog, Digital & IP Telephones, and SIP based video desk phones.		
		IP User License for 50% additional ports to be provided than current requirement from Day 1. The system should have future expansion capacity to expand up to 20000 ports.		
		The Communication servers must be Commercial of the shelf Servers (COTS) & work in an Active-Active redundancy mode. It should be possible to define servers load balancing mode. The solution with embedded server / appliance Server or with standalone traditional / hybrid traditional PCM/TDM EPABX type gateways will not be acceptable.		
		The communication servers must work in an Active-Active redundancy mode. It should be possible to define servers load balancing mode. Both servers should work together in load balancing mode with defined user capacity i.e., all servers should be active with call processing with predefined SIP phones / gateways register on any of the server for load distribution. If any Server Fails in the Cluster adjacent server should automatically take the load of the failed sever along with load of gateway and end points without breaking on-going calls. Redundant Server/Hot stand-by mode of working is not acceptable.		
		The proposed solution should have to be a robust on the latest platform of Server-Gateway technology with a distributed architecture which must be a state of the art system being used as per latest Telecom standards. The proposed system should have 2 no's of Servers to be located in geo-redundancy mode, Both the Servers should be in one Cluster.		
		Both the servers must be provided in a cluster mode. If one cluster server fails, one of the other cluster servers in the network must be able to take the complete load of the calls automatically (without any manual intervention) and without dropping any existing calls (IP,TDM & PRI) or data (CDR, CTI). Management of all servers in cluster should be from same web page. All servers should have same database.		
		The OEM offered unified communication and call manager application must have valid trademark registration certificate as per Govt. of India trademark act 1999, Section 23, rule No. 62(1). Vendor to submit a copy of the same certified by respective exchange OEM.		
		The telephony system must be able to register SIP phones/SIP video phones and MGCP phones directly to it.		

		System should work on Geographically distributed Architecture		
		It should be possible to install Telephony system in VMware EXSi 5.5 or higher.		
		All Data (Numbers, COS, Routing, Applications) should reside in all the Servers		
		Database replication in All servers should be automatic and real time		
		Should support N+1 Redundancy Architecture as well as 1+1 redundancy Architecture		
		Should support Remote Survival Nodes		
		In case of failure of one server, the SIP Phones, SIP Gateways, MGCP Phones should register with second Server automatically		
		System Diagnostics should be done in Server		
		Hot Standby for SIP Phones and Gateways i.e., SIP Phones and Gateways should register automatically to next available telephony server.		
		COTS - commercial off-the-shelf Servers should be used for telephony system. OEM made or proprietary made servers will not be accepted.		
		Telephony system should use Linux Operating System		
		System should support CSTA phase III Protocol		
		Full continuation for call signalling and media must be supported		
		Calls must not be disconnected and control must remain throughout the swap to an alternate server including full call control (transfer, conference actions, continuation of CDR data for the existing call).		
		Load Balancing of end points must be possible by the administrator		
		There must be no restriction on the number of endpoints being backed up in case of one server failure.		
		UC platform servers must provide full failover and redundancy		
		Vendor must submit valid latest Type test TEC-GR (**Vide TEC-GR spec. No.: TEC/GR/SW/PBX-005/01/SEP.2016**) (Generic Requirement) approval certificate issued by Telecommunication Engineering Centre (TEC), Department of Telecommunication, Govt. of India tested with IPv4 & IPv6 for both SIP terminals and SIP Trunks from days 1 for the particular model of IP-PBX with Server & Media Gateway system quoted. Notarized copy of the same is required to submit along with the technical bid.		
		Hardware of the offered IP Telephony Exchange of server – Gateway architecture with redundancy system should be from OEM, Hardware of Chinese/ ROC (Republic of China)/Countries taking ant India movements are not allowed quote as per Land border sharing policy of Govt. of India. IP telephony system UC Software, IP/SIP Phones,		

		Analog Media Gateways, Call Billing and accounting software, Emergency conference communication, Help Desk and voice mail must be from the same OEM of IP Telephony Exchange. No Third party solution is allowed.		
		The Bidder to demonstrate complete system as Proof of Concept/Explain over presentation to GSCL technical team of all the above criteria for Technical qualification after Opening of the technical Bid. Each and every feature mentioned in technical specs to be demonstrated. Failing which bid will be summarily rejected. The cost of POC /Demo will be responsibility of bidder.		
	System should support the following SIP RFCs:	RFC 3261 (SIP: Session Initiation Protocol)		
		RFC 3262 (Reliability of Provisional Responses in Session Initiation Protocol)		
		RFC 3263 (Locating SIP Servers)		
		RFC 3264 (An Offer/Answer Model with Session Description Protocol (SDP))		
		RFC 3265 (Specific Event Notification)		
		RFC 2327 (SDP- Session Description Protocol)		
		RFC 1889 and 1890 (RTP/RTCP)		
		RFC 3515 (REFER)		
		RFC 2833 (DTMF over IP)		
	Scalability	It should be possible to add more sites and users without the need to change the software and existing configuration.		
		The system UC Software must be scalable to at least 20,000 endpoints in single cluster architecture. Proof of reference document to be submitted by OEM on their letter head.		
		Also Call Manager system must support unlimited SIP trunks within the same application within the same server. The system must be modular, scalable and distributable.		
		The IP PBX system must be tested ready with both IPv4 & IPv6 as per Govt. of India guidelines dtd. January 2020. Test certificate issued from TEC to be submitted along with a technical bid. Self-declaration by bidder/OEM will not be accepted.		
		The call signalling server must handle at a minimum of 100K BHCC.		
		The system must be modular, scalable and distributable		
	System Survivability	The UC platform must consist of one or many servers where each server in the cluster provides complete 100% application functionality.		
		In case of a failed server, all endpoints registered with that server need to register instantly with a different server in the cluster with no interruption to on-going calls.		
		Media Gateways must have survival mechanisms that allow them to maintain 100% of the telephony services for their users in case of failure in the WAN links when the signalling with the call server drops.		

		The life cycle of the entire system being provided must be at least Ten (10) years.		
		The system gateway must be able to restart automatically without human intervention when the external AC power supply is resumed after complete power failure (even after the batteries are discharged).		
		The telephony system must be capable of providing 99.999% availability.		
	Distributed Architecture	The UC platform must have distributed architecture and centralized control for all the sites in the network.		
		The proposed solution must support Hybrid cloud solution in order to guarantee business continuity with overall survivability regardless of a failure at any single location.		
		The proposed solution must enable part of the cluster to be hosted in a Cloud Service Provider (CSP) to run all applications.		
		The proposed solution must have built in redundancy using a cloud solution to provide automatic disaster recovery option.		
		The proposed solution should have provision to be installed using an image of the application an easily implemented on the Cloud Service Provider servers.		
	Quality of Service (QOS)	The voice and signalling frames must be marked [tagged] in order to be recognized.		
	Server – Physical Attributes	COTS – Commercial Off-the-Shelf servers must be used.		
		The redundant server must have separate hardware, not sharing elements like hard drives and RAM etc., to avoid a single point of failure.		
		The server should have AC power supply.		
		The system must be based on server gateway architecture with external appliance servers		
		No card based processor systems / soft switch should be quoted.		
		The call processor must run on Linux OS.		
	Minimum Server Specifications:	The CPU must be minimum 4 core processor		
		The server must have at least 16GB RAM		
		The server must have Hard Drives (1TB each) of storage		
		The server must have a Dual 1GB network interface.		
		Form Factor for physical server (Not Virtual Machine) should be 1 U		
		Should be Compatible to work with VMware EXSi 6.5 or higher		
	System Security	Administration of the system should be using HTTPS		
		It should support the Interop with leading SBC		
		System should use TLS (Transport Layer protocol) to encrypt SIP, HTTP, FTP and SRTP (Secure Real-time Transport Protocol) and SRTCP to encrypt RTP and RTCP		
		System Audit Logs for 30 days		

		Certificate management		
		System should have auto Provisioning profiles contain pre-configured sets of features that must automatically polls and updates registered phones with the latest phone firmware and configuration files.		
	Mobility	The system should have Call Back feature. If the user dials his own extension from predefined number (mobile/landline) then system should disconnect the call and then system should call the user to provide the dialtone so that user can make intercom or PSTN calls.		
		The system should have Call Through feature. If the user dials his own extension from predefined number then system should provide dialtone to make intercom or o/g calls.		
		The system should have one number (Forking, reach-me-anywhere) feature. Users should be able to receive calls on any of their phones, from almost anywhere. An incoming call rings on all or specific phones until the user answers the call. The user can transfer the call, establish a conference, and so on, whether the answering device is an internal device, an external phone, or a cellular handset. If the answering phone is an external device, the call automatically becomes an authorized mobility call.		
		The system should support SIP Client on smart phone for Android as well as for iOS.		
	SIP Endpoints	All SIP phones must support the standard SIP protocol. No proprietary protocols are allowed to be used.		
		SIP phones must support the configuration of programmable buttons with functions such as Break-in, Conference call, Deflect, silent monitoring and more.		
		SIP phones must work in conjugation with the following applications:		
		1. Contact Centre (Agents Phones)		
		2. Attendant Console		
		3. Managed Audio Conferencing		
		4. Managed Video Conferencing		
		5. UC clients		
	Automatic Call Distribution (ACD)	Busy ACD Group announcement		
		Hunt Group Release		
		IVR-ACD		
		Log In / Log Out		
		Multiple Announcements:		
		1. Mandatory announcement - All incoming callers to an ACD/HUNT group must be able to hear an introductory announcement in its entirety usually explaining about the company, product, or campaign.		
		2. First announcement - If all agents are busy, callers must be able to hear this announcement once usually informing		

		them that their call has been placed in queue. (The system must be able to cut short this announcement if an agent becomes available to attend to the caller.)		
		3. Music - If no agents are available after the first announcement (or no First and Periodic announcers have been configured), the caller must be able to hear background music while in queue.		
		4. Periodic announcement - Alternating with background music, these announcements can also be played to callers in queue according to the Periodic Announcement Interval (see above) until the ACD/HUNT call is answered.		
		Release / Resume		
		Wait Queue		
		Wrap-Up Time		
		Automatic Release of ACD Agent		
		Automatic Call Distribution (ACD) Extended Overflow		
	Zone Page	A phone user must be able to simultaneously broadcast a message over all types of endpoints.		
		The maximum quantity of endpoints in one zone should not be less than 100.		
	System Administration	System administration should be web based.		
		All programming of system should be done through a web-based GUI interface.		
		The administrator should have Dynamic Profiles.		
		The system should allow for complete multi-level administration. The administrator must be able to define at least five (5) different administration level profiles that can be applied to allow subsets of users to access and manage particular pages in the systems Web Portal		
	Certification Requirements	The OEM must have ISO 9001, ISO 45001, ISO 270001 and ISO 90003 certification in all the company's activities. Duly certified copies of the same is required to be submitted along with technical bid. Non-submission will be considered for technical rejection of bids.		
	System Features	ANI (Caller ID) Restriction		
		ARS (Automatic Route Selection)		
		Auto Attendant		
		Call Forward at Night/Holiday		
		Call Forward Destinations		
		Call Forward for Undefined Stations		
		Call Forward on Busy		
		Call Forward on DND (Do Not Disturb)		
		Call Forward on Logout		
		Call Forward on No Answer		
		Caller id based routing for individual extension		
		Deflect (Divert) Call		

		Digit Train Conversion		
		Direct-In-Dial		
		Direct-In-Line (DIL)		
		Hot Line		
		Interactive Voice Response (IVR)		
		Least Cost Routing		
		Look Ahead Routing (LAR)		
		Numbering Plan		
		Personal Routing Rules based on caller id and DNIS		
		Predetermined Night Answer		
		Toll Restriction – Digit Analysis		
		Toll Restriction – Trunk Groups		
		Trunk to Trunk Connection		
		Trunk Transfer Restriction		
		Classes of Service		
		Night Answer Central Bell / UNA Pickup		
		Page Queue		
		Recall		
		Recall / Incomplete Destination		
		Second Ring back Tone		
		Speed Dial Public (System) and Private		
		Virtual Numbers		
		Music On Hold		
		each User should support up to 6 devices i.e., SIP phone / analog phone / soft phone / mobile client etc.		
		Voice Page		
		Silent Monitor		
		Zone Page		
		Barge In		
		Connection to MS Teams using SBC		
		Wake up		
	Extension Features	Answer Call Waiting by Transfer		
		Auto Set Relocate		
		Auto-Answer		
		Automatic Disconnect		
		Automatic Number Identification (ANI) Display		
		Browse Personal Directory		
		Busy Lamp Field		
		Call Forward All		
		Call Hold		
		Call Log		

		Call Parking and Call Pickup		
		Call Waiting		
		Caller ID Control		
		Caller-ID Screening		
		Caller id based routing for individual extension		
		Calling Number and Name		
		Camp-on Idle		
		Configurable DSS Buttons		
		Direct Dial without Off Hook (Hands Free)		
		Directed Call Pickup		
		Display Automatic Number Identification (ANI)		
		Display Dialled Number and Name		
		Display Dynamic Call Divert Information		
		Display Select Hold Display		
		Display Time/Date Function		
		Do Not Disturb (DND)		
		DSS/BLF		
		Elapsed Time Display		
		Group Call Pickup		
		Hands Free		
		Hands-Free Announce and Reply (Idle State)		
		Last Number Redial		
		Login and Logout		
		Message Waiting Indication		
		Multi Appearance (Call Waiting)		
		Multiple Line Appearance		
		On-Hook Dialing		
		Placing Multiple Calls on Hold		
		Privacy – ANI Restriction		
		Reminder/wakeup Call		
		Restrictions – Station		
		System Non-Exclusive Hold		
		Transfer with Consultation		
		Transfer without Consultation (Blind)		
		Voice Page		
		Emergency Preemption		
		Listen to Paging while in a call (Busy Condition)		
		ULA - User Line Appearance (ULA)		
	Emergency Response conference	The Emergency communication solution must be embedded within the platform, not installed on a separate server and should be from the same OEM of the telephony		

	communication System	system. It should have the facility to automatic dial out to connect up to 120 participants in a single conference. System should also have 120 party managed meet me conference. It should be possible to further divide 120 party conference bridge into any combination like 10 X 10 party, 5 x 20 party etc. if required. The meet me conference should be secured means to enter to the conference bridge; the user should enter the password.		
		The emergency communication management should be from Web Browser/HTML5 based GUI based interface from Windows PC and Touchscreen Devices.		
		If SIP camera is connected on same LAN network, it should have the ability to view the video (of the location) from a camera to the Dispatcher screen and create an alarm.		
		It should have the ability to view video using streaming with HTML5.		
		It should have the ability to view video using Adobe Flash Player		
		The Group Operator should have following features as below:		
		1. The Group Operator must be able to add / remove members		
		2. The Group Operator must be able to add other conference members		
		3. The Group Operator must be able to mute / unmute (User, None, All)		
		4. The Group Operator must be able to lock / unlock the conference		
		5. The Group Operator must be able to close the conference		
		6. It must be possible to dial out a pre-defined group (or multi-groups) of participants/numbers by simply pressing the pre-assigned key.		
		7. Each pre-set conference must have its own unique dial number such that when this group number is dialled; all the number stations will ring simultaneously.		
		8. Any combination of stations and external numbers must be able to be defined as members of the Group Call.		
		9. Participants may join a conference in the audible or in the mute mode, if in mute mode, the right to speak must be selectively offered to attendees per their request by a special signal sent to the Group Operator by the attendees.		
		10. Attendees must be able to be added or excluded at any time by the Group Operator		
		11. The conference must be terminated when the Group Operator leaves (auto terminate if all members left are muted).		
		12. The Group Operator must be able to barge into an existing user call based on pre-emption predefined rules.		

		13. Group operator must support two SIP phones so that if one phone is busy in conference, the second phone can be used to add participants.		
		14. Both group operator SIP phones should be controlled by web based conference management GUI for telephony feature like answer, hold, transfer etc. if required in future.		
		15. The same Group operator should also function as operator console		
		16. Mute Ring Button – When a call comes to the Dispatcher phone, the Dispatcher can mute the ring, The call will continue.		
		17. Add Department attribute to user – In the Phone Book, add a department name for the user. The Dispatcher can do a search based on the Department		
		18. Configurable Background – Change the background of the Dispatcher screen from the Application		
		19. Join Incoming Calls to an open Conference – When a call arrives to the Dispatcher, he can add that call to an open conference		
		20. Stage Conference from the Dispatcher screen – the Dispatcher can create an ad-hoc conference from the Dispatcher screen.		
		21. Change Meet me Access Code – The password of a conference can be changed by the Dispatcher to block or allow callers to join a conference		
	Contact Centre Specification	**1.1 General capabilities**		
		1.1.1 The proposed solution must be embedded within the platform, not installed on a separate server and should be from the same OEM of the telephony system.		
		1.1.2 The system must be an All-in-one solution that provides solution for UC&C. Bidder should supply 5 agent licence, one supervisor and 5 port IVR for help desk.		
		1.1.3 Single server deployment with intuitive and central management capabilities should support true multimedia.		
		1.1.4 Help desk managers must be able to easily prioritize customers and incoming contacts regardless of the media used.		
		1.1.5 The same set of business and routing rules can be applied to voice / chat calls, emails, and faxes if required.		
		1.1.6 The help desk must support multi-layer routing including Priority, Skill Based, Statistical, Business Rules, and Customer Defined Values.		
		1.1.7 Help desk must have embedded IVR, enabling managers to design routing plans and accurately assess help desk activity trends.		
		1.1.8 The IVR application must be a GUI application that can be managed by the customer.		
		1.1.9 The customer must have the ability to build new self-services applications like new IVR flow for new service.		

		1.1.10 Customer must have the ability to define/change routing rules by himself based on customer's profile.		
		1.1.11 The help desk must support Outbound, Call-back and Campaigns – including preview, progressive and automated outbound dialling.		
		1.1.12 The supervisor must be able to see the status of help desk agents in real-time in his PC like logout, busy, free, release, non ACD etc. in graphical form in pie chart / bar chart.		
		1.2 **Contact Centre facilities**		
		1.2.1 Real-time Monitoring – must provide supervisors with statistical information about the current status of the help desk with on line refresh (1sec). The application must include pre-defined list of reports and the customer (end user) should be able to choose reports as needed.		
		1.2.2 The Real Time application must provide the ability to build/change the workspace for each user and by user (not vendor or distributor).		
		1.2.3 The RT must provide the ability to move agents to/from different groups/queues for current login only.		
		1.2.4 Historical Reports – must be able to collect all information from call entry to call termination. Call profile details for internal investigation purposes should be part of the contact centre solution.		
		1.2.5 The help desk solution must have an embedded Management Information System (MIS) suite that monitors all help desk activities, generating reports that summarize the past performance of the system over a given time period, and providing statistical analysis of the help desk within a specified period. Real-time and historical reports provide:		
		Help desk agent should be able to do following activities from agent application installed on PC:		
		Login/Logout from group		
		Release/Resume		
		Ready		
		Wrap-up Code		
		Release for Break		
		Release for Meeting		
		Control Wrap Up		
		Supervisor Help		
		Agent Board		
		Answer		
		Hold		
		Retrieve		
		Hang Up		

		Integration Capabilities with Sales Force, Microsoft dynamics, SAP CRM & Oracle & SIEBEL		
		Solution should be integrated with CRM		
	PRI Gateway – 1 Ports	PRI gateway with 1 ports (30 channel) to be provided from same OEM of telephony system.		
		Voice Proxy – RTP voice proxy function for NAT/firewall traversal		
		Fax Relay – T.30 transparent mode, T.38 fax relay		
		Call Handling – configurable dialling plan, up to 500 routing rules		
		Configuration Interface – Web Utility		
		Remote Management – Telnet, HTTP, TR069		
		PSTN – ISDN PRI standard: ANSI, NI-2, DMS, 5ESS		
		SIP – RFC3261, RFC2976, RFC3515, RFC3581		
		DTMF – tone detection generation and detection; DTMF relay: RFC2833, INFO (SIP)		
		DTMF detection and progress tone detection		
		Play ring-back tone		
		T.30 and T.38		
		RTP proxy for NAT traversal		
		Ethernet – RJ-45, 10/100/1000 Base-T		
		Trunking Interface – RJ-45		
		Power Input – Single 230 V AC		
		Operation Humidity – 10% to 90% (non-condensing)		
		Operation Temperature – 0 to 40ºC		
		Traditional EPABX type media Gateways having universal slots will not be accepted. The Media Gateway of mentioned ports capacity must be 19" rack mountable compact & modular in configuration with size must be 2U or less. So that to save space for installation.		
		The proposed Media Gateway should only consist only PRI configuration. Media Gateways with unnecessary additional type of extensions and trunks ports facility should not be accepted.		
		Any accessories like connector, cables etc. should be supplied by the contractor.		
	Voice Logger – 8 Channel	Voice Logger (8 Channel) fully integrated with IP telephony system should be supplied with active recording to record any logical entity like analog phone, Digital phone, SIP phone, analog trunk, digital trunk, SIP trunk, trunk group, conference call etc. without doing parallel tapping of the phone / trunk.		
		Voice logger application should be from the same OEM of IP telephony system. Third party voice logger system should not be quoted.		

		Should allow setting up advance recording rules from telephony system and sending advanced Meta data for recording.		
		Standards based - Should uses SIP and CSTA to connect to IP telephony system. Standard Voice file formats (GSM, PCM etc.) and databases (MS-SQL, My SQL, Oracle etc.)		
		It should enable centralized recording and does not require any port mirroring. Voice logger system with Diagnostics capability should provide a comprehensive monitoring and alarm system, empowering the IT department to detect and manage any abnormalities that may occurs in the Recording System.		
		Search and Display - The voice logger should enable user to access and manage your voice recording files via a client or by using a web browser. It should also support monitoring agent's screen and voice calls in real time.		
	Basic IP Phones	· SIP phone should be from the same OEM of IP telephony system		
		· minimum 128x48-pixel or more graphical LCD with backlight		
		· 2 VoIP accounts		
		· 4 soft keys		
		· 4 Function keys (Phonebook, MWI, Headset, Redial)		
		· Auto provision via FTP/TFTP/HTTP/HTTPS for mass deployment		
		· SRTP/ HTTPS/ TLS, 802.1x		
		· Volume adjustment, ring tone selection, Headset, Wall-Mountable		
		· IPv4 / IPv6		
		· Codec: G.722, G.711, G.726, G.729, G.729A, iLBC,opus		
		· VAD, CNG, PLC, AGC, AEC, RTCP-XR (RFC3611), VQ-RTCPXR (RFC6035)		
		· Full-duplex hands-free speakerphone		
		· SIP (RFC3261)		
		· NAT Traversal: STUN mode or 3rd party SBC		
		· DTMF: In-Band, RFC2833, SIP Info		
		· IP Assignment: Static/DHCP		
		· 1xRJ9 handset port		
		· LED for call and message waiting indication		
		· Dual-port Gigabit Ethernet		
		· Power over Ethernet (IEEE 802.3af), Class 2		

5.14 INDUSTRIAL GRADE SWITCH

Industrial Grade Switch **8 Port Switch**			
SL No	**Minimum Specifications**	**Technical Compliance (Yes/No)**	**Remark**
1	The Switch Should be Industrial grade in nature and should have 8x10/100/1000 Base-T PoE+ ports and 4x100/1000 Base-X SFP ports and to be supplied with required module.		
2	Switch should support maximum PoE Budget of 240watt		
3	The switch should have minimum switching capacity of 24Gbps.		
4	Switch Should support 16K MAC addresses and 4000 VLAN		
5	Switch should support Jumbo frame, ITU-T G.8032, IEEE 802.1ad, IEEE 802.1Q, IEEE 802.1v, IEEE 802.3ac, IEEE 802.1AX, DHCP Server and Relay for IPv4 and IPv6, DHCP Option 82		
6	Switch should support IGMP v1/v2/v3 snooping, MLD v1/v2 snooping with min 512 multicast group.		
7	Switch should support ACL, BPDU protection, Dynamic ARP Inspection, DHCP Snooping, STP root guard, IP Source Filtering, RADIUS and TACACS+.		
8	Should support UDLD, Digital Diagnostic monitoring, Port and VLAN mirroring and IEEE 802.1ag or equivalent.		
9	Should support SNMPv6, Telnetv6 and SSHv6, NTPv6, Openflow and have USB or equivalent interface for easy backup and restore.		
10	Switch should support MAC Sec/FIPS 180-1 and IEEE 1588v2 PTP		
11	Operating Temperature of switch should be -40°C to 75°C		
12	The switch should have internal/external (DIN rail mountable) AC power supply.		
13	Protection Class should be minimum IP 30 and NEMA TS-2		
14	Switch should be EN55022, EN55024, IEC 61000-4-2, IEC 61000-4-3, IEC 61000-4-4, IEC 61000-4-5, IEC 61000-4-8, IEC60068-2-31, IEC60068-2-27, IEC60068-2-6 and RoHS.		
15	Should support UDLD or equivalent feature to prevent loops on detecting unidirectional links, Connectivity Fault Management, Monitoring Temperature, Supply voltage, Average transmit power, Average receive power and Laser bias current of the FO module, should have feature if any intrusion is detected on fiber link the particular port should be shutdown automatically.		

16	All the switches should be offered with min 5 years replacement warranty with proper back-up on respective-OEM letter Head. All the switches and FO Modules should be from the same OEM.		

16 Port Switch

SL No	Minimum Specifications	Compliance	
		Yes/No	
1	The Switch Should be Industrial grade in nature and should have 16x10/100/1000 Base-T PoE+ ports and 4x100/1000 Base-X SFP ports and to be supplied with required module.		
2	Switch should support maximum PoE Budget of 240watt		
3	The switch should have minimum switching capacity of 40Gbps.		
4	Switch Should support 16K MAC addresses and 4000 VLAN		
5	Switch should support Jumbo frame, ITU-T G.8032, IEEE 802.1ad, IEEE 802.1Q, IEEE 802.1v, IEEE 802.3ac, IEEE 802.1AX, DHCP Server and Relay for IPv4 and IPv6, DHCP Option 82		
6	Switch should support IGMP v1/v2/v3 snooping, MLD v1/v2 snooping with min 512 multicast group.		
7	Switch should support ACL, BPDU protection, Dynamic ARP Inspection, DHCP Snooping, STP root guard, IP Source Filtering, RADIUS and TACACS+.		
8	Should support UDLD, Digital Diagnostic monitoring, Port and VLAN mirroring and IEEE 802.1ag or equivalent.		
9	Should support SNMPv6, Telnetv6 and SSHv6, NTPv6, Openflow and have USB or equivalent interface for easy backup and restore.		
10	Switch should support MAC Sec/FIPS 180-1 and IEEE 1588v2 PTP		
11	Operating Temperature of switch should be -40°C to 75°C		
12	The switch should have internal/external (DIN rail mountable) AC power supply.		
13	Protection Class should be minimum IP 30 and NEMA TS-2		
14	Switch should be EN55022, EN55024, IEC 61000-4-2, IEC 61000-4-3, IEC 61000-4-4, IEC 61000-4-5, IEC 61000-4-8, IEC60068-2-31, IEC60068-2-27, IEC60068-2-6 and RoHS.		
15	Should support UDLD or equivalent feature to prevent loops on detecting unidirectional links, Connectivity Fault Management, Monitoring Temperature, Supply voltage, Average transmit power, Average receive power and Laser bias current of the FO module, should have feature if any intrusion is detected on fiber link the particular port should be shutdown automatically.		

16	All the switches should be offered with min 5 years replacement warranty with proper back-up on respective-OEM letter Head. All the switches and FO Modules should be from the same OEM.		

5.15 Internet Router & Core Router

Sl. No.	Parameter	Technical Specification	Technical Compliance (Yes/ No)	Remark
1	Multi-Services	Should deliver multiple IP services over a flexible combination of interfaces		
2	Ports	As per overall network architecture proposed by the bidder, the router should be populated with required number of LAN/WAN ports/modules, with cable for connectivity to other network elements		
3	Speed	As per requirement, to cater to entire bandwidth requirement of the project.		
4	Interface modules	Must support minimum 2* 10G Port with necessary SFP+ Modules (UTP or Fiber as per bidder design. Fully loaded). Must have capability to interface with variety interfaces.		
5	Protocol Support	Must have support for TCP/IP, PPP Must support IPSEC VPN Must have support for integration of data and voice services Routing protocols of RIP, OSPF, MPLS,PIM-SSM ,IS-IS, BGP+ etc. Support IPV4 & IPV6		
6	control	Control and Filtering features for flexible user control policies		
7	Remote Access	Remote access features		
8	Redundancy	• Redundancy in terms of Power supply(s). Power supply should be able to support fully loaded chassis • All interface modules, power supplies should be hot-swappable		
9	QOS Features	• RSVP		

		• Priority Queuing • Policy based routing • shaping • Time-based QoS Policy Bandwidth Reservation / Committed Information Rate		

5.16 24 Port L3 Switch (fully loaded)

Sl. No.	Parameter	Technical Specification	Technical Compliance (Yes/ No)	Remark
1	Ports	Must support minimum 24* 10G Port with necessary SFP+ Modules.(UTP or Fiber as per bidder design) (Fully loaded switch)		
2	MAC	Support 8K MAC address.		
3	Forwarding rate & Switching Capacity	Switching capacity of min. 40 Gbps or better and equivalent or better packet forwarding rate (Mbps)		
4	Port Features	Must support Port Mirroring, Port Trunking and 802.3ad LACP Link Aggregation port trunks		
5	Flow Control	Support IEEE 802.3x flow control for full-duplex mode ports.		
7	Protocols	• Support 802.1D, 802.1S, 802.1w, Rate limiting • Support 802.1Q VLAN encapsulation, IGMP • Support based on 802.1p priority bits with at least 8 queues • DHCP support & DHCP snooping/relay/optional 82/ server support • Shaped Round Robin (SRR) or WRR scheduling support. • Support for IPV6 ready features Support up-to 255 VLANs and up-to 4K VLAN IDs		

8	Access Control	• Support port security • Support 802.1x (Port based network access control). Support for MAC filtering.		
9	VLAN	• Support 802.1Q Tagged VLAN and port based VLANs and Private VLAN The switch must support dynamic VLAN Registration or equivalent		
10	Protocol and	• Network Time Protocol or equivalent Simple Network Time Protocol support • Switch should support segmentation classification should be based on user-definable application types:DSCP, Port based, TCP/UDP port number		
11	Management	• Switch needs to have console port for management via a console terminal or PC • Must have support SNMP v1,v2 and v3 • Should support 4 groups of RMON Should have accessibility using Telnet, SSH, Console access, easier software upgrade through network using TFTP etc. Configuration management through CLI/GUI based software utility and using web interface		

5.17 24 Port Distribution Switch (Fully Loaded Non PoE)

Sl. No.	Technical Specification	Technical Compliance (Yes/ No)	Remark
1	24 port switch, 24 port RJ45 (10/100/1000) with uplink		
2	MAC Table 8K, VLAN support 4096		
3	Packet Forwarding Rate should be 40 Mbps or better Switching capacity of min. 40 Gbps or better		
4	Switch should support Layer 2 switching protocols such as Standard Spanning Tree 802.1d,Rapid Spanning Tree (RSTP) 802.1w Multiple Spanning Tree		

	(MSTP) 802.1s (up to 8 instances),PortFast , BPDU Filter, Root Guard, Loop Guard, BPDU Guard , Error Recovery for enabling disabled link		
5	Switch should support VLAN, Port based VLAN, 802.1Q tag based VLAN, MAC based VLAN, Protocol based VLAN, Management VLAN, Private VLAN Edge (PVE), Q in Q (double tag) VLAN, GARP VLAN Registration Protocol (GVRP) for propagating VLAN		
6	Switch should Support DHCP Relay, DHCP Server		
7	Switch should Support Security Secure Shell (SSH), Secure Socket Layer (SSL), 802.1x, IP Source Guard, Port Security, DHCP Snooping, Loop Protection, Storm Control		
8	Switch should Support Various ACL - Source Destination MAC, VLAN ID, DSCP/ IP precedence, TCP/ UDP source and destination ports, 802.1p, Ethernet type, Internet Control Message Protocol (ICMP) packets, TCP flag		
9	Switch Should Support RADIUS/TACACS+Switch should support segmentation		
10	Switch should Support Port Mirroring		
11	Switch should Support SNMP, syslog, CLI, GUI, NTP		
12	Switch should have 90- 240 V AC input & console port for local access		

5.18 24 Port PoE Switch

Sl. No	Technical Specification	Technical Compliance (Yes/ No)	Remark
1	Shall support a minimum of 24 ports 10/100 RJ 45		
2	Switching capacity non-blocking, should be MAC binding feature in interface/Ports		
3	Should support 24 port POE as per 1EEE 803.af for IP cameras. (each port Power as per Bidder design)		
4	capable of handling 45-degree temperature.		

5.19 SAN SWITCH

SL	**Technical Requirement**	**Technical Compliance (Yes/No)**	**Remark**
1	The switch should have hot-swappable redundant power supply & fan module without resetting the switch, or affecting the operations of the switch.		
2	The switch should be able to support non-disruptive software upgrade.		
3	The switch should be able to support process restart		
4	The switch should be capable of creating multiple hardware-based isolated Virtual Fabric (ANSI T11) instances. Each Virtual Fabric instance within the switch should be capable of being zoned like a typical SAN and maintains its own fabric services, zoning database, Name Servers and FSPF processes etc. for added scalability and resilience		
5	The switch should be capable of supporting hardware-based routing between Virtual Fabric instances		
6	The switch should support graceful process restart and shutdown of a Virtual Fabric instance without impacting the operations of other Virtual Fabric instances		
7	The switch should support Smart Zoning increasing the overall scalability of the SAN Fabric.		
8	Inter-switch links should support the transport of multiple Virtual Fabrics between switches, whilst preserving the security between Virtual Fabrics		
9	The switch should be equipped with congestion control mechanisms such that it is able to throttle back away from a congested link.		
10	The switch should be capable of discovering neighbouring switches and identify the neighbouring Fibre Channel or Ethernet switches.		
11	The fibre channel switch should be rack-mountable. Thereafter, all reference to the switch’ shall pertain to the ‘fibre channel switch		
12	The switch to be configured with minimum of 96 ports 16 Gbps FC configuration backward compatible to 4/8.		
13	All 96 x FC ports for device connectivity should be 4/8/16 Gbps autosensing Fibre Channel ports.		
14	The switch shall support hot-swappable Small Form Factor Pluggable (SFP) LC typed transceivers		
15	The switch should support hardware ACL-based Port Security, Virtual SANs (VSANs), and Port Zoning.		
16	The switch should support routing between Virtual Fabric instances in hardware.		
17	The switch shall support FC-SP for host-to-switch and switch-to-switch authentication		
18	The switch should be able to load balance through an aggregated link with Source ID and Destination ID. The support for load balancing utilizing the Exchange ID should also be supported		

5.20 SAN STORAGE

S No	**Technical Requirement**	**Technical Compliance (Yes/No)**	**Remark**
1	Storage Solution should be provided with NSPoF (No single point of failure) Architecture.		
2	The solution should allow upgrades of hardware and software for investment protection.		
3	Controllers: Minimum dual controllers with symmetric active-active architecture. Each controller shall be configured with minimum 6 core or higher CPU		
4	Cache Memory: Should be provided with minimum 768GB Global cache or more.		
5	Connectivity: Minimum 2 ports per controller to be provided for host connectivity		
6	RAID Support: RAID 5/6 level Support		
7	Redundancy: Fans and power supplies: Dual redundant, hot- swappable		
8	Storage subsystem should support 10TB/14TB/18TB or higher NLSAS/SATA/equivalent 7.2K drives in the same device array.		
9	Should be supplied with 3 PB effective usable capacity storage with NL-SAS drives.		
10	Should have the capability to designate global hot spares that can automatically be used to replace a failed drive anywhere in the system.		
11	Should be configured with required Global Hot-spares for the different type and no. of disks configured, as per the system architecture best practices.		
12	Multipath: Multi-path & Load balancing should be supported. Unlimited host multipath licenses should be quoted from day one.		
13	Thin Provisioning: Array should be supplied with Thin provisioning for the configured capacity.		
14	De- duplication: Array should have capability to provide compression, de-duplication and encryption.		
15	Tiering: Should support inbuilt automated tiering feature that migrates the most frequently accessed data to the SSD/RAM. Necessary licenses for configured capacity if required without additional cost		
16	Snapshots: Should be able to take "snapshots" of the stored data. Offered Storage shall have support to make the snapshot in scheduled or auto snaps. Snapshot should support both block and file.		
17	Replication: Array should have the capability to do remote replication using IP technology		
18	Software Licenses : All the necessary software and licenses to configure and manage the storage space, RAID configuration, logical drives allocation, snapshots, compression, de-dup, replication, auto-tiering for the configured capacity.		
19	Monitoring: Should support the functionality of monitoring of Disk drive and Storage system for all possible hard or soft failure.		
20	The Storage should be jointly validated by VMS (Video Management System) software and storage for batter integration requirement		
21	Warranty: Five years on site warranty from OEM		

5.21 BACKUP SOFTWARE

SL	Technical Requirement	Technical Compliance (Yes/No)	Remark
1	The solution should offer centralized, web-based administration with a single view of all back up activities and should have alerts generation facility in case of any issue in backup process.		
2	Support de-duplication at source and at target (disk) on any commodity storage volume. Based on policy backup software should be able to move data to a Tape/Disc library automatically		
3	Support scheduled unattended backup using policy-based management for all Server and OS platforms		
4	Should have in-built frequency and calendar based scheduling system.		
5	Should be able to backup any applications in online mode through online SAN based backups of databases through appropriate agents; Important Applications such as Database, webserver, application, emails irrespective of the number of servers / CPUs, configuration of the servers, etc.		
6	Should be capable of having multiple back-up sessions simultaneously		
7	Should be capable of taking back up of SAN environment as well as LAN based backup.		
8	Should support different types of backup such as Full back up, Incremental back up, Differential back up, Selective back up, Point in Time back up and Progressive Incremental back up and snapshots		
9	Should have the ability to integrate with archival software and create a single repository for backup and archive for space efficiency and easier data management.		
10	Should have in-built media management and supports cross platform Device & Media sharing in SAN environment.		
11	Should be able to rebuild the Backup Database/Catalogue from tapes in the event of catalogue loss/corruption.		
12	Should have online backup solution for different type of databases such as Oracle, MS SQL, MySQL and Sybase / DB2 etc. on various OS.		
13	Should be able to copy data across firewall.		
14	Should also be capable of reorganizing the data onto tapes within the library by migrating data from one set of tapes into another, so that the space available is utilized to the maximum. The software should be capable of setting this utilization threshold for tapes		
15	Should be able to support versioning and should be applicable to individual backed up objects.		

5.22 Server Load Balancer

Sl. No	Technical Specification	Technical Compliance (Yes/ No)	Remark

1.	The Load Balancer device should be a dedicated Hardware Appliance with the following features:		
	a. Should support multiple virtual network functions in which each VNF has a dynamic or dedicated resource allotted to it like CPU, RAM, Hard Disk, SSL cores.		
	b. The appliance shall deliver the high availability required by modern data centres. It should support Active/Passive or Active / Active HA configurations using standard VRRP protocol or equivalent		
	c. The Load Balancer shall automatically synchronize configurations between the pair and automatically failover if any fault is detected with the primary unit.		
2.	The Load Balancer shall support offloading of SSL connections and should deliver 10 Gbps or better		
3.	Proposed device should have minimum 8 x 10G SFP+ ports prepopulated and up to 2 x 40 QSFP ports		
4.	Proposed device should support up to 04 virtual instances with capability to run multiple virtual network Functions.		
5.	The server load balancer should deliver minimum 1 Million concurrent sessions		
7.	Local Application Switching, Server load Balancing, HTTP,TCP Multiplexing, HTTP Pooling, HTTP Pipelining, Compression, Caching, TCP Optimization, Filter-based Load Balancing, Transparent Deployments, Content-based Load Balancing, Persistency, HTTP Content Modifications, Band Width Management(BWM), Support for connection pooling to TCP request, Support for distributed denial-of-service (DDoS) protection		
8.	The solution should support XML-RPC for integration with 3rd party management and monitoring. Should also support SAA, SAML, Hardware binding and AAA support along with SSO. Solution must support machine authentication based on combination of HDD ID, CPU info and OS related parameters i.e. mac address to provide secure access to corporate resources."		

5.23 Servers

Sl. NO.	Parameter	Technical Specification	Technical Compliance (Yes/ No)	Remark
1	Processor	Latest series/ generation of 64-bit x86 processor(s) with minimum 24 or higher Cores as per bidder design Processor speed should be minimum 2.1 GHz Minimum 2 processors per each physical server		
2	RAM	Minimum 128 GB Memory per physical server scalable		

		up to 1.5 TB		
3	Internal Storage	2 x 600 GB SAS (10k rpm) hot swap		
4	Network interface	4 X 10GbE LAN ports for providing Ethernet connectivity or equal Fiber ports as per bidder design		
5	Power supply	Dual Redundant Power Supply		
6	RAID support	As per requirement/solution (Since RAID 5 provides balanced cost, reliability, capacity, and performance requirements simultaneously, RAID 5 may be considered.)		
8	Form Factor	Rack mountable		
9	Virtualization	Shall support Industry standard virtualization hypervisor like Hyper-V, VMWARE, Oracle VM etc.		

5.24 Server for Video Analytics

Sl. No	Parameter	Technical Specification	Technical Compliance (Yes/ No)	Remark
1	Processor	Latest series/ generation of 64-bit x86 processor(s) with 24 or higher Cores Processor speed should be minimum 2.1 GHz Minimum 2 processors per each physical server		
2	RAM	Minimum 128 GB Memory per physical server scalable up to 1.5 TB		
3	Internal Storage	2 x 600 GB SAS (10k rpm) hot swap		
4	Network interface	4 X 10GbE LAN ports for providing Ethernet connectivity		
5	Power supply	Dual Redundant Power Supply		
6	RAID support	As per requirement/solution (Since RAID 5 provides balanced cost, reliability, capacity, and performance requirements simultaneously, RAID 5 may be considered.)		
7	Operating System	64-bit latest version of operating system as per requirement of AI solution		

8	Form Factor	Rack mountable		
9	Virtualization	Shall support Industry standard virtualization hypervisor like Hyper-V, VMWARE, Oracle VM etc.		
11	GPU	Minimum 2 GPU each server, A10 or better (server grade GPU cards not workstation grade)		

5.25 KVM Module

Sl. No	Parameter	Technical Specification	Technical Compliance (Yes/ No)	Remark
1	KVM Requirement	Keyboard, Video Display Unit and Mouse Unit (KVM) for the IT Infrastructure Management at Data Centre		
2	Form Factor	19” rack mountable		
3	Ports	minimum 8 ports		
4	Server Connections	USB or KVM over IP.		
5	Auto-Scan	It should be capable to auto scan servers		
6	Rack Access	It should support local user port for rack access		
7	SNMP	The KVM switch should be SNMP enabled. It should be operable from remote locations		
8	OS Support	It should support multiple operating system		
9	Power Supply	It should have dual power with failover and built-in surge protection		
10	Multi-User support	It should support multi-user access and collaboration		

5.26 Rapid Deployable System

Sl. No.	Features	Description	Technical Compliance (Yes/ No)	Remark
1	Camera Type	Mobile Speed Dome		
2	Certification	UL/BIS ,CE,FCC and RoHS		
3	Image Sensor	1/2.8" CMOS or better		
4	Max. Mbps CVBR	6		
5	Compression	H.264,H.265		
6	Streaming	Min. Triple compressed stream (Individually Configurable)		
7	Encryption	HTTP(SSL/TLS)/HTTPS		
8	Video Authentication	For video authentication, classic watermarks/ digital signature must be embedded in Video Stream along with name, time, date stamped which cannot be tampered.		
9	Physical Layer	10/100 base Tx Ethernet		
10	Protocol	Minimum TCP, HTTP, RTP, RTSP, SNMP, IPV4, IPv6, FTP, NTP, DHCP, RTP, SMTP, UDP, UPnP, ICMP, IGMP, QoS, 802.1x, DNS, DDNS, HTTPS		
11	IP Support	Static/dynamic or both		
12	Remote Administration	Remote configuration and status using web- based tool		
13	System Update	Remote system update over Network using web client		
14	PC Client	PC application client with a channel recording feature support		
15	Web Client	Viewer through HTTP (min.) System Configuration Setting/ Streaming		
16	Simultaneous Connection	5 users or more		
17	Lens Type	5.9-135.7mm, 20x motorised, Autofocus, Auto-iris, Varifocal		
18	Dynamic Noise Reduction	3D		
19	Auto Exposure	Automatic Level Control/Electronic Level Control		
20	Intelligent Defog	Yes		
21	Illumination	Colour: 0.05 lux, F1.6, B/W: 0.01 lux, F1.6 At 30 IRE, Inbuilt IR (60 mtrs. or better)		
22	Signal Process	Digital Signal Process		
23	Auto Gain Control	Yes		
24	Back Light Compensation	Yes		
25	High Light Compensation	Yes		
26	Electronic Shutter	1/10000s to 1 s or better		
27	White Balance	Yes		
28	Wide Dynamic Range	96db		
29	Day and Night	Yes, (ICR)		
30	Operating Temperature	0 °C to 60 °C; Humidity 20 80% RH (non-condensing)		

31	Power Source	Suitable adaptor shall be supplied to make the equipment work on 230V +10%, 50Hz and Power over Ethernet (POE 802.3 at) OR 12 V DC through NVR		
32	Internet protocol Support	IPv4 and IPv6		
33	Housing	Poly Carbonate/ Aluminium Construction with IP-66 Including pole mount/wall mount accessories, Power and data cables		
34	Presets	100 presets or higher		
35	Accessories	All required accessories at site for installation of camera to be provided like Pole Mount, Corner brackets, Connector kit, screws etc.		
	NVR			
36	IP video input	8 Ch independent POE interfaces		
37	Two-way audio	1 Ch		
38	Incoming bandwidth	at least 80 Mbps		
39	Encoding technique	H.264,H.265		
40	Recording resolution	Min.1920 x 1080		
41	VGA output	1-ch with resolution upto 1280 x 800		
42	CVBS output	1-ch		
43	Live view	Simultaneous 8 Ch		
44	HDD type	Pluggable 2 - 2.5-inch SATA HDDs / SSDs		
45	Capacity	2 TB capacity HDD each		
46	Protection	Safety lock support anti-theft for storage hard disk.		
47	Backup interfaces	Hard disk box, USB interface supporting data backup		
48	Dialling	3G / 4G with SIM card		
49	Wi-Fi	802.11 b/g/n supported, 2.4GHz		
50	GPS	Support		
51	Network interface	1; RJ45; 10M/100M self-adaptive Ethernet interface		
52	Antenna interface	1 SMA interface for 1 3G or 4G antenna, 1 WIFI antenna and 1 GPS antenna		
53	Serial interface	RS-232		
54	USB interface	Front USB Port		
55	SIM card	1, standard SIM card slot		
56	Operating system	Linux		
57	Operating method	IR remote control		
58	Working temperature	-10°C to 55 °C		
59	Working humidity	10% to 90%		
60	Display	Yes		
61	TFT	7 inch TFT to be provided along with all necessary cables for connecting with NVR/Camera for display and power adapter etc.		
62	Joystick	to be provided		

5.27 24 Port Copper Patch Panel, fully loaded

Sl. No.	Technical Specifications	Technical Compliance (Yes/ No)	Remark
1	Patch panel should be modular design, to be populated with 24 nos. Cat 6 UTP RJ 45 Keystone Jack as per specifications provided		
2	Each Ports should be with individual spring loaded shuttered/ hinge type cover for dust protection. Each port (jack) and individual replaceable.		
3	Material: Should Be made of cold rolled steel and conform to TIA / EIA 568-C.2 Component Compliant		
4	Should have integral rear cable management shelf.		
5	Commercial Standards:		
	ANSI/TIA 568-C.2 and IEEE 802.3bt Component Compliant		
	FCC Subpart F 68.5 Compliant		
	IEC-603-7 Compliant		
	ISO 11801 Class E Compliant		
	ETL Verified for Category 6 Component Compliance Or BIS Equivalent		

5.28 40 MM HDPE Duct

Sl. No.	Functional Requirement		Technical Compliance (Yes/ No)	Remark
1	Wherever cables are laid underground, it must be laid within HDPE duct as per the specifications below.			
2	LAN/ OFC Cable should not be laid together with Power cable. If cables are laid using conduit, then there should be separate conduit for LAN cable and power cable.			
3	When taking multiple cables through a single HDPE Duct it should be ensured that there is always space available to take one more additional cable through it if required later.			
Sl. No.	**Technical Specifications**		**Technical Compliance (Yes/ No)**	**Remark**
	Outer Diameter	As per design considering passive components to be used in Project. To be industry standard as applicable.		

1	Raw material used for the HDPE pipe shall meet the following requirements:		
	i. the anti-oxidant establishers, colour master batch and other additive used shall be physiologically harmless and shall be used only to minimum extent necessary to meet the specification.		
	ii. Usage of any additives used separately or together should not impair the long-term physical and chemical properties of the HDPE pipe.		
	iii. Suitable Ultra-Violent stabilizers may be used for manufacture of the HDPE pipe to protect against UV degradation when stored in open for a minimum period of 8 months.		

	iv. The base HDPE resin used for manufacturing outer layer of pipe shall conform to any grade of IS-7328 or to any equivalent standard meeting the following requirement. Density 940 to 958 kg/m3 at 27o C Melt Flow Rate 0.12 - 1.1g/10 minutes at 190oC & 5kg load		
	v. In case of HDPE pipe of two concentric layer construction, the friction reducing, polymeric material to be used as the inner layer lubrication material shall be integral with HDPE layer. The lubricant materials shall have no toxic or dramatic hazards for safe handling. Permanent Lubricated (Per Lub) HDPE Pipes should be sourced from the manufacturer with ISO 9000 accredited manufacturing facility.		
2	**Plastic coupler:** The coupler shall be used to join two HDPE pipes. The coupling shall be able to provide a durable water tight joint between two pipes without deteriorating the strength of the pipes. The strength of coupler shall match the primary strength of the HDPE pipe. It should be push fit type. Threaded coupler is not acceptable. The jointing shall meet the air pressure test of 15 kg/cm2 for a minimum period of 2 hours without any leakage		
3	**End plug:** This shall be used for sealing the ends of empty pipe, prior to installation of FO cable and shall be fitted immediately after laying of the HDPE pipe, to prevent entry of any unwanted elements such as dirt, water, moisture, insects/rodents etc.		
4	**Cable sealing plug:** This is used to hold the cable and prevent entry of any unwanted elements, as specified above.		
5	**End cap:** This cap is made of hard rubber, shall be fitted with both ends of HDPE pipe to prevent the entry of any unwanted elements such as dirt, water, moisture, insects/rodents during transportation and storage		
6	The HDPE Pipe should comply with the following standards A. IS: 4984 - Specification for HDPE pipe. B. IS: 2530 - Method for tests for polyethylene molding materials and compounds. C. IS: 9938 -Recommended colours for PVC insulation for LF wires and cables. D. TEC-spec no -HDPE pipe for use as duct for G/CDS-08/01 optical fibre cable. E. IS: 7328 - HDPE material for molding and extrusion. F. ASTM D 1693 - Test method for environmental stress cracking of ethylene plastics. G. ASTMD 1505 - Test method for density. H. ASTMD 3895 - Method for Oxidation Induction test.		

5.29 Specifications for Passive Components

Double Jacket CAT6 UTP Outdoor Cable			
Sl. No.	**Functional Requirement**	**Technical Compliance (Yes/ No)**	**Remark**
1	All passive network passive components should be from the same OEM and OEM to provide 30 years performance warranty against this.		
2	RJ-45 Field Termination plug as per specifications provided to be used with the field device and not standard RJ45 plug.		
3	LAN/ OFC Cable should NOT be laid together with Power cable. If cables are laid using conduit, then there should be separate conduit for LAN cable and power cable.		

4	All the cables to be tagged either with wrap around labels or Cable flags using machine labelling. Handwritten labels are not allowed.		
5	Wherever cables are laid underground, it must be laid within HDPE duct as per the specifications provided.		
6	All CAT6 patch cords to be used should be pre-fabricated ones and not locally made at site except for the cable connecting the SPD output to the field device as Field Termination plug to be used on the device side.		
Sl. No.	**Technical Specifications**	**Technical Compliance (Yes/ No)**	**Remark**
1	4 Pair Cable with integral cross -member pair separator for uniform characteristic impedance.		
2	Category 6 Unshielded Twisted 4 Pair 100 Ω cable shall be compliant with ANSI/ TIA/ EIA-568-C.2- 1/ ROHS Additional ISO/ IEC 11801 2ndEd. Transmission Performance Specification for 4 Pair 100Ω Category 6 Cabling		
3	Category 6 UTP cables shall extend between the work area location and its associated telecommunications closet and consist of 4 pair, UTP cable jacket.		
4	Conductor: Solid Copper		
5	Conductor Diameter: 0.574, ± 0.01mm (23AWG)		
6	Inner Jacket: LSZH/ PE/ PVC		
7	Outer Jacket: PE –Black, Anti-Rodent, LSZH/ PE/ PVC		
8	Max Temperature: -10°C to +60°C		
9	**Mechanical Test**		
10	Should have Pulling force more than 10 Kg.		
11	**Electrical Test**		
12	Conductor Resistance: <9.38Ω /100m		
13	Resistance Unbalance 5% Max		
14	Mutual Capacitance: < 5.6nF/100m		
15	Capacitance Unbalance: 330pF/100m.		
16	Characteristic Impedance: 100 +15 Ω conductor		

12 Core Outdoor Armoured Single Mode OS2 Type Outdoor Fiber Cable Double Sheathed

Sl. No.	Specifications	Requirement	Technical Compliance (Yes/ No)	Remark
1	Cable Type	12 Core fiber Cable, Single Mode OS2 Type, Armoured, Double Sheathed Gel filled cable complying to ISO.IEC 11801 - 2nd Edition, type OS1; AS/ACIF S008; AS/NZS 3080, EIA/TIA 568-C.3.;ITU-T REC G 652D spec, complied for Low Water Peak fibre suitable for use in direct burial and IEC 60793/60794-1-2, outdoor ducts and backbone cabling		

2	Armour	Corrugated Steel Tape Armour - Thickness > 0.15mm		
3	Water Blocking	Thixotropic Gel (Tube), Petroleum Jelly (Interstices)		
4	Attenuation	,@ 1310nm <=0.35 db/Km MAX ,@1550nm <=0.22 db/Km MAX		
5	Loose tube diameter	2.0mm (nominal) – PBTP		
6	Inner Sheath thickness	1.1 mm(nom)		
7	Outer Sheath	UV proof HDPE Black (1.8 mm Nominal Thickness)		
8	Core/Mode-Field (um)	9 ± 0.4 µm		
9	Clad Diameter (um)	125 ± 1		
10	Coat Diameter	245 ± 10		
11	Loose tube material	Single PBTP Loose tube filled with water blocking Thixotropic gel		
12	Jacket material	UV Stabilised Polyethylene (HDPE)		
13	Central Strength Member	Non Metallic (FRP)		
14	Max. Tensile Strength:	3500N		
15	Maximum Crush Resistance	6000N/10 mm		
16	Cable Diameter	13.5±1.0 mm		
17	Max. Bending Radius (during installation)	20D		
18	Fibre Identification	Colour coded		
19	Cable weight Kg/Km	175-185± 10%kg/km		
20	Operating Temperature	.-40 Degree C to +70 Degree C		
Fiber Optic LIU 12 Port loaded with SC Adapter, Splice Tray, SC Pigtail and Splice Protector				

Sl. No.	Specifications	Requirement	Technical Compliance (Yes/ No)	Remark
1	Fiber optic patch Panel	The 1U Multi-Function Fibre Enclosure is a configurable rack mount unit for storing and terminating incoming fibre cable.		
		The fibre enclosure has been designed to accommodate various termination types and adapter configurations. Accommodates up to 4 Modlink Cassettes or up to 4 nos of 6 or 12-Pak adapter plates.		
		The enclosure must, have a sliding drawer for ease of reconfiguring fibers, incorporates a heavy-duty ball bearing slide mechanism, allowing easy access to fibers		
		The adapter plates must be an interchangeable front plate which can facilitates upgrades as & when required.		
		Copper grounding stud tie down points at each cable entrance point.		
		The enclosure must have front cable management to properly route patch cords.		
		Fibre management enclosures that can be used as rack mount enclosure for integrated applications.		
2	Material	Powder coated Mild Steel		
		Rugged steel construction in graphite finish		
		Rear, side & base access for Incoming / Outgoing fiber cables		
3	Cable Management rings	Management rings within the system to accommodate excess fibre cordage behind the through adapters and maintain fibre bend radius.		
4	Sliding cover	Panel cover is of slide out for easy maintenance. Incorporates heavy-duty ball bearing slides for smooth and limited extension of the drawer unit, allowing for patch cable access while protecting installed patch and trunk cables from damage during re-entry of the enclosure		

5	Optical Fibre Adapter Plates	SC Adapter SM Plate - loaded with 12 Nos SC Adapter		
6	Pigtails	SC, Single mode, 9/125 µm - 1.5 mtrs (12 Nos)		
7	Splice Tray	12 Port Splice Tray - 1 No		

Fibre Optic Splice Enclosure

Sl. No.	Functional Requirement	Technical Compliance (Yes/ No)	Remark
1	To be used for Straight through application for jointing of Optical Fibre Cable.		
2	Should be mounted on the pole using accessories from the FOSC OEM		
3	All passive network components along with accessories should be from the same OEM and OEM to provide 30 years performance warranty against this.		

Sl. No.	Technical Specifications		Technical Compliance (Yes/ No)	Remark
1	Type	Fiber Optic Joint closure shall be environmentally sealed enclosure for fiber management in the outside environment.		
2	Size options	Shall be available for 48 fiber splice options.		
3	Cable inlets	2 IN/ 2 OUT cable inlet options shall be provided.		
4	Splice trays	4 nos. and splice trays to be hinged for access to any splice without disturbing other trays		
5	Cable Handling	Closure shall be compatible with most common cable types.		
6	Environment	The closure shall be suitable for usage in aerial, pedestal and underground environments. Shall be at least IP 65 rated for outdoor usages.		
7	Compliant	Must be ROHS or BIS Equivalent		

5.30 Rack with Fire Suppression System

Sl. No	**Technical Specification**	**Technical Compliance (Yes/ No)**	**Remark**
1	Floor Mount Rack		
2	42U x 800 x 1000 Skeleton with Castor Mounting Provision		
3	800W Front Perforated Door with Swing Handle Lock		
4	800W Rear Perforated Door with Swing Handle Lock		
5	1000D Openanale Side Panel – Pair		
6	100MM Reducing channel * 1Pair		
7	Castors set of 4Nos and Levellers		
8	19" MGMT Rails * 2Pair		
9	Roof Mounted Four Fan Unit of 90CFM / 230V with power cord		
10	19 Socket 32AMPs, 230 Volt PDU		
11	100mm Rear cable basket - 1pair		
12	Horizontal Cable Manager 1U - 4nos		
13	Hardware Packet of 20nos - 2nos		
14	Fixed Shelf - 1nos		
15	With inbuilt Fire Suppression System , Optical smoke detector, Clean agent		

5.31 POLE FOR CCTV CAMERA

Sr.		**Description**	**Compliance (Yes / No)**	**Remark**
1	Pole Type	Galvanized pole as per IS:2629 and Fabrication as per IS:2713 Pipes should be as per IS 1161		
2	Fininsh	Poles should be Hot Dipped Galvanized with min 75Micron		
3	Height	6 Meters / 7Meters Height as per site requirement		
4	Pole Diameter	Nominal Bore : 175NB Outer Diameter : 193MM		
5	Pipe Thickness	Min 4.5MM		
6	Cantilever	2M / 4M Cantliver Arm should be provided as per site requirement The cantilever should be fitted such that they can be rotated to change the direction or adjust the angle, if at all required. The Cantilever should be strong enough so as to mount at least 2 CCTV camera’s and associated fixtures like IR, etc., if required.		
7	Bottom base plate	Minimum base plate of size 40x40x2 cm		
8	Pipes, Tubes	All wiring must be hidden, through tubes/pipes. No wires shall be visible from outside.		
9	Foundation	Minimum 1 meter; To ensure that video feed quality is not impacted due to winds in different climatic conditions and from vibration caused due to heavy vehicles on road		
10	Mounting Facility	Should support pole, cantilever, Junction Box		

CYBER SECURITY COMPONENTS SPECIFICATION

5.32 Next Generation Perimeter Firewall

Sl.No	Item Description	Technical Specification	Technical Compliance (Yes/No)	Remark
1	**Make**	To be mentioned by the bidder/ Vendor		
2	**Model No.**	To be mentioned by the bidder/ Vendor		
3	**Country of Origin**	To be mentioned by the bidder/ Vendor		
4	**Hardware Architecture**	The proposed hardware based firewall should not consume more than 2RU Rack-mountable space		
		Proposed Firewall should not be proprietary ASIC based in nature & should be multi-core CPU's based architecture to protect latest security threats.		
5	**Performance Capacity**	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), 4 x 10G SFP+ ports from day one. The device should be upgradable to 8 x 1G Cu ports, 2 x 40G and 8 x 10G/25G in the same chassis in future.		
		Appliance should have minimum 1 TB (SSD) Built in Storage from day 1.		
		Appliance should support 35 Gbps or more Firewall throughput & 20 Gbps or more IPS throughput.		
		Appliance should support 18 Gbps or more Threat Protection throughput		
		The device should have Concurrent Sessions: 8 Million or higher & New connection/Sec: 200,000 or higher		
		Firewall Should support at least 15 Gbps or more IPsec VPN throughput and support 2000 IPsec Site-to-Site VPN tunnels & 4000 IPsec VPN clients and 20 Gbps or more IPS Throughput		
		Firewall Should support at least 8 Gbps or more TLS/SSL inspection & decryption throughput and support 1000 SSL VPN clients. The appliance should have 500,000 SSL DPI connections.		
6	**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.		
		solution should support policy based routing, Application based routing and also Multi Path routing.		
		Application Control : 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 inspections on following protocols DNS,FTP,H.323 ,SMTP,SQLnet, RTSP, Skinny, 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.		
		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 using low-cost internet 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 Pictorial view of a particular access rule, NAT and Routing rule which helps in finding real-time statistics. Displays the rules which are actively used or not being used & enabled or disabled..		
7	**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 DPI 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.		
		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 55 + categories.		
		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.		
		Firewall should support HTTP Request tempering protection, Directory traversal prevention, SQL injection Protection, Cross site scripting Protection (XSS) & DNS security		
		Should provide complete protection by performing full decryption and inspection of TLS/SSL and SSH encrypted connections regardless of port or protocol.		
		Solution should support an on premise based Multi-engine Sandboxing for preventing zero-day threats. One on-premise Sandbox solution/device should be proposed which should integrate with the proposed Firewalls. Both the Sandbox appliance and Firewalls should be essentially from the same OEM.		
		The on-premise sandbox should have memory based inspection, Multi-Stage Analysis with reputation check, static analysis and dynamic analysis, Reporting and Role-Based Access and Closed Network Support. Should allow/Block list for file hash or IP/Domain and Analysis of files up to 100MB. Should have False positive and false negative reporting with automatic whitelist and blacklist. The on-premise sandbox should have Hardened OS with Secure Boot and chain of trust for anti-tampering.		
		It should have 12,000 files per hour for Threat lookup throughput and min 300 files per hour for Dynamic Analysis throughput. VMs supported should be Windows 7 32/64, Linux 64. It should have 2 x 1TB SSD		

		storage and 6 x 1Ge interfaces, 2 x 10G SFP+ interfaces and a dedicated management port.		
		The Sandbox should have technology that detects and blocks malware that does not exhibit any malicious behaviour and hides its weaponry via encryption. Should detect and block mass-market, zero-day threats and unknown malware. The technology should discover packed malware code that has been compressed to avoid detection, the technology should allow the malware to reveal itself by unpacking its compressed code in memory in a secure sandbox environment. It should see what code sequences are found within and compares it to what it has already seen. The Firewall should have the capability to block/prevent from Side Channel attacks like Meltdown, Spectre, Foreshadow, Foreshadow-NG, Portsmash etc.		
		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.		
		Should have ability to prevent potentially malicious files from entering the network and those files sent to the sandbox for analysis to be held at the gateway until a verdict is determined.		
		Deep packet SSL should be available on the same platform & License for DPI SSL should be along with appliance.		
		The Firewall solution should have detection and prevention capabilities for C&C communications and data exfiltration.		
		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.		
8	**High-Availability Features**	The proposed solution should support active-passive / standby / active high availability. The Firewalls should be proposed with High Availability configuration (Active-Passive with State Sync) from day 1.		
		The device should support stateful session failover to a standby appliance in the event of a hardware failure without any manual intervention.		

9	**Visibility and Monitoring**	Should provide real-time monitoring and visualization 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.		
10	**Management & Reporting Feature**	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 which includes configuration, logging, monitoring, and reporting are performed by the Management Centre onprem and on cloud.		
		The Centralize management platform should support multidevice firmware upgrade, certificate management, global policy template to push config across multiple firewall in single click.		
		The Centralize management 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.		
		Firewall should have reporting facility to generate reports on virus detected over different protocols, top sources for viruses, destination for viruses, top viruses 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		
		The solution should have configurable options to send the alert emails based on event type & reports as a mail to the designated email address		
		Analytics platform support Real-time risk monitoring and analysis of all network and user that passes through the firewall ecosystem		

		The 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.		
		Logging and reporting solution should be supported. Should have Multi Tenant and Device Group level management		
		Should have reporting facility to generate reports on virus detected over different protocols, top sources for viruses, destination for viruses, top viruses etc.		
		The solution shall have readymade templets to generate reports like complete reports or attack reports, bandwidth report etc.		
11	**Certification, Warranty, Installation, Testing and Commissioning**	The Firewall solution offered must be ICSA certified for Network Firewall, Anti-virus or Common Criteria NDPP (Firewall and IPS) – Certification.		
		The Firewall OEM should be having "recommended rating" by NSS Labs for consecutive three years in the last six years. OEM should have scored minimum 97% in Exploit Block rate in the last NSS Lab for NGFW report (2019).		
		Proposed Solution should support 24x7x365 telephone, email and web-based technical support.		
		OEM should have TAC and R&D centre in INDIA.		
		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.		
		Bidder must carry out on site installation, testing and commissioning.		

5.33 Next Generation Core Firewall

Sl. No	**Technical Specification**	**Technical Compliance (Yes/No)**	**Remark**
	Hardware Specification		
1	Firewall should be ICSA Labs Certified		
2	Proposed solution should come from firewall appliance family which has more than 10 years of ICSA labs certification		

3	Minimum internal storage 1000 GB SSD for detailed graphical Logs & Reports on Appliance		
4	Appliance must have 16 GB RAM or Higher		
5	Firewall should have 2 or higher USB 2.0 / USB 3.0		
6	Firewall should have Redundant Hot-Swappable Power Supply		
7	Firewall should have Redundant Hot-Swappable Fan		
8	Proposed solution should have open standard multicore processor based architecture and not proprietary ASIC based architecture		
	Interface Requirement		
1	Solution should have 1/2 x Management Port + 1 x Console Port (RJ45/MicroUSB)		
2	8 Ports of 1G Copper		
3	4 Ports of 10G SFP+ (Fiber Ports)		
4	6 or Higher Expansion Slot for Future Expansion (1G Copper / 1G SFP / 10G SFP+/ 40G QSFP+)		
	Performance Capacity		
1	Concurrent Sessions -30000000 or Higher		
2	New Sessions/second - 300000 or Higher		
3	Firewall Throughput - 70 Gbps or Higher		
4	Threat Protection Throughput- 12 Gbps or Higher		
5	VPN Throughput - 18 Gbps or Higher		
6	NGFW Throughput - 20 Gbps or Higher		
7	IPS Throughput - 30 Gbps or Higher		
8	Firewall IMIX Throughput - 32 Gbps or Higher		
	Next Generation Firewall Features		
1	The proposed system should have firewall with stateful packet filtering technology & must support one-to-one and dynamic user based NAT with a facility to create rules based on usernames, Source & Destination IP address, Hosts, network, IP Range		
2	The firewall of the proposed system should be based on a hardened OS, should be capable of delivering network protection services at all layers along with options of network gateway level anti virus, anti spam, intrusion detection and prevention, content filtering, multiple ISP load balancing, failover and VPN solutions.		
3	The firewall should be able to support deployment in transparent mode , Bridge mode, layer 3 transparent proxy mode		
4	The firewall of the proposed system should provide Predefined services based on port numbers and Layer 7 application and ability to create user-definable services which can be used to define firewall rules		
5	Minimum 20 perpetual Virtual Firewall licenses to be provided with the solution. Scalable upto 25.		
6	The proposed system must provide inbuilt PPPoE client and should be capable to automatically update all required configuration (NAT Policies, VPN Configuration, Firewall Rules) whenever PPPoE IP get changed.		
7	The firewall of the proposed system should support 802.1q based VLAN tagging to segregate devices logically		
8	The proposed solution should have option to configure firewall policies to block or allow rules based on Country based Geo Location		
9	The proposed solution must have control mechanism to perform policy based control for Application, shaping and visibility for Users, Groups, IP address & Network.		
10	The proposed solution should be able to detect & block known applications like P2P & IM.		

11	The proposed solution should provide guaranteed and burstable bandwidth for applications.		
12	Should have Role based and multi factor authorization for Administration		
13	The proposed solution should be able to detect & block known applications based on time schedule.		
14	The Proposed solution should have an option to provide complete policy enforcement and visibility of roaming users and should restrict the remote user from disabling it.		
15	The organization policy framework must be extended to the remote users and ideally it should control the Web and Application filter of remote user		
16	The proposed solution should be able to alert on user activity outside business hours		
	URL Filtering & Web Protection		
1	Should support 85+ Web categories		
2	Should support blocking of category based HTTPS sites without having to provide the URL of the site to be blocked		
3	Should support HTTPS transparent proxy		
4	The proposed system should support browsing proxy and gateway mode simultaneously		
5	The proposed solution should block HTTPS URLs with complete path instead of only sites names		
6	The proposed solution should support regular expression in blocking of HTTPS sites		
7	Should enforce Google/Yahoo Images strict filtering through a web interface.		
8	Web based management through https and command line interface support		
	Application Filtering		
1	The proposed solution should support Application Filtering in the same appliance.		
2	The proposed solution should have inbuilt Application category database.		
3	The proposed solution should provide policy-based shaping by application for User, Group, IP address & Network.		
4	The proposed solution should be able to detect & block known applications like P2P & IM.		
5	The proposed solution should have 2500+ application database & 5000+ application signature		
6	The proposed solution must give reports based on username / IP address.		
	Intrusion Prevention System		
1	Intrusion Prevention system should be appliance based or integrated with the NGFW solution		
2	The proposed IPS system should have signature and anomaly base intrusion detection and prevention system		
3	The proposed system should have configuration options to prevent all the common DOS and DDOS attacks like syn flood, ICMP flood, UDP flood, Ping of death. Should have prevention option for more than 30 common attacks. Real-time intrusion detection for minimum 6000+ signatures.		
4	The IPS should be able to detect, respond to and alert any unauthorized activity. Product detects the attacks and the network misuse that represent risk to the customer.		
5	NIDS shall be able to detect incidents that originate from inside the network perimeter as well as from outside the network perimeter and shall be able to take action on the basis of configured policies.		
6	Support at least 25000+ or more signatures with online download support of newer signatures.		

7	The proposed system should automatically update the attack signatures database from a central database server		
8	The proposed system should be able to detect and block HTTP proxy both from Content filtering solution & also from IDP		
	Gateway Anti-Malware		
1	Gateway level Anti Malware solution should be an appliance based.		
2	The proposed system should scan for viruses even for downloads from HTTPS sites		
3	Proposed solution should be cloud based Anti-APT solution to scan for zero day malwares		
4	Embedded Anti Malware support. Should have option to automatically update the new virus pattern updates. Anti Malware should be supported for HTTP, HTTPS, FTP, POP3, SMTP, SMTPS (Port 465), SMTPTLS (Port 587), POP3. Anti Malware scanning should be signature based and should provide ZERO HOUR Anti Malware support.		
5	Gateway level Anti Malware should provide high-performance protection against viruses in SMTP, SMTPS (Port 465), SMTPTLS (Port 587), POP3, HTTP, HTTPS and FTP . It should block viruses and worms from penetrating into an organization's internal network through e-mail attachments, malicious Web pages, and files obtained through FTP.		
6	Virus gateway should provide real-time detection of viruses and malicious code at the gateway for IMAP SMTP, SMTPS (Port 465), SMTPTLS (Port 587), POP3, HTTP, HTTPS and FTP Internet .		
7	The proposed solution should be licensed per unit as against per user.		
	APT		
1	The Proposed solution should Provide advance protection to prevent zero day threats, ransomware and evolving malware		
2	The Proposed solution should Analyse executable programs and documents like Microsoft Office files, PDF files, JAR, DLL, PE		
3	This Proposed solution should examine compressed archives like gzip, tar, zip, rar and 7z Support for malicious files under Windows, Linux, Mac OS and Android Performs advanced memory analysis of executable programs to detect malicious files		
4	The Proposed solution should Provides threat analysis dashboard to provide insight of real time threats Dump and analyse network even when encrypted with SSL/TLS		
	VPN		
1	This feature should be easy to configure and use. Should have a support inbuilt for IPSEC VPNs, SSL VPN, PPTP, L2TP, VPN CLIENT pass through, should support DES, 3 DES and AES encryption, IKE certificate authentication , RSA secure ID & Vasco Token support		
2	The proposed SD WAN solution should provide complete threat protection, including firewall, network DLP, gateway anti malware, intrusion prevention system (IPS), URL Filtering and application control		
3	The proposed solution should be managed centrally		
4	Support for IPSec, L2TP, PPTP & SSL VPN.		
5	Support Encryption : DES, 3DES, AES, twofish, blowfish & serpent encryption		
6	Authentication support : Preshared Key, Digital Certificates.		
7	support for Automatic IKE (Internet Key Exchange) and IKEv2		
8	Supports IPSEC NAT traversal		
9	Supports Hash Algorithms – MD5, SHA1, SHA2.		
10	Should support for IPSEC and PPTP VPN pass through so that computers or subnets on your internal network can connect to a VPN gateway on the Internet		

	Logging and Reporting solution		
1	The proposed system should have integrated on-appliance reporting solution.		
2	The proposed system should provide individual users download & Upload data usage report.		
3	The proposed system should email daily group browsing reports to respective group heads in pdf format.		
4	The proposed system should provide user and IP address based reports.		
5	The proposed system should have options to create users with different access rights (E.g. users who can only view reports and not manage the system)		
6	The reporting solution of the proposed system should be able to provide detailed Audit log for auditing and tracking system		
7	Should support logging on the Next Generation Firewall appliance only and should not require additional Hardware or Software for Logging. It should provide various kinds of reports like virus reports, URL filtering reports, Top visited websites, Systems infected by Spywares, User or IP wise download for the day. It should have graphical reports of usages ISP wise, Application wise and IP wise.		
	Additional Point		
1	Self-Declaration for Local Supplier-Local Content/Make in India Certification from OEM/ Manufacture should be submitted/Uploaded as per Format of Annexure-II from MeitY Notification file No 1(10)/20217 CL-ES dated 6/12/2019. If the bidder fails to submit the same, the bidder shall be liable to be rejected/disqualified.		
2	The product shall have Indian Standard, IC3S/Common Criteria (provided by STQC in India common-criteria- certification-0) or Alternatively from International equivalents, NDPP or NSS or ICSALabs, at least one of them should be provided while bidding.		

5.34 Next Generation Firewall for Viewing Station

	Technical Specification	**Technical Compliance (Yes/No)**	**Remark**
	Hardware Specification		
1	Firewall should be ICSA Labs Certified		
2	Proposed solution should come from firewall appliance family which has more than 10 years of ICSA labs certification		
3	Minimum internal storage 500 GB SSD for detailed graphical Logs & Reports on Appliance		
4	Appliance must have 4 GB RAM or Higher		
5	Proposed solution should have open standard multicore processor based architecture and not proprietary ASIC based architecture		
	Interface Requirement		
1	1 Ports of 1Gbps Copper		
2	2/3 x USB 2.0/3.0 port and 1 system console port (RJ45/MicroUSB/USB)		
	Performance Capacity		
1	Concurrent Sessions – 6350000 or Higher		
2	New Sessions/second – 120000 or Higher		

3	Firewall Throughput - 15 Gbps or Higher		
4	Threat Protection Throughput-1 Gbps or Higher		
5	VPN Throughput – 1 Gbps or Higher		
6	NGFW Throughput - 3 Gbps or Higher		
7	IPS Throughput - 3 Gbps or Higher		
8	Firewall IMIX Throughput - 5 Gbps or Higher		
	Next Generation Firewall Features		
1	The proposed system should have firewall with stateful packet filtering technology & must support one-to-one and dynamic user based NAT with a facility to create rules based on usernames, Source & Destination IP address, Hosts, network, IP Range		
2	The firewall of the proposed system should be based on a hardened OS, should be capable of delivering network protection services at all layers along with options of network gateway level anti virus, anti spam, intrusion detection and prevention, content filtering, multiple ISP load balancing, failover and VPN solutions.		
3	The firewall should be able to support deployment in Bridge mode, layer 3 transparent proxy mode		
4	The firewall of the proposed system should provide Predefined services based on port numbers and Layer 7 application and ability to create user-definable services which can be used to define firewall rules		
5	The firewall of the proposed system should support 802.1q based VLAN tagging to segregate devices logically		
6	The proposed solution should have option to configure firewall policies to block or allow rules based on Country based Geo Location		
7	The proposed solution must have control mechanism to perform policy based control for Application, shaping and visibility for Users, Groups, IP address & Network.		
8	The proposed solution should be able to detect & block known applications like P2P & IM.		
9	The proposed solution should provide guaranteed and burstable bandwidth for applications.		
10	Should have Role based and multi factor authorization for Administration		
11	The proposed solution should be able to detect & block known applications based on time schedule.		
12	The Proposed solution should have an option to provide complete policy enforcement and visibility of roaming users and should restrict the remote user from disabling it.		
13	The organization policy framework must be extended to the remote users and ideally it should control the Web and Application filter of remote user		
	URL Filtering & Web Protection		
1	Should support 85+ Web categories		
2	Should support blocking of category based HTTPS sites without having to provide the URL of the site to be blocked		
3	Should support HTTPS transparent proxy		
4	The proposed system should support browsing proxy and gateway mode simultaneously		
5	The proposed solution should block HTTPS URLs with complete path instead of only sites names		
6	The proposed solution should support regular expression in blocking of HTTPS sites		
7	Web based management through https and command line interface support		
	Application Filtering		
1	The proposed solution should support Application Filtering in the same appliance.		
2	The proposed solution should have inbuilt Application category database.		

3	The proposed solution should provide policy-based shaping by application for User, Group, IP address & Network.		
4	The proposed solution should be able to detect & block known applications like P2P & IM.		
5	The proposed solution should have 2500+ application database & 5000+ application signature		
6	The proposed solution must give reports based on username / IP address.		
	Intrusion Prevention System		
1	Intrusion Prevention system should be appliance based or integrated with the NGFW solution		
2	The proposed IPS system should have signature and anomaly base intrusion detection and prevention system		
3	The proposed system should have configuration options to prevent all the common DOS and DDOS attacks like syn flood, ICMP flood, UDP flood, Ping of death. Should have prevention option for more than 30 common attacks.		
4	The IPS should be able to detect, respond to and alert any unauthorized activity. Product detects the attacks and the network misuse that represent risk to the customer.		
5	NIDS shall be able to detect incidents that originate from inside the network perimeter as well as from outside the network perimeter and shall be able to take action on the basis of configured policies.		
6	Support at least 25000+ or more signatures with online download support of newer signatures.		
	Gateway Anti-Malware		
1	Gateway level Anti Malware solution should be an appliance based.		
2	The proposed system should scan for viruses even for downloads from HTTPS sites		
3	Proposed solution should be cloud based Anti-APT solution to scan for zero day malwares		
4	Embedded Anti Malware support. Should have option to automatically update the new virus pattern updates. Anti Malware should be supported for HTTP, HTTPS, FTP, POP3, SMTP, SMTPS (Port 465), SMTPTLS (Port 587), POP3. Anti Malware scanning should be signature based and should provide ZERO HOUR Anti Malware support.		
5	The proposed solution should be licensed per unit as against per user.		
	APT		
1	The Proposed solution should Provide advance protection to prevent zero day threats, ransomware and evolving malware		
2	The Proposed solution should Analyse executable programs and documents like Microsoft Office files, PDF files, JAR, DLL, PE		
	VPN		
1	This feature should be easy to configure and use. Should have a support inbuilt for IPSEC VPNs, SSL VPN, PPTP, L2TP, VPN CLIENT pass through, should support DES, 3 DES and AES encryption, IKE certificate authentication , RSA secure ID & Vasco Token support		
2	The proposed SD WAN solution should provide complete threat protection, including firewall, network DLP, gateway anti malware, intrusion prevention system (IPS), URL Filtering and application control		
3	The proposed solution should be managed centrally		
4	Support for IPSec, L2TP, PPTP & SSL VPN.		
5	Support Encryption : DES, 3DES, AES, twofish, blowfish & serpent encryption		
6	Authentication support : Preshared Key, Digital Certificates.		

7	support for Automatic IKE (Internet Key Exchange) and IKEv2		
8	Supports IPSEC NAT traversal		
9	Supports Hash Algorithms – MD5, SHA1, SHA2.		
10	Should support for IPSEC and PPTP VPN pass through so that computers or subnets on your internal network can connect to a VPN gateway on the Internet		
	Enterprise Cloud		
1	The proposed solution should have an integrated cloud security solution in appliance.		
2	The proposed solution should have option to download 32 and 64 bit Enterprise cloud clients.		
3	The proposed solution should have ISP failover for cloud client.		
4	The proposed solution should have DLP reporting for cloud client.		
5	The proposed solution should have URL filtering, App Filtering on cloud client.		
	Logging and Reporting solution		
1	The proposed system should have integrated on-appliance reporting solution.		
2	The proposed system should provide individual users Bandwidth data usage report.		
3	The proposed system should email daily group browsing reports to respective group heads in pdf format.		
4	The proposed system should provide user and IP address based reports.		
5	The proposed system should have options to create users with different access rights (E.g. users who can only view reports and not manage the system)		
6	Should support logging on the Next Generation Firewall appliance only and should not require additional Hardware or Software for Logging. It should provide various kinds of reports like virus reports, URL filtering reports, Top visited websites, Systems infected by Spywares, User or IP wise download for the day. It should have graphical reports of usages ISP wise, Application wise and IP wise.		
	Additional Point		
1	Self-Declaration for Local Supplier-Local Content/Make in India Certification from OEM/ Manufacture should be submitted/Uploaded as per Format of Annexure-II from MeitY Notification file No 1(10)/20217 CL-ES dated 6/12/2019. If the bidder fails to submit the same, the bidder shall be liable to be rejected/disqualified.		
2	The product shall have Indian Standard, IC3S/Common Criteria (provided by STQC in India common-criteria- certification-0) or Alternatively from International equivalents, NDPP or NSS or ICSALabs, at least one of them should be provided while bidding.		

5.35 Zero Day Network Threat Protection System

Sl. No.	Technical Specifications	Technical Compliance (Yes/No)	Remark
1	Solution must be a custom built on premise solution and must not be network perimeter security component part devices like UTM and NGFW and not be a CPU and chip based function.		

2	The proposed solution should have capabilities to configure files, IP, URLs and Domains to Black list or white list.		
3	The Proposed solution should provide correlated threat data such as: IP addresses, DNS domain names, URLs, Filenames, Process names, Windows Registry entries, File hashes, Malware detections and Malware families through a dashboard		
4	The proposed solution must be able to provide intelligence feed for malware information, threat profile and containment remediation recommendations where applicable.		
5	The proposed solution should be able to support XFF (X-Forwarded-For) to identify the IP Address of a host in a proxy/NAT environment.		
6	The proposed solution should have a built-in document vulnerabilities detection engine to assure analysis precision and analysis efficiency..		
7	The proposed solution should have virtual patching feature along with Indicators of Compromise build and sharing.		
8	Proposed solution should have 2 TB in RAID 1 of on box storage from day one with a scalability of 8 TB and should be able to run at least 30 parallel sandboxes images scalable up to 60 for analysis of payload		
9	Customized sandbox solution should support following operating systems (Windows 7, Win8/8.1, Win 10, Windows Server 2008, 2012, 2016 and 2019) and able to inspect threats for Linux, Mac & Mobile OS Malwares. Solution must have the capability to analyse large files more than 40 MB file size.		
10	Solution should support third part VA scanners (Qualys, Foundstone, Nessus) to fine tune the policies for zero day threat protection against vulnerabilities.		
11	The Solution must have inline sensor with capability of hardware based fail-open & Software Fail Open, which must allow to pass through uninterrupted.		
12	Solution should have inline inspection throughput of 1 Gbps for all kinds of real world , scalable to 5 Gbps in a single device, optionally if required must support Active-Active in HA or Active-Passive mode.		
13	Must have minimum 4 x 10G monitoring interface (with SFP - SR modules) and 4 X 1 GE with fail-open capability and latency on network inline device must be <60 microseconds.		
14	The solution must use prevention techniques and provide zero-day protection against worms, Trojans, spyware, key loggers, and other malware from penetrating the network.		
15	The solution must accurately detect intrusion attempts and discerns between the various types and risk levels including unauthorized access attempts, pre-attack probes, suspicious activity, vulnerability exploitation and zero-day attacks.		
16	The solution filter must support network action set such as Block (drop packet), Block (TCP Reset), Permit, Trust, Notify, Trace (Packet Capture), Rate Limit and Quarantine & must support signatures, protocol anomaly, vulnerabilities and anomaly filtering methods to detect attacks and malicious		

17	The solution must have filter categories for easy management: - Exploits, Identity Theft/Phishing, Reconnaissance, Security Policy, Spyware, Virus, Vulnerabilities, Network Equipment, Normalization, Peer to Peer, Internet Messaging, Streaming Media and must be able to control the known bad host such as spyware, botnet C2 server, spam and so on based on country of origin, exploit type and the reputation score.		
18	The solution must have Inline sensors with custom sandboxing for simulation and create IOC's on real time basis as per sandboxing analysis and revert back to sensors to block threats on real time.		
19	The proposed solution should be able to inspect the multi-protocol sessions to detect and flag the suspicious activity including suspicious file downloads through the web and internal infections.		
20	The proposed solution should be able to detect lateral movement (East-West) of the attack without installing agents on endpoint/server machines & support 100+ protocols for inspection like HTTP, FTP, SMTP, SNMP, IM ,IRC,DNS and P2P protocols Internal direction, SMB ,Database protocol (MySQL, MSSQL, Oracle) & should support to monitor from multiple segments like WAN, DMZ, Server Farm, Wi-Fi network, MPLS links etc.		
21	The Proposed solution should provide correlated threat data such as: IP addresses, DNS domain names, URLs, Filenames, Process names, Windows Registry entries, File hashes, Malware detections and Malware families through a portal		
22	The proposed solution should be able to provide customizable sandbox to fulfil Customer's environments and needs for both 32-bits and 64-bits OS.		
23	Solution must be capable of performing multiple file format analysis which includes but not limited to the following: LNK, Microsoft objects, pdf, exe files, compressed files, .chm, .swf, .jpg, .dll, .sys, .com, .hwp , .js, .jse, .ps1, .vbe, .vbs, .hta, cmd, .bat, .htm, .hta, .xdp and solution should have an built-in document vulnerabilities detection engine to assure analysis precision and analysis efficiency.		
24	The proposed solution must provide the capability to export network packet files and encrypted suspicious files for further investigation and solution should be able to detect known malwares before sending suspicious files to Sandbox for analysis.		
25	The proposed solution have the capability to performs tracking and analysis of virus downloads and suspicious files and solution should support exporting of analysis results such as C&C server IP and malicious domain listing.		
26	The proposed solution should have capability to include User-defined and context-derived passwords for protected archives.		
27	The proposed solution should have capabilities to configure separate notifications to the administrator or individuals based on specific events like, Sandbox detection, Black List and license events etc.		

28	The proposed solution should have an intuitive Dashboard that offers real time threat visibility and reports with (but not limited to) HTML/CSV/PDF formats and provide the flexibility to generate on-demand reports in daily/weekly/monthly/yearly or specific range (by day and time)		
29	The proposed solution should support logging of important parameters like Source IP, Destination IP, ports, protocol, Domain, time stamp etc. of the attacks sessions.		
30	The proposed solution should have the flexibility to provides customizable dashboard and solution should have the option to provide Investigative dashboard that is capable of displaying correlated graphical data that is based on link-graph, geo-map, chart , tree-map/pivot table and solution should be able to corelate local APT attacks with Golbal historical APT attacks..		
31	Should have minimum 25 million legitimate concurrent Sessions and 400,000 new Connections per second from day one & should have at least security effectiveness rate 99 % as per 2017 NSS Labs Breach Prevention report		
32	The Proposed solution should be able to generate out of box reports to highlight Infections, C&C behavior, Lateral Movement, Asset and data discovery and Exfiltration		
33	Solution must be able to share threat intelligence with integrated third-party vendor products or services such as SIEM systems.		
34	Solution must be able to connect to TAXII server for obtaining threat intelligence & must be able to act as a TAXII server and share threat intelligence to subscribed TAXII clients.		
35	Solution must be able to provide web-based API such as Restful API for sharing threat intelligence and integrating with security operation automations and sharable threat intelligence must include at least 4 types - IP, URL, domain and file checksum.		
36	Solution must allow admin to define custom threat intelligence including IP, URL, domain and file checksum, and deploy them to managed products / devices.		
37	Solution should allow admin to define custom threat intelligence by importing/exporting YARA rules and should allow users to define custom threat intelligence by importing/exporting STIX.		
38	Solution must have ability to export threat intelligence thru Data Exchange Layer (DXL) communication fabric that connects and optimizes security actions across multiple vendor products		
39	Solution should produce high fidelity threat detection and help SOC prioritize threat response and ability to go back in time by analyzing historical data and pin point patient 0.		
40	Should able to identify the point of entry of an attack, identify all the hosts that are infected of the same threat, identify all the hosts that have connected to the malicious site/CnC server and display in a single view the entire threat attack lifecycle.		

41	Solution must add additional context to the threat intelligence and analysis and alerts. It includes information about the threat actors and malware used and other indicators of compromise are included so you can search for the attackers in your environment.		
42	Number VMs should be consider :20		
43	Number of throughput should be consider: 4Gbps		

5.36 Next Generation Anti-Virus and Endpoint Detection & Response

Sl. No.	Specifications	Technical Compliance (Yes/No)	Remark
	Mandatory Specifications		
	The solution should include all components to comply below requirement. If any third-party hardware software database is required should be included.		
1	The footprint of the overall solution at the endpoint must be very light in terms of Memory, Hard disk usage and CPU. The entire endpoint software should be single agent software deployed with all features and functions of NGAV, EDR, Threat Hunting, IT Hygiene, Vulnerability Management and Device Control and do not require any agent or software update to enable or disable these modules. Agent footprint must be under 70MB memory and 1-2% CPU.		
2	The proposed solution should be in Leaders Quadrant of Gartner End Point Protection Platform and Forester Wave EDR for last two years.		
3	Solution should be managed form a on premise server or cloud. Should provide 99.9 % of uptime all components should be in HA mode both DC and DR including all hardware, software & database components required to protect both on premise and roaming users.		
4	Solution should protect from all (known, unknown, zero day, ransomware and fileless attacks) if any APT or sandboxing solution required to protect should be included in HA		
5	The proposed solution should provide protection and management of Windows, Linux, container, Mac endpoints including Android and IOS. Protect all workloads on-premise or on cloud platform such as (Amazon Web Services EC2, Google Cloud Platform and Azure) from the same management console. Agent installation and update should not require any reboot.		
6	Container support (OCI) by capturing container activity and metadata, and solution must provide full visibility into containers and add runtime security		
7	Solution must continuously monitor endpoint activities for both on premise and roaming uses, captures events and forensic details of interest in near real time.		
8	Solution must provide post-execution behaviour based detection and prevention based on Indicator of Attack (IOA) mapped against the MITRE ATT&CK framework		

9	Endpoint agent must support policy controlled automated agent version update N-1, N-2.		
10	Solution should provide threat hunting platform with instant results. Threat hunting activity must not impact CPU or memory of system at all i.e. no increase in CPU and memory of managed endpoint during hunting activity at one system or all endpoints at enterprise. It should not be based on network sweeps or endpoint scans. OEM's should specify time required to hunt vulnerable application version, hash or vulnerability organisation wide(all assets online, offline & roaming).		
11	Proposed solution should capture telemetric data to provide threat hunting capabilities for forensic artefacts in real-time and for historical search in less than a minute, even for endpoints offline or out of corporate network without crawling endpoints. * Local IP and Public IP of endpoint had communicated in last 7 days. * User logon activities (login and logoff time with user name) for Last 7 days. * All Process & Service execution including admin tools and CMD commands with process id user details for last 7 days. * All PowerShell Activities on endpoint for last 7 days. * Unique executable written on endpoint. * Suspicious File Activities (Zip, RAR & Scripts written). * Files Written to Removeable Media * Manual Registry Addition. * Scheduled Tasks Registered and Firewall Rules Set on endpoint. * DNS request & Network connection with Port Number made from endpoint with detailed command line & file name for min last 7 days. * Details of Network Listening ports on endpoint with file name and command line. *Should be able to see network connections by Country or External IP's connected to. * List of Usernames or Systems where remote logins have taken place. This can quickly identify suspicious behaviour by user account or systems.		
12	The administrator should be able to find in real time and historical search capabilities in less than a minute where a specific file (by hash) has executed, with which file name, in which process and at what exact time. First time & last time executed on which host with time. The solution should not crawl endpoints and provide details even for machines offline or out of corporate network.		
13	The Administrator should be able to see a list of Usernames or Systems where remote logins have taken place. This can quickly identify suspicious behaviour by user account or systems.		
14	The Administrator should be able to see the executable run from a temporary directory or recycle bin on all systems in their environment.		
15	EDR solution should provide risk assessment dashboard for endpoints with assessment score for both OS and Agent configuration with details of checks failed to proactively avoid configuration issues.		
16	Solution should provide full remote remediation capabilities from the management console even for roaming users on public network (eg. delete registry, file, push or pull file/package, execute commands and powershell script, etc)		

17	Solution must offer memory protection (e.g. ASLR, structured exception handling overwrite protection, null page protection, heap spray preallocation, etc.)		
18	The proposed solution should be able to track more than 130+ adversary groups. The details of adversary and TTP should be available in the management portal along with their other well- known names in the community like APT28 is also known as Fancy Bear, Sofacy, Tsar Team, Sednit.		
19	If detection belong to known adversary, solution should provide threat actor with TTP's to proactively investigate and tune protection policies.		
20	The Management Portal should provide capability to filter threat actor information based on Origin, Target Country, Target Industry & Actor Motivations.		
21	Solution must be able to remotely contain an endpoint using mechanism not related to the operating system firewall. Containment must persist after a reboot.		
22	The EPP solution must provide visibility of * When the local admin passwords last reset happened. * User logging as Domain Administrator or with Local Admin Rights. * User Login Interactive, Terminal service and Service Account. * Assets visibility of host with no endpoint security agent. * Rouge devices in network (printer, camera's, network devices) in network. * Application Inventory with hash and version organisation wide or specific endpoint		
23	Proposed OEM should adhere compliance to SOC II, PCI DSS, HIPAA/HITECH, SOX and/or other regulatory frameworks		
24	Solution should include 24/7 managed threat hunting as an additional service from the OEM. Threat hunters should have minimum 8+ years of threat hunting experience.		
25	Proposed OEM should have inhouse IR, breach investigation, Red Team, Blue Team services.		

5.37 Privileged Access Management Solution

A	**Single - Sign On and Authentication Models**	**Technical Compliance (Yes/No)**	**Remark**
1	The solution should be able to create seamless single sign-on for various technologies such as Operating Systems, Databases, Network and Security Devices.		
2	The solution should have a Generic Target System Connectors to enable one to uses this connector for non-standard devices etc		

3	The solution should be agentless i.e. does not require to install any agent on target devices		
4	The solution should support transparent connection to the target device, without seeing the password or typing it in as part of the connection		
5	The solution should support direct connections to windows, ssh, databases and other managed devices without having to use a jump server.		
6	The solution should have an inbuilt dual factor authentication for soft token, mobile OTP etc. Also it should have an inbuilt authentication for Bio-Metrics without having to acquire another biometric authentication server.		
7	The solution should be able to integrate with enterprise authentication methods e.g. multiple 3rd party authentication methods including LDAP, RADIUS and a built-in authentication mechanism		
8	The solution should also provide local authentication and all the security features as per best standards.		
9	The solution should provide flexibility **user/device wise** for local authentication or enterprise authentication		
10	The solution should support an application integration framework for web based as well as .exe based applications. There should be strong out of the box support including ease of integration with any third party connectors.		
11	The solution should provide a method for creating new connectors with minimal intervention required from OEM.		
12	The solution should provide multi-tenancy feature whereby the entire operations can be carried out within a tenant or line of business.		
13	The solution should provide multi-domain feature whereby the entire operations can operate in an distributed environment		
14	The solution should be able to handle multi-location architecture or distributed architecture with seamless integration at the User Level. For example: Multiple datacentre may have multiple secondary installations but the primary installation will also simultaneously work for all users and all locations		
B	**Shared Account Password Management**		
1	The solution shall perform password change options which is parameter driven		
2	The solution should set password options every x days, months, years and compliance options via the use of a policy		
3	The solution should be able to manage SSH Keys		

4	For Linux/Unix servers, the solution should have an option to generate the SSH key pair directly from the tool.		
5	Ability to create exception policies for selected systems, applications and devices		
6	The solution should enable an administrator to define different password formation rules for target accounts on different target systems and supports the full character set that can be used for passwords on each target system.		
7	The solution enables an administrator to change a target-account password to a random value based on a manual trigger or automatic schedule.		
8	Allow single baseline policy across all systems, applications and devices (eg one single update to enforce baseline policy		
9	The solution should support changing a password or group of passwords according to a policy (time based or 'on-demand')		
10	Ability to generate 'One-time' passwords as an optional workflow		
11	Ability to send notifications via email or other delivery methods triggered by any type of activity		
12	Ability to send notification via email to the user requesting the password that checkout is complete		
13	All locally stored target-account passwords should encrypted using AES or similar encryption with at least 256 bit keys.		
14	The solution should automatically reconcile passwords that are detected 'out of sync' or lost without using external restore utilities		
15	The solution should have the ability to reconcile passwords manually, upon demand		
16	The solution should automatically verify , notify and report all passwords which are not in sync with PIM		
17	The solution should have the ability to automatically "check-out" after a specific time and "check-in" within a specified time.		
18	The solution should set unique random value anytime a password is changed. The password generated should be strong and should not generate a similar value for a long iteration.		
19	The tool allows secure printing of passwords in Pin Mailers. Lifecycle of printing and labelling of envelopes should be part of the module.		
20	Secured Vault platform - main password storage repository should be highly secured (built-in firewall, hardened machine, limited and controlled remote access etc.)		

21	The proposed solution should restrict the solution administrators from accessing or viewing passwords or approve password requests		
22	The solution should have the capability to seamlessly change the passwords for the large number of desktops. It should be able to handle floating IPs		
23	The solution should have provision for secure offline access of managed credentials in case of vault failure (break glass scenario)		
24	Offline access of managed credentials in case of vault failure should generate audit logs that are synced with the Vault once it's back online.		
25	The solution should have provision to allow authorized users to upload their sensitive/confidential files in the Vault for secured and encrypted storage.		
26	Files uploaded in Vault for secured and encrypted storage should be allowed to be shared between PAM users with an option to expire the share after defined period of time (in days).		
C	**Access Control**		
1	The solution should be able to restrict usage of critical commands over a SSH based console based on any combination of target account, group or target system and end-user.		
2	The solution should restrict privileged activities on a windows server (e.g. host to host jumps, cod/telnet access, application access, tab restrictions) from session initiated with PIM		
3	The solution should be able to restrict usage of critical commands on command line through SSH clients on any combination of target account, group or target system and end-user.		
4	The solution should be able to restrict usage of critical commands on tables for database access through SSH, SQL+(client/), front-end database utilities on any combination of target account, group or target system and end-user.		
5	The solution should provide for inbuilt database management utility to enable granular control on database access for Sql, my Sql, DB2, Oracle etc.		
6	The solution enables an administrator to restrict a group of commands using a library and define custom commands for any combination of target account, group or target system and end user.		
7	The solution should provide secure mechanism for blacklisting/whitelisting of commands for any combination of target account, group or target system and end user.		

8	The solution can restrict user-specific entitlements of administrators individually or by group or role.		
9	The solution should have workflow control built-in for critical administrative functions over SSH including databases (example user creation, password change etc) and should be able to request for approval on the fly for those commands which are critical.		
10	The solution can restrict target-account-specific entitlements of end users individually or by group or role.		
11	The solution can restrict end-user entitlements to target accounts through a workflow by days and times of day including critical command that can be fired.		
12	The solution should provide for a script manager to help in access controlling scripts and allow to run the scripts on multiple devices at the same time.		
13	System should be able to define critical commands for alerting & monitoring purpose and also ensure user confirmation (YES or NO) for critical commands over SSH.		
14	It should be possible to grant access to a managed asset using a specific method of access. For e.g. access to a SQL database ONLY through SQL Management Studio.		
D	**Privileged Session Management and Log Management**		
1	The solution should be able to support a session recording on any session initiated via PIM solution including servers, network devices, databases and virtualized environments.		
2	The solution should be able to **log commands** for all commands fired over SSH Session and for database access through ssh, sql+		
3	The solution should be able to log/search text commands for all sessions of database even through the third party utilities		
4	The solution should be able to log/search text commands for all sessions on RDP		
5	The solutions should support selective option for enabling session based recording on any combination of target account, group or target system and end-user.		
6	All logs created by the solution should be tamper proof and should have legal hold		

7	The solution logs all administrator and end-user activity, including successful and failed access attempts and associated session data (date, time, IP address. Machine address, BIOS No and so on). The tool can generate — on-demand or according to an administrator-defined schedule — reports showing user activity filtered by an administrator, end user or user group.		
8	The tool can restrict access to different reports by administrator, group or role.		
9	The tool generates reports in at least the following formats: HTML, CSV and PDF		
10	System should be able to define critical commands for alerting & monitoring purpose through SMS or Email alerts		
11	The solution should provide separate logs for commands and session recordings. Session recordings should be available in image/ video based formats		
12	The session recording should be SMART to help jump to the right session through the text logs		
13	Secure and tamper-proof storage for audit records, policies, entitlements, privileged credentials, recordings etc.		
14	The proposed solution shall cater for live monitoring of sessions and manual termination of sessions when necessary		
15	The proposed solution shall allow a blacklist of SQL commands that will be excluded from audit records during the session recording. All other commands will be included.		
16	The proposed solution shall enable users to connect securely to remote machines through the tool from their own workstations using all types of accounts, including accounts that are not managed by the privileged account management solution.		
17	The proposed solution shall allow configuration at platform level to allow selective recording of specific device.		
18	The proposed solution shall allow specific commands to be executed for RDP connections (e.g. Start the connection by launching a dedicated program on the target machine without exposing the desktop or any other executables).		
19	The proposed solution shall support correlated and unified auditing for shared and privileged account management and activity.		
21	The proposed system shall support full colour and resolution video recording.		
22	The proposed system shall support video session compression with no impact on video quality.		

23	The solution should provide a secure method to facilitate access to managed asset in case of PAM failure for identified users (local vault)		
24	These managed assets accessed in offline mode should generate access logs that are synced with the PAM solution once it's back online.		
25	The solution should provide an option to supervise privileged user activity with real time session shadowing capability.		
E	**PIM Security**		
1	The solutions should use minimum FIPS 140-2 validated cryptography for all data encryption.		
2	The Solution should be TLS 1.2 and SHA-2 compliant for PCI-DSS compliance		
3	All communication between system components, including components residing on the same server should be encrypted.		
4	All communication between the client PC and the target server should be completely encrypted using secured gateway. (Example: a telnet session is encrypted from the client PC through the secured gateway)		
5	The Administrator user cannot see the data (passwords) that are controlled by the solution.		
6	Secured platform - main password storage repository/Vault should be highly secured (hardened machine, limited and controlled remote access etc.).		
7	The solution should secure master data, records, entitlement, policy data and other credentials in tamper proof storage container.		
8	The solution should store Password and SSH keys safekeeping in the certified vault (minimum AES 256-bit encryption)		
9	The solution should not require direct third party access to PAM Database		
10	The solution should support common protocols to connect to PAM servers to ensure the best interoperability with environments.		
F	**PIM Administration**		
1	The solution should have central administration web based console for unified administration.		
2	The tool uses Active Directory/LDAP as an identity store for administrators and end users.		
3	The tool enables an administrator to define groups (or similar container objects) of administrators and end users.		
4	The tool enables an administrator to add an administrator or end user to more than one group or to add a group to more than one supergroup.		

5	The tool enables an administrator to define a hierarchy of roles without limit.		
6	Administrative configurations (e.g. configuration of user matrix) shall be accessible via a separate client where client access is controlled by IP address.		
7	Important configuration changes in the solutions (example changes to masters) should be based on at least 5 level workflow approval process and logged accordingly		
8	The tool should have a provision to enable maker-checker configuration for critical administrative actions. For e.g. new user creation, on-demand password change etc.		
9	Segregation of Duties - The Administrator user cannot view the data (passwords) that are controlled by other teams/working groups (UNIX, Oracle etc.).		
10	The solution should provide for self service portal for users and devices for ease of on boarding both users and devices.		
11	All administrative task should be done LOB wise i.e. Line of Business Wise		
12	All administrative tasks/actions should be logged along with change in configuration value i.e. value before change made and after the change made.		
13	The solution should have Auto-Onboarding Feature for both User and Devices without having to do any manual activity.		
G	**System Architecture**		
1	The solution architecture should be highly scalable both vertically as well as horizontally.		
2	The proposed solution shall provide multi-tier architecture where the database and application level is separated.		
3	The solution should work at the network layer instead through a jump server. This will have achieve large number of sessions.		
4	The proposed solution shall provide scalability where it is not limited by the hardware. Also the solution shall provide modular design for capacity planning and scalability metrics.		
5	The proposed solution shall have the ability to support multiple mirrored systems at offsite Disaster Recovery Facilities across different data centre locations.		
6	The proposed solution shall have built-in options for backup or integration with existing backup solutions		
7	The proposed solution shall handle loss of connectivity to the centralized password management solution automatically.		

8	The proposed solution shall not require any network topology changes in order to ensure all privileged sessions are controlled by the solution.		
9	The proposed solution shall support distributed network architecture where different segments need to be supported from a central location.		
10	The proposed solution shall support both client based (in the case where browser is not available) as well as browser based administration		
11	The proposed solution should be 100% agentless that includes password storage, password management and session recording features.		
12	The solution must support parallel execution of password resets for multiple concurrent requests.		
13	The solution should provide fully failover from a single active instance to a backup/standby instance with a fully replicated repository		
14	The solution should support multiple active instances with load balancing and fully automatic failover to another active instance		
15	The solution if required should be available to install on a virtual sever		
16	The system should be highly available (24x7x365) and redundant from a hardware failure, application failure, data failure, and or catastrophic failure. Uptime availability should be 99.99% per calendar month.		
17	The solution should have an ability to have direct connection to target device as well as using secured gateway channel.		
18	Solution should not require CAL license to integrate PAM		
19	Solution should support hybrid architecture		
H	**Out of box Integration**		
1	Ability to integrate with enterprise authentication methods e.g. multiple 3rd party authentication methods including AD, LDAP, Windows SSO, PKI, RADIUS and a built-in authentication mechanism.		
2	Ability to integrate with Bio-Metric Solutions		
3	Ability to integrate with Hard and Soft token solutions		
4	Ability to integrate with ticketing systems.		
5	Ability to integrate with Automation software for enhancing productivity in the data center		
6	The proposed solution supports integration with the Hardware Security Module (HSM) devices to store the encryption keys.		
I	**Ticketing System integration**		
1	The solution can force the requestor of password / session to provide a reason, including a service desk incident ticket number, for the request.		

2	The solution can communicate with a workflow engine to verify an incident ticket number cited in the end user's request.		
3	The solution provides the capability to enable end users to retrieve (or reset) a target-system password only after approval by a designated approver (to allow dual control). Approval criteria can be based on any combination of target account, group or target system and end-user identity, group or role, as well as contextual information such as day of the week or time of day.		
4	Ability to enforce ticketing integration as well as approval workflow for specific ticket types (e.g. change/incident ticket)		
5	Inbuilt ticketing system with 5 level workflow approval with ticket level validation, risk and impact assessments as per LOB wise, Service type and user type. This ticketing system to help in creating a work order on an executer, who will then request for the access through the request workflow with this valid ticket		
J	**SIEM Integration**		
1	The solution should be able to integrate with leading SIEM Solutions.		
2	The solution should be able to integrated with applications like VA Systems, performance monitoring applications to eliminate hard coded passwords		
K	**Application Password Management (Hard-Coded Password Management)**		
1	The solution should have an ability to eliminate, manage and protect privileged credentials in applications, scripts, configuration files etc.		
2	The solution should be able to authenticate and trust the application requesting the privileged password based on various authentication methods		
3	Application Servers Support - The product should support removing static hard coded passwords from Data Sources in Application Servers. Please elaborate.		
L	**Auto Discovery of Privileged Accounts**		
1	The solution should be able to perform auto discovery of privileged accounts on target systems and perform two way reconciliation.		
2	The solution should provide feature for user governance on the target devices i.e. autodetect users and schedule a governance workflow and user certification process with adequate review process.		
3	Map privileged and personal accounts on various target systems		

4	Ability to quickly identify all non-built-in local administrator accounts in your environment (flag possible 'backdoor' accounts)		
5	Ability to quickly identify private and public SSH keys, including orphaned SSH keys, on Unix/Linux machines, extracts key related data and ascertain the status of each key		
M	**Notification Engine**		
1	The solution should have capability to provide alerts and notification for critical PIM events over SMS & Email		
2	The solution should have capability to provide alerts and notification for all administration/configuration activities over SMS & Email		
3	Customizable notification for command executed on SSH and Telnet based devices		
4	Customizable notification for command/Process executed on Windows		
5	Notification on target being access on criteria like Line of Business or Groups		
6	Solution should have threat analytics and customised reporting capabilities		
N	**Solution Workflow**		
1	The solution should have inbuilt workflow to manage		
2	Electronic Approval based Password Retrieval		
3	Onetime access / Time Based / Permanent Access		
4	5 level approval workflow with E-mail and SMS notification with delegation rules		
5	Ability to provide for delegation at all levels in the workflow		
6	Mobile device support - ability to send a request to access a password, approve the request and retrieve the password, all from a hand-held mobile device e.g. smart phones		
7	Supports a workflow approval process that is flexible to assign multiple level of approvers based on product or model (i.e. require 2 or more approvals before access is allowed).		
8	Supports a workflow approval process that requires approvers to be in sequence before final approval is granted.		
9	Supports a workflow approval process that requires approvers to be in sequence before final approval is granted.		
O	**Dashboard & Reporting**		
1	Dashboard Capabilities should included real-time view of activities performed by the administrators		
2	The system shall have the ability to run all reports by frequency, on-demand and schedule.		

3	The solution should provide detailed and scheduled reporting with the following basic report sets Entitlements Reports, User's activities, Privileged Accounts inventory and Activities log		
4	The solution should have ability to report on all system administrative changes performed by PIM Administrators with relevant auditable records		
5	The solution should be able to report password lockouts (failure logon attempts)		
6	Ability to report password checkouts on systems and users requesting passwords		
7	Ability to report password lockouts (failure logon attempts)		
8	Ability to report on password change following verification process		
9	Ability to report on password status		
10	Reports should be customizable		
11	Audit data can be exported for use for any BI Tool		
12	Reports shall be automatically distributed by email		
13	Access to audit reports (and report configuration) shall be restricted to "auditor" end-users		
14	Ability to replay actual session recordings for forensic analysis		
15	The recorded session should be compressed and not take much space on storage and only active session has to be monitored		
16	Dashboard - for at a glance critical events and password policies. *Describe your dashboard capabilities*		
P	**Brand and Technology**		
1	OEM Should have 24*7 support		
2	The Solution must be a leading, mature, internationally recognized and widely used brand that has been in existence for at least 10 years.		
Q	**Additional Functions**		
1	Access Management •The Solution should allows an end user/bot to use the command line/tools like MobaXterm, SecureCRT to not only authenticate a user in PAM solution but also establish a connection to any *nix target device.		
2	Architecture •Should include an enterprise version which will be highly scalable to support the High Availability at both DC and DR sites.		

3	Architecture •The solution should be scalable to be configured as Active-Passive from DC to DR using its auto failover technique. •The solution should have the ability to support DR in multiple geographical locations and networks.		
4	The module should enable the admin to take remote connection of user endpoint without the need to possess local password or without using any third party.		
5	The solution should have End Point Privilege Management and Threat Analytics.		

5.38 SECURITY INFORMATION & EVENT MANAGEMENT(SIEM)

Sl. No.	SIEM Details		
1	The solution should be able to collect logs from different infrastructure components such as Servers, Firewalls, Databases, Applications.	**Technical Compliance (Yes/No)**	**Remark**
2	The solution should normalise the logs to collect insights from the logs		
3	The proposed solution should have connectors to support the listed devices/ applications, wherever required the vendor should develop customized connectors at no extra cost		
4	The Solution should support collectors at separate locations.		
5	The user interface to monitor and investigate events from the SIEM tool should be interactive and should provide capabilities necessary for further analysis		
6	The proposed solution should be configurable, manageable, and should have ability to be monitored through a centralized management console		
7	The solution should have ability to perform trend analysis basis the historical data collected.		
8	The solution should have ability to do full-text search on any field in the indexed data		
9	Solution should enable the easy customizable dashboards and customizable dashboards based on various visualizations		
10	Solution should anticipate likely threats to the customer both from outside as well as arising from customer’s internal infrastructure.		

11	The solution should provide an inventory solution through collected information		
12	Vendor should have capabilities to detect anomalies such as brute force, command injections, indicators		
13	Solution should collect existing logs from security controls such as firewalls , IPS devices , to detect targeted attacks.		
14	The solution should have capabilities to detect any compromises by linking related alerts collected together over a period of time.		
15	Solution should have capabilities to correlate alerts between sources & destination Ips to find similar or colluding threat signals.		
16	Solution should have detection models to find out threats sources are linked to the same attacker by grouping alerts with common characteristics like time, day location, target asset profiles etc.		
17	In addition to the advanced analytics capabilities solution should have capabilities to define rules on event logs captured from various sources to detect suspicious activities Examples		
	• Failed login attempts		
	• Vendor logins from unauthorized subnets		
	• Vertical & Horizontal port scans		
	• from blacklisted Ips		
18	Solution should support criticality levels of alerts from a number of security products including Firewalls, Routers ,AV etc.		
19	The proposed solution should support collection of events through customization of connectors or similar integration for the assets that are not natively supported		
20	The proposed solution should be able to collect data from new devices added into the environment, without any disruption to the ongoing data collection.		
21	The proposed solution should have connectors to support listed devices/ applications, wherever required the vendor should develop customized connectors.		
22	All logs transferred to SIEM should be Authenticated (timestamped across multiple time zones) encrypted and compressed before transmission.		
23	The proposed solution should support log collection from all major operating systems and their versions but not limited to Windows, Linux, AIX, Solaris etc.		
24	The collectors should be able to store/retain both normalized & raw data for forensic purposes		
25	The proposed solution should have capabilities to store the event data in its original format in the central log storage		

26	The proposed system shall be able to capture all details in raw log, events and alerts and normalize them into a standard format for easy comprehension.		
27	The proposed solution should support multiple log collection protocols.		
28	The proposed solution should prevent tampering of any type of logs and log any attempts to tamper logs. It must provide encrypted transmission of log data to the log management.		
29	The proposed solution (SIEM) should be able to perform the correlations between different logs.		
30	Events should be presented in a manner that is independent of device specific syntax and easy to understand for all users		
31	Log Retention should be customizable as per the customer requirement		
32	The solution should be able to parse logs generated by custom developed applications.		
33	The solution should be able to send notification over multiple channels		
34	The solution should be able to integrate with third party threat intelligence sources over APIs to enrich events and cases		
35	The solution should allow to create custom visualizations and graphs as per customer requirement		
36	The solution should allow access to the raw logs for investigation and RCA activities		
37	The solution should be able to export dashboards as pdf reports.		
38	The solution should have User management module for authentication and authorization		
39	The proposed solution should support log collection, correlation and alerts for the number of devices /applications		
40	The proposed solution must ensure all the system components continue to operate when any other part of the system fails or loses connectivity.		
41	The proposed solution must automate internal health checks and notify the user in case of problems.		
42	The proposed solutions should be able to collect data from new devices added into the environment, without any disruption to the ongoing data collection.		
43	The proposed solution should have connectors to support all the devices/applications of all project landscape described in this RFP.		
44	The proposed solution should be able to continue to collect log data during database backup, de-fragmentation and other management scenarios, without any disruption to service		

45	The proposed solution should provide options to load balance incoming logs to multiple collector instances.		
46	The proposed solution should support log collection from all operating systems and their versions including but not limited to Windows, Unix, Linux, etc.		
47	The proposed solution should be able to store/retain both the log meta data and the original raw message of the event log for forensic purposes.		
48	The proposed solution should allow the creation of an unlimited number of new correlation rules		
49	The proposed solution should be able to integrate with security and threat intelligence feeds data feeds (i.e. geographic mapping, known botnet channels, known hostile networks, etc.) for the purpose of correlating events. These data feeds should be updated automatically by the proposed solution.		
50	The proposed solution should be able to parse and correlate multi line logs		
51	Events should be presented in a manner that is independent of device specific syntax and easy to understand for all users		
52	The dashboard should show the status of all the tools deployed as part of the SIEM		
53	It should be possible to categorize events while archiving for example, events for network devices, antivirus, servers etc.		
54	The Dashboard design for the proposed solution should be editable on an ad hoc basis as per the individual user need		
55	The proposed solution should allow applying filters and sorting to query results.		
56	The proposed solution should generate alerts on e-mail notifications for all critical/high risk alerts triggered from SIEM		
57	The proposed solution should have the ability to perform free text searches for events, incidents, rules and other parameters.		
58	The proposed system should identify the originating system details while capturing event data.		
59	The proposed solution should be able to store both normalized and RAW logs		
60	The Solution should have its own integrated case management to analyse the alerts.		
61	The solution should be able to send notification over multiple channels integration such as slack, teams, telegram.		
62	The solution should be able to categories the events based on the mitre attack framework.		
63	Solution should enable easy customizable dashboards visualizations:		
	· Bar chart		

	· Pie		
	· Donut		
	· Area Chart		
	· Line Chart		

5.39 Threat Intelligence Management

Sl. No.	Minimum Specifications or better	Compliance (Yes / No)	Remarks
1	Provider offers an agent-free product, requiring no software of any kind to be installed, and is fully manageable via a web-browser through a web-based administration console		
2	Provider offers integration with third-party products via an open REST-based API, with "out-the-box" integration for various security analytics, network and infrastructure, orchestration and automation, and threat intelligence platforms, accomplished via public/private API keys and oauth2 endpoints		
3	Provider offers threat data fully integrated across all threat intelligence capabilities, in addition to full integration with first-party endpoint security detection capabilities		
4	Provider derives threat intelligence collection from multiple sources, to include but not limited to, data collected across 20-30 million globally deployed sensors in over 180 countries collecting at least 3.5 trillion threat intelligence events per week, 100,000 hours of provider serviced incident response (IR) engagements per year, 400,000+ unique malware samples a day, deep and dark web chatroom and forums, deep and dark web marketplaces, network telemetry, and the surface web		
5	Provider offers an indicator-of-compromise database covering at least 14 IOC data-types, to include but not limited to sha256, sha1, md5, IP address, domain, URL, mutex, and bitcoin addresses, automatically generated from the data collected across 20-30 million globally deployed sensors in over 180 countries collecting at least 500 billion threat intelligence events per day		
6	Provider includes context for indicator-of-compromise with attribution to malware family, threat actor, cyber kill chain mapping, MITRE ATT&CK framework mapping, finished intelligence (FINTEL) reporting, threat type, and targeted industry.		
7	Provider offers confidence level assessment for every indicator-of-compromise		
8	Provider offers integrated ability to view related indicators with no more than one-click in the UI		
9	Provider offers various filtering options for indicator-of-compromise (IOC), in particular the IOC type, confidence level, malware family, threat actor, and threat target		
10	Provider offers the ability to visualize indicator-of-compromise (IOC) relationships between multiple IOCs, threat actors, intelligence reports and, if applicable, first-party endpoint security product detections		
11	Provider offers a comprehensive threat actor profile database, tracking over 140 publicly named nation state, e-crime, and hacktivist threat actors while mapping tactics, techniques, and procedures to the cyber kill chain while enumerating the threat actors origin, last known activity, target nations, and target industries		

12	Provider attributes e-crime threat actor tactics, techniques, and procedures to services used, services offered, customers, victims, crimes, monetization methods, technical tradecraft, and marketing		
13	Provider offers various filtering options for the threat actor profile database, in particular the ability to filter for origin, target country, target industry, and threat actor motivation		
14	Provider offers ability to submit file samples for detonation in any combination of Windows 7 32-bit, Windows 7 64-bit, Windows 10 64-bit, Ubuntu Linux 64-bit, and Android sandbox environments for static and dynamic analysis, to determine the behaviors indicated when the sample is detonated, with analysis including threat actor attribution and integration with a comprehensive threat actor profile database, finished intelligence (FINTEL) reporting, indicator-of-compromise database, MITRE ATT&CK framework mapping, and string comparison against providers malware database comprised of over 1.3 billion samples		
15	Provider sandbox offers the ability to detonate PE files (.exe, .scr, .pif, .dll, .com, .cpl, etc.), Office (.doc, .docx, .ppt, pptx, .ppsx, .xls, .xlsx, .rtf, .pub), PDF, APK, executable JAR, Windows Script Component (.sct), Windows Shortcut (.lnk), Windows Help (.chm), HTML Application (.hta), Windows Script File (*.wsf), Javascript (.js), Visual Basic (*.vbs, *.vbe), Shockwave Flash (.swf), Perl (.pl), Powershell (.ps1, .psd1, .psm1), Scalable Vector Graphics (.svg), Python (.py) and Perl (.pl) scripts, Linux ELF executables, MIME RFC 822 (*.eml) and Outlook *.msg files, and both unprotected and password protected ace, arj, 7z, bzip2, gzip2, iso, rar, rev, tar, wim, xz, and zip archive files		
16	Providers sandbox enriches any detonation with additional context from internal intelligence data sources and malware repository		
17	Provider sandbox is capable of being fully automated via an open REST-based API		
18	Provider sandbox is capable of being integrated with first-party endpoint security product, automating the delivery, detonation, and analysis of quarantined executable files		
19	Provider offers manual, human-based malware forensics and analysis conducted on customer submitted samples on an ad-hoc basis		
20	Provider maintain a searchable repository of indexed malware containing no less than 1.9 billion samples including binaries, macros, document files, and other file types		
21	Provider offers ability to identify malware with code reuse and string similarity through YARA rule hunting, and ASCII, WIDE, and HEX string searching against providers malware database containing 1.9 billion samples		
22	Provider offers ability to be alerted when new malware samples matching specific YARA hunts are added to providers malware database		
23	Provider offers web-browser plug-in supporting customer open source (OSINT) data enrichment and correlation by scraping indicators of compromise from the surface web and in-browser documents, to include PDF documents, matching the data up against provider threat intelligence. Supported scrapable indicators of compromise include, domain, IP address, URL, sha256 file hash, sha1 file hash, md5 file hash, and Bitcoin addresses		
24	Provider offers attribution of alerts to known threat actors		
25	Provider offers Continuous Monitoring by Human Analysts		
26	Provider offers detailed information and descriptions of malware families		

27	Provider offers in-depth analysis and reporting on threat actor trends		
28	Provider offers on-demand analysis of IP addresses and domains		
29	Provider offers threat intelligence collected from over 100,000 hours of provider serviced incident response (IR) work per year		
30	Provider offers threat intelligence collected from over 400,000 unique malware samples a day		
31	Provider leverages graph technology for storing and retrieving data from databases, capturing individual nodes with freeform properties, and potential complex relationships between nodes, and connecting these nodes via vertices for executing queries supporting the understanding of patterns and connections between disparate data types		
32	OEM should be running their business operations in India for last 4 years and must have office based in India for atleast last 4 years		
33	The proposed OEM Threat Intelligence solution should be positioned as leaders in latest Forrester Wave Intelligence Services analyst report		

5.40 VAPT Certification & STQC Audit for DC for every year

Sl. No.	VAPT Certification & STQC Audit for DC for every year	Technical Compliance (Yes/ No)	Remark
1	Security Testing (including penetration and vulnerability test): Security test shall be conducted to demonstrate security requirements at network layer and software applications		
2	Components shall pass vulnerability and penetration testing for rollout of each phase		
3	Components shall also pass web application security testing for portal, mobile app, and other systems.		
4	Security testing shall be carried out for exact same environment/architecture that shall be set up for go-live		
5	Penetration test shall be carried out periodically and vulnerability analysis shall be carried half-yearly during maintenance phase		
6	For all applications hosted on-cloud or hosted on premises, the security testing shall be a mandatory requirement.		

5.41 INTEGRATED COMMAND AND CONTROL(ICCC) ROOM INTERIOR

Technical Specification for Control Room Interior and Control Desk	Technical Compliance (Yes/No)	Remark

System Integrator / Contractor to ensure that the control room interior solution provider has all these certificates / reports prior to tender RFP release date, and these certificates / test reports must be submitted along with the bid. These certificates are mandatory to ensure that the solution meets the desired functionality & norms therefore, general compliance / self-compliance shall be deemed unacceptable.			
Sr. No.	**Specification**		
1.	The purpose of this document is to define the specifications of control room interior and control desk.		
1.1	**Scope of Work:** The scope of the project includes designing; engineering, supply & installation of 24X7 mission critical control centre interiors. Being a project of national repute this state-of-the-art facility & all its components like ceiling, flooring, paneling, glass partitions, control desks, ceiling light & luminaire's electrical etc. must look integrated and therefore it shall be treated as a part of one single solution i.e., Control room interior solution. Main bidder to submit MAF (Manufacturer's Authorization Form) from one professional control room interior solution. To ensure an integrated solution, to qualify as per the international control room design & safety norms; main bidder shall bring one single professional control room interior solution provider on board with an experience of designing, manufacturing and installing at least twenty control room interiors along with control desk. Corresponding purchase orders/work orders and their appreciation/completion letters to be submitted along with the bid.		
1.2	The Control Room Interior Solution Provider shall have experience of supplying below products in any one year out of last seven financial years to qualify: -		
	a) Acoustic Modular Metal Paneling / Partition – minimum 300 Sq. Meter		
	b) Acoustic Modular Metal False Ceiling - minimum 300 Sq. Meter		
	c) Acoustic laminate/carpet flooring – minimum 300 Sq. Meter		
	d) At least 50 control desk modules with modular removable Polyurethane Edge.		
1.3	It is mandatory for the main bidder that the control room interior solution provider supplies all elements & executes all the activities at site like ceiling, flooring, control desks, paneling, partitions & illumination to avoid interface & quality related issues.		

1.4	The critical components of the control room i.e., designer metal ceiling, carpet/laminated flooring, modular metal wall paneling/partitions shall not emit formaldehydes, TVOC beyond permissible limits i.e. 9 µg/m^3, 0.22 mg/m^3 respectively. This is to ensure healthier air quality for the operators. Therefore, the control room interior shall be greenguard gold certified (Modular metal ceiling, Flooring & Modular metal wall paneling) from UL / Intertek. Valid certificate/report to be submitted along with the technical bid.		
1.5	The paneling/partition shall be of factory-made removable type self inter lockable metal panels with front sheet of Preformed Textured Hot dip galvanized sheet with rigid polyvinylchloride (PVC) film on one side and on the other side a coating to avoid rust (sheet thickness 0.6mm & PVC Coating at least 0.11mm). The metal wall Paneling and Partitions surface finish shall be made up of EN ISO 11925-2, EN 13823 certified material. The ceiling material shall be of factory made acoustic modular metal false ceiling of powder coated panels.		
1.6	The project demands for a contemporary, aesthetically appealing, ergonomically designed, safe and 24X7 working facility. Conventional wooden cladding, Gypsum, Aluminum Composite panels, Laminates, Fabric, Paint, Plaster of paris (for control room area) are prone to damages & ageing. These components shall not be used to ensure maintenance free working environment. Control room interior solution provider to submit an undertaking on letterhead to comply the same.		
1.7	Tiles Perforation – To achieve acoustics without deteriorating the aesthetical appeal of the control room it is necessary that the wall paneling shall have micro-perforations (less than 1.6mm diameter each) all over the surface with a density of 5000 holes per square feet. Audit certified design feature on modular wall paneling tile having clean perforations and providing smooth finish on front fascia of tiles. The tile shall have 5000 holes per square feet on front side of the tile. Valid audit certificate (from UL / Intertek) to be submitted along with the technical bid.		

1.8	To provide acoustically superior environment and ensure proper attenuation of airborne sound, it is necessary that the sound transmission class (STC) value of wall paneling and partition shall be minimum 35 (According to IS: 9901 (Part III) – 1981, DIN 52210 Part IV-1984, IS0: 16283 (Part I) -2014, test report (from UL / Intertek) to be submitted along with the technical bid.		
1.9	As control room is a mission critical area and in an unlikely case of damage to the existing wall paneling tiles the same shall be replaceable within 20 seconds and thereby preventing loss of time of operators and ongoing operations. Audit Certified feature of Modular wall paneling tile having secure locking arrangement for equidistant mounting. Locking arrangement enables easy replacement without using any tool within 20 seconds. The feature shall provide easy flexibility of locking all tiles in one column through gravity. Valid audit certificate (from UL / Intertek) to be submitted along with the technical bid.		
1.1	The wall paneling shall be robust & strong enough to sustain the routine loads/minor impacts of typical control room environment. The wall paneling/partition structure shall have audit certified feature of Load bearing capacity of 300 Kgs to hold any display unit on clamp having minimum length of 750mm. Valid audit certificate (from UL / Intertek) to be submitted along with the technical bid.		
1.11	Seismic safety of user & control room equipment is a prime concern area. The metal paneling, metal linear plank ceiling & false flooring shall sustain the seismic vibrations as per design spectrum IS 1893 for zone 4 or better vibrations. The test shall be carried out by authorized government agency. Test Report to be submitted along with the technical bid.		
1.12	From fire safety point of view the metal wall paneling tiles shall be class A fire rated as per the norms of comparative measurements of surface flame spread and smoke density measurements with that of select grade red oak and fiber-cement board surfaces under the specific fire exposure conditions. The proposed metal paneling & metal ceiling tiles shall be Class A certified/tested as per ASTM e84 (from UL / Intertek) for surface spread of flame and smoke generation. This is mandatory to ensure that the materials used in the interiors do not provoke fire. Valid certificate / report to be submitted along with the technical bid.		

1.13	The modular metal paneling & metal ceiling shall comply to the lead-free directive to ensure restriction of hazardous substances so that the final product does not contaminate the environment. The final product i.e., modular metal paneling & metal ceiling does not contain hazardous substances and we give a healthy life to our coming generations it is necessary that the modular metal paneling & metal ceiling system shall be RoHS certified/tested (from UL / Intertek). Valid certificate to be submitted along with the technical bid.		
1.14	To avoid dark spots/areas in the control room it is necessary that continuous linear lights are used across the width/length of the control room. Audit certified design feature of integrated channel in ceiling for quick installation & replaceability of continuous linear light. The ceiling system having integrated inbuilt channel for installation of cove lights and shall permit quick and easy replacement of cove light without using any tools. Replacement to be carried out within 120 Seconds per meter. Valid audit certificate (from UL / Intertek) to be submitted along with the technical bid.		
1.15	Illumination: - Control Room illumination shall be designed as per ISO 11064 norms.		
1.16	Metal modular false ceiling shall have Noise absorption coefficient (NRC) value 0.60 according to IS:8225-1987, ISO: 354-1985 and ASTM 423-90. Test report to be submitted along with the technical bid.		
1.17	Designer Acoustic Laminate Flooring		
	To avoid distraction of users because of unwanted noise generated from movement of chairs/people in the room it is necessary that the proposed flooring shall damp such impact noises. Acoustic flooring (shall reduce impact sound by 14dB (ISO 717-2)). It shall be twin-layer linoleum built up from minimum 2mm acoustic laminate and a 2mm cerement backing. Flooring shall be decorative type of approved shade, pattern, texture, and design and of approved manufacturer. Dimensions shall be as per the final approved design and site requirement. Flooring shall be laid over concrete floor with laying compound strictly as per manufacturer's specification.		
1.18	Designer False flooring		

	a) Mandatory – Top surface shall be acoustic laminate flooring. Height above the RCC floor – upto 150 to 450mm as per layout. The flooring shall be manufactured of fiber reinforced calcium sulphate panels having edges finished with PVC edge band and top surface shall be finished with durable & environment friendly acoustic laminate pasted with glue. Tile size shall be 600mm X 600mm.		
	b) The Panel shall have density of 1600KgM^3 , Fire resistance DIN EN 1366-6 2005-02, Core material thickness shall be minimum 30mm.		
	c) The acoustic laminate shall be made up of twin-layer linoleum built up from 2mm Laminate.		
	This false floor panel shall rest on Edge support rigid grid system having Galvanized Iron base plate dimensions as 100mm X 100mm. The stringer shall be fixed on pedestal having height adjustment of ±25mm.		
1.19	Straight Glass Partition Material (12mm thick toughened glass)		
	1) Full height glass partitions walls shall be made of 12mm toughened glass with frame-less structure. Proper structure shall be made to ensure the fixing of glass from RCC slab above false ceiling and holding channels on flooring.		
	2) Straight and vertical structural members shall not be visible. Glass shall be fitted on extrusion with tool less technology and having a provision for replacing glass with perforated sheet/acoustic tile by removing the glass.		
	3) NOTE: - The nature of installation shall be replaceable, expandable and flexible to cater the future expansion/technical up-gradation.		
1.2	12mm thick Frameless tempered clear glass door with fittings (Single / Double Doors): - With door spring and locking arrangements and both way handle and patch fittings.		
1.21	Metallic Door (Single / Double Doors): - With door hinges and locking arrangements and both way handle. Prepare with rigid thermo fused film metal panels. Specification: 0.6mm thick Metal panel sheets, internal cavity filled with adequate quantity of honeycomb. Material of the partition and that of metal door will remain the same. The door thickness shall be minimum 45mm and frame thickness shall be minimum 115mm.		

1.22	The Control Desk shall conform to high standard of engineering as mentioned in the document; meeting the specified codes, standards and designs. It shall be capable of performing 24X7 operations under the specified environmental condition in compliance to control room ergonomic norms i.e. ISO 11064. All the certificates and reports mentioned below and in BOQ shall be submitted along with the technical bid.		
1.22.1	**Structure: -**		
	Made of heavy-duty extruded vertical and horizontal aluminium profiles. The extrusions shall be duly powder coated with 40+ microns over all surfaces. All sheet metal parts shall be finished with a durable, black, electrostatic powder coating. OEM shall have a valid trademark registration certificate issued by the Government of India for the Control Desk proposed in this tender. Valid Trademark registration certificate to be submitted along with the technical bid.		
	To allow future extension and expansion, a weld-free system shall be proposed. Interconnecting joints shall not be visible. The structure shall be rigid enough to withstand BIFMA X5.5 tests. OEM shall have had BIFMA X5.5 certificate for at least seven years prior to April 1st, 2023. The structure shall allow easy assembly of hinged shutters, slat wall, gland plate, and monitor arms in extremely rigid manner. Valid certificate of BIFMA X5.5 from authorized agencies to be submitted along with technical Bid.		
1.22.2	The EPD (Environmental product declaration) of Control Desk shall be verified in accordance with ISO 14025 (from UL/Intertek) for Impacts on Environment by Control Desk. Valid report/document from UL/Intertek to be submitted along with the technical bid.		
1.22.3	**Table top:** - The material of the working surface shall be minimum 25 mm thick MDF with High-Pressure laminate. The proposed Control Desk's life cycle should be assessed (from approved LCA consultant) for environmental impacts associated with all the stages of a product's life for cradle to grave analysis. Valid report/document from UL/Intertek to be submitted along with the technical bid.		
1.22.4	**Slat Wall: -** Slat wall shall be made of approximately 2mm thick extruded aluminium (aluminium alloy). The proposed Control Desk shall be UL Listed and valid certificate to be submitted along with the technical bid.		

1.22.5	**Modular removable PU nosing:** The front edge of consoles is the component which comes in frequent contact of the operator. The soft polyurethane edge is meant to prevent injury (accidental impact) to operator during emergency and it also reduces the contact stress. In case of damage to this edge the desk design shall permit quick & easy replacement within half an hour without taking any shutdowns or removal of the tabletops. Audit certified design feature of modular PU Edge: High-density poly-urethane foam moulded on industrial grade aluminium core to form 50mm deep tapered edge to be installed on worktop. In case of damage or wear, the edge shall be mechanically replaceable within 30 minutes without opening or removing the worktop. Valid UL audit certificate to be submitted along with the technical bid. Extruded PU edging/PVC T-beading shall be deemed unacceptable.		
1.22.6	**Monitor Arm: -** The Console shall feature ergonomic display mounting arms. It shall enable quick & easy replacement of VESA mounts & arm extensions as per the ergonomic. UL audit certified design feature of monitor arm assembly shall have auto lock, push & remove feature for quick release of VESA mounts and modular arm extensions for ease in maintenance and fixing of monitor by one technician within 30 seconds without using any tools. Valid UL audit certificates to be submitted along with the technical bid.		
1.22.7	The proposed control desk shall be ANSI/BIFMA e3-2019 certified/tested at least for level 3 from UL/Intertek as per Furniture Sustainability Standard to identify the sustainability level of the furniture with respect to the environmental, health & wellness, and social impacts applicable to product(s). Valid certificate to be submitted along with the technical bid.		
1.22.8	**Shutters & Side Legs: -** Front, and back shutters shall be of 18 mm Laminated MDF Board with premium finish. Side leg shall be of 25mm of the same finish. The proposed console shall be Greenguard Gold certified. OEM shall have had this certificate for at-least five years prior to April 1st, 2023. Valid certificate from UL/Intertek to be submitted along with the technical bid.		

1.22.9	**Cable Trays and Wiring: -** The Console shall be designed with vertical and horizontal cable trays to allow for continuous cable management between the cabinets. Wire shall be routed into the cabinet through gland plate. The proposed console shall be RoHS Certified/tested from UL/Intertek and the valid certificate/ test report shall be submitted along with the technical bid.		
1.22.10	**Hardware:** - All bolts shall be of SS material to avoid rust due to environment. The remaining hardware shall be Nickel Plated MS.		

5.42 SAFETY AND SECURITY SYSTEM FOR INTEGRATED COMMAND AND CONTROL CENTRE (ICCC)

Conventional Fire Alarm System			
Sl No.	Technical Specification	Technical Compliance (Yes/No)	Remark
A	General Requirements		
1	Conventional Fire Alarm Panel with support for 2 Zone or more, in-built auto-dialer (4G GSM and PSTN support), in-built TCP/IP Communication Module for connectivity with Central Monitoring Software, Tactile Keypad for easy operation, CE Certified		
2	Smoke Detector with accessories including response indicator and Manual Call Point - 2 Sets to be installed in each partition		
3	Hooter cum Strobe with separate power supply and inbuilt Li-ion Battery to ensure function even incase of power failure - 1 No. to be installed in each partition		
4	At least 10% spares to be delivered to ensure proper maintenance.		
	Technical Requirements		
1	Fire Alarm Panel should provide LED indication of system and individual zone status. 16*2 characters LED display or better		
2	Fire Alarm should have in-built UPS type SMPS with inbuilt battery charger		
3	Fire Alarm should have in-built transient protection for power supply and mother board.		
4	Fire Panel should have tactile keypad for easy panel operation.		
5	Fire Alarm Panel should have facility to detect hooter tamper		
6	Fire Alarm Panel should have internal memory for logging at least 200 events		
7	Fire Panel should have in-built Inbuilt TCP/IP module to communicate with Central Moniotring Software and integration with Video Management Software should be supported for alarm monitoring		

8	Fire Alarm System should be installed and wiring should be done as per OEM guidelines and same should be certified by OEM.		
	OEM Criteria		
1	OEM should have ISO 9001, ISO 14001 and ISO 27001 certification and direct presence in India.		
2	OEM of Fire Alarm System should have supplied Fire Alarms to at least 1 Central/State/PSU institution in the last 3 years.		
3	OEM of Fire Alarm system should confirm integration with offered VMS for single dashboard alarm monitoring. Also same confirmation is required from OEM of VMS.		
4	OEM/Authorized Distributor of OEM should have direct presence in India along with Helpdesk and dedicated support technicians for providing remote and on- site service support.		
5	MAF from OEM of Fire Alarm is mandatory. MAF should confirm back-to-back support for the entire duration of the project lifecycle.		

Feature Spec

Sl. No.	**Spec Details**	**Technical Compliance (Yes/No)**	**Remark**
1	The Main Digital Addressable Water Leak Detection Panel shall Operate on 230 V A.C. with battery backup. It will provide supervision of Interface modules. The Main Water Leak Detection Panel shall provide minimum: 1. 10.1 inch Touch Screen Display to indicate Module No. and distance to Leak Location in Meters. 2. Event Log with date and time. 3. SIM Naming facility. 4. RS485 Communication with Interface Modules. 5. Builtin Modbus/Bacnet output for BMS Communication. 6. Built-In audible sounder and one Common Hooter Output. 7. Fault Relay output. 8. Common Alarm Relay Output.		
2	The Water Leak Interface Module shall operate with A.C. local supply. The Water Leak Interface Module shall provide supervision for the water sensing cable. The Interface Module shall provide, at minimum, the following: 1. Sensing cable capacity 150 mtrs. 2. LCD display to indicate distance to Leak Location in Meters . 3. Red LED for Power On. 4. Red LED for Alarm. 5. Fault Relay output. 6. Common Alarm Relay Output. 7. RS485 Communication with Main Water Leak Detection Panel 8. Built-In audible sounder and one Common Hooter Output.		
3	The Liner Water Leak Cable shall provide, at minimum, the following:		

	1. Water detection cable shall consist of 4 conductors, 2 water sensitive and 2 data. 2. The cable shall be restorable and corrosion resistant, and shall not require replacement after being wet. 3. Maximum length of Liner Leak Detection Cable not to exceed 150 meters per Interface Module. 4. Cable shall be installed in the path of a potential water leak.		
4	SOUNDER: The sounder shall give audible alarm when any sensor operates. It shall be complete with electronic oscillations, magnetic coil (sound coil) and accessories ready for mounting (fixing). The sound output from the Hooter should not be less than 85 decibels at the source point.		

5.43 CLOUD SERVICE(DR)

Sl. No	CSP ELIGIBILITY CRITERIA	Technical Compliance (Yes/No)	Remark
1	. The cloud service provider (CSP) should have been operating in India for the last 5 years		
2	· CSP should be a registered firm or a company in India and the proposed Data Centers (DC & DR) should have jurisdiction in India		
3	· Neither the current organization nor the holding company should have been Debarred and / or blacklisted by any organizations of Govt. of India/ Central PSU/ state government entities as on bid submission date		
4	· Proposed Cloud Service Provider (CSP) should be STQC audited and MeiTY empanelled and offer all services from India only as per guidelines of MeiTY		
5	· The CSP must have a turnover of at least 200 Crore in each of the last 5 years or 500 Crore in each of the last 3 years from data center and cloud services.		
6	· The Primary and DR Data Centre (Cloud) shall be physically located in India. The proposed Datacenter for DR should be at least 100 KM from current Primary Datacenter, and it should not be in same River Flood plain		
7	· The proposed data center must be Tier III or above for better availability of cloud services and certified under: o TIA 942/ Uptime Institute Certification o Data Centre should be either Seismic Zone-II or Seismic Zone-III only		
8	· CSP to have ISO-22301 certification for business continuity.		
9	· CSP should be a Leader in latest Gartner Magic Quadrant for “Cloud Infrastructure as a Service”.		

10	· CSP should have minimum 2 data centers each empanelled with MEITY to be used as DC and DR which are atleast 500 km apart.		
11	· The CSP should provide financially backed SLAs for all the services offered and these SLAs should be declared in public portal of CSP.		
12	· The CSP should provide native marketplace with certified applications which can be deployed on cloud. The CSP should also provide capability for administrators to create private marketplace with images from the public marketplace.		
13	· The CSP should provide all variants of cloud service as per MeiTY guidelines. o Infrastructure as a Service (IaaS), o Platform as a Service (PaaS) o Software as a Service (SaaS)		
14	· The CSP must provide the following services from both DC and DR proposed in this RFP o VM and dedicated physical server based compute services for x64 platform o Multiple options of storage including managed disks, unmanaged disks, block storage, file share and data lake storage in multiple performance tiers. o PaaS services for analytics, AI, Kubernetes and container based offerings. o Options for container registry and resource template libraries to support faster deployment and best practice implementation. o CI/CD services to support quick dev and test deployments. o Support for both proprietary and open source versions of Linux distributions o Managed instances and Database as a service for Microsoft SQL, MYSQL and PostGreSQL. o Certified marketplace for purchase of third party solutions. o Options for shipping of data from CSP to department if required for backup purposes o Native Firewall, EDR and WAF services both as a native PaaS from the CSP as well as certified third party solutions selectable from a marketplace hosted by the CSP without intervention from CSP. o Native Bastion host as a service to ensure secure and resilient access to VMs without opening up public IP addresses. o Native CSP VPN based access to cloud services to ensure no open direct public IP based access to any cloud service under this RFP. o Native CSP provided Media services and CDN for media streaming and large file transfer between department/organization and CSP o Offering for perimeter, host and in-memory security solutions for the compute and storage offerings provided by CSP.		
15	· The CSP should be a OEM of the following native services: o Layer 3 and Layer 4 Firewall o Layer 7 Firewall (WAF) o SIEM & SOAR o Vulnerability Scanner o Endpoint Security o Backup Tools o Disaster Recovery Tools		

16	· The CSP should have minimum following experiences. o Providing the Public Cloud Services (PaaS, SaaS) in India for last 5 years o Should have minimum 10 Government / Private Customer reference/ PO in India o Should have minimum 05 reference of Government Entity in India for providing (PaaS, SaaS) Services.		
17	· CSP should support both BYOL (Bring your own license) as well as PAYG (Pay as you go). The OS offered should come with continuous updates and upgrades for the entire contract duration.		
18	· Monitoring services for cloud resources hosted in the data center and support for customized report generation.		
19	· The CSP should support per hour, per month and options for long term (1 yr. & 3 yr.) reservation of compute VMs and DB as a service for MYSQL, PostGreSQL and Microsoft SQL servers.		
20	· The CSP should provide options for dynamic pricing as well as fix unit pricing of all the resources proposed under this RFP for a period of 5 years.		
21	· CSP should have accreditations relevant to security, availability, confidentiality, processing integrity, and/or privacy Trust Services principles. SOC 1, SOC 2, SOC 3.		
22	· Data Centers should be compliant at a minimum with the following: o ISO 9001 o ISO/IEC 27001 o ISO/IEC 27017 o ISO/IEC 27018 o ISO/IEC 27701 o PCI DSS Level 1		
23	· CSP should support a minimum uptime of 99.5% for each of its services. A publicly available documentation needs to be provided for the same.		
24	· The CSP must support dedicated connectivity from atleast 3 ISP providers for department/organization to chose between at the time of deployment.		
	SPECIFICTION FOR CLOUD SERVICES for Guwahati Intelligent City Surveillance Project	**Technical Compliance (Yes/No)**	**Remark**
1	**Minimum VM and Compute Requirements:**		
	· Virtual Machines offered should be with the latest generation processor offered by the processor OEM.		
	· Physical core to vCPU ratio should not be more than 1:2 for all proposed Virtual Machines		
	· Ability to automatically increase/scale the number of Instances/VMs during demand spikes to maintain performance (i.e. ‘scale-out’)		

	· Cloud service architecture should be in such a way that avoids VM outages or downtime when the provider is performing any kind of hardware or service maintenance at the host level		
	· Required Operating System should be offered along with the Virtual Machines and should support both BYOL (Bring your own license) as well as PAYG (Pay as you go). The OS offered should come with continuous updates and upgrades for the entire contract duration.		
	· MSP should have capability to provide dedicated hosts in its native Cloud Infrastructure in India, which allows usage of existing third-party software license		
	· CSP Should offer monthly uptime of 99.5% or higher (as published in the CSP's Public Portal)		
	· Cloud provider should offer the following instance types – o General Purpose – optimized for generic applications and provides a balance of compute, memory, and network resources. o Memory optimized – optimized for memory applications. o Compute optimized – optimized for compute applications. o Storage optimized – include very fast/large amount of local storage for NoSQL databases and Hadoop. o GPU – intended for graphics and general-purpose GPU compute applications		
	· Cloud provider should offer instances that provide a baseline level of CPU performance with the ability to burst above the baseline.		
	· Cloud provider should offer instances that run on hardware dedicated to a single Guwahati Smart City Ltd.		
	· Cloud provider should offer instances that can run nested virtual machines, that is virtual machine inside a virtual machine.		
	· Cloud provider should be able to support following Linux distributions - Red Hat, SUSE, Ubuntu, CentOS, and Debian		
	· Cloud provider should be able to support the last two major Windows Server versions		
	· Guwahati Smart City Ltd must be able to specify and modify server configuration (CPU, memory, storage) parameters seamlessly.		
	· Cloud service should support local storage for compute instances to be used for temporary storage of information that changes frequently.		
	· Cloud service must offer self-service provisioning of multiple instances concurrently either through a programmatic interface (API/CLI) or through a management console.		

	· Guwahati Smart City Ltd should be able to logically group instances together for applications that require low network latency and/or high network throughput.		
	· Guwahati Smart City Ltd should be able to split and host instances across different physical data centers to ensure that a single physical failure event does not take all instances offline.		
	· Cloud service should be able to automatically increase the number of instances during demand spikes to maintain performance and decrease capacity during lulls to reduce costs.		
	· Guwahati Smart City Ltd should be able to import their existing image and save it as a new, privately available image that can then be used to provision instances in the future.		
	· Cloud service must support the ability to take an existing running instance or a copy of an instance and export the instance into a VMDK or VHD image format.		
	· Cloud service must be architected in such a way to avoid instance outages or downtime when the provider is performing any kind of hardware or service maintenance.		
	· Cloud service must be architected in such a way to automatically restart instances on a healthy host if the original physical host fails.		
	· Cloud provider must be able to schedule events for Guwahati Smart City Ltd's instances, such as a reboot, stop/start, or retirement. Depending on the event, Guwahati Smart City Ltd might be able to take action to control the timing of the event.		
	· Cloud service should support containers, including Docker and/or other containerization platforms.		
	· Cloud provider should offer a highly scalable, high performance container management service.		
	· Cloud service should be able to run Guwahati Smart City Ltd code in response to events and automatically manage the compute resources.		
	· Cloud provider should offer license portability and support for Microsoft apps like SQL Server and SharePoint Server, Active Directory as service		
	· Cloud provider should offer license portability and support for Oracle apps like Oracle Database 11g, 12c etc.		
	· Cloud provider should offer license portability and support for IBM apps like DB2 and WebSphere.		
	· Cloud provider should offer a simple pay-as-you-go pricing where Guwahati Smart City Ltds can pay for compute capacity by the hour with no long-term commitments.		
	· Cloud provider should offer VMs with upto 4 TB size.		

	· Cloud provider should be able to support running Generation 2 virtual machines		
2	**Minimum Storage Requirements:**		
	· For all volumes pertaining to production VMs, Solid State Device (SSD) based Block Storage should be offered providing minimum 4 IOPS per GB per Volume.		
	· For the proposed Block Storage, CSP should offer the capability to increase the Volume size in minimum increments of 10GB or lower so that charges are for the actual usage. Offers the ability to increase the size of an existing block storage volume without having to provision a new volume and copy/move the data.		
	· Block Storage with minimum monthly uptime of 99.99% or higher (as published in the CSP's Public Portal)		
	· Object storage should be replicated across multiple DC's for better resiliency and should be designed for 99.99% availability and 99.99999999999999% (16 9's) durability.		
	· Support complete eradication of data such that it is no longer readable or accessible by unauthorized users and/or third parties.		
	· Offer server-side encryption of data 'at-rest', i.e., data stored on volumes and snapshots		
	· Offer object storage tiering capability, i.e. the ability to recommend transitioning an object between object storage classes based on its frequency of access.		

	· **Object Storage** o Cloud provider should offer secure, durable, highly scalable object storage for storing and retrieving any amount of data from the web. o Cloud provider should support an extremely low-cost storage for archival. The CSP should automatically tier the data. o Cloud service should support encryption for data at rest using 256-bit Advanced Encryption Standard (AES-256) encryption to encrypt your data. o Cloud service should support encryption using Guwahati Smart City Ltd provided keys. These keys should be used to manage both the encryption, as data is written to disks, and decryption, when data is accessed. o Management Service that creates encryption keys, defines the policies that control how keys can be used, and audits key usage to prove they are being used correctly. o Cloud Service should support managing an object's lifecycle by using a lifecycle configuration, which defines how objects are managed during their lifetime, from creation/initial storage to deletion. o Cloud provider should provide a strong regional isolation, so that objects stored in a region never leave the region unless Guwahati Smart City Ltd explicitly transfers them to another region. o Cloud service should be able to send notifications when certain events happen at the object level (addition/deletion). o Cloud service should be able to host a website that uses client side technologies (such as HTML, CSS, and JavaScript) and does not require server-side technologies (such as PHP and ASP.NET). o Cloud Service should support versioning, where multiple versions of an object can be kept in one bucket. Versioning protects against unintended overwrites and deletions. o Cloud service should support flexible access-control policies to manage permissions for objects. o Cloud service should be able to provide audit logs on storage buckets including details about a single access request, such as the requester, bucket name, request time, request action, response status, and error code. o CSP should offer a mechanism to avoid accidental deletion of data. In such case data when deleted should be preserved for a minimum of 3 months. o Cloud service should support a lower cost option for noncritical, reproducible data at lower levels of redundancy. o Cloud service should allow uploading a single object as a set of parts where each part is a contiguous portion of the object's data and these object parts can be uploaded independently and in any order. o Cloud provider should offer a service to speed up distribution of static and dynamic web content. o Cloud service should support read-after-write consistency for PUT operations for new objects. o Cloud provider should offer a storage gateway appliance for seamlessly storing on-premises data to the cloud. o Cloud provider should support moving large amounts of data into the cloud by bypassing the internet. o Cloud provider should support moving large amounts of data out of the cloud by bypassing the internet. o Cloud provider should support replicating data to DR site and should provide read-only access to the replicated data.		

	· File Storage o Cloud provider should offer a simple scalable file storage service to use with compute instances in the cloud. o Cloud service should offer SSD backed storage media to provide the throughput, IOPS, and low latency needed for a broad range of workloads. o Cloud service should support petabyte-scale file systems and allow thousands of concurrent NFS connections. o Cloud service should support consistent low latency performance between 5-15 MS at any scale. o Cloud service should support scalable IOPS and throughput performance at any scale. o Cloud service should support thousands of instances so that many users can access and share a common data source. o Cloud service should automatically scale up or down as files are added or removed without disrupting applications. o Cloud service should be highly durable - file system object (i.e. directory, file, and link) should be redundantly stored across multiple datacentres. o Cloud service should support read after write consistency (each read and write operation is guaranteed to return the most recent version of the data).		
3	**Cloud Native Monitoring & Management & Security Services**		
	· **Cloud Resource Monitoring**: Capability to monitor cloud environment centrally, custom monitoring metrics, monitor and store logs, view graphs & statistics, set alarms, monitor and react to resource changes. Support monitoring of custom metrics generated by applications and services and any log files your applications generate. Gain system-wide visibility into resource utilization, application performance, and operational health, using these insights to react intelligently and keep applications running smoothly.		
	· **Audit Trail**: Logs of all user activity within a CSP account including actions taken through the CSP's Management Console, CSP's SDKs, command line tools, and other CSP services. The recorded information includes the 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 returned by the Cloud service.		
	· **Cloud Advisor**: Analyses the Cloud environment and provides best practice recommendations (or checks) in five categories: cost optimization, security, fault tolerance, performance, and service limits.		
	· Cloud Service Providers must offer Cloud native turnkey SIEM offering by which GSCL can configure real-time analysis and alerting of security events. At a minimum, the integration or service must support alerting, log retention and some form of forensic analysis that is able to search across logs and periods of time for patterns.		

	· Cloud Service Providers must include, at minimum, a local identity management system (that is, local accounts) with granular role-based authorization for network services in both the service interfaces and management console. At a minimum, the role-based authorization must support assigning authorization based on individual users and groups of users and delineation must be assignable per firewall, load balancer, IP address and network segment and support, as applicable, the following granular actions: create, delete and configure.		
	· Cloud Service Providers must allow GSCL to access the cloud service via an IPsec VPN tunnel or Secure Sockets Layer (SSL) VPN tunnel over the public Internet. This must be a self-service capability from the provider side, although Guwahati Smart City Ltd will have to make configurations on their end.		
	· CSP must provide an option to the Guwahati Smart City Ltd to encrypt the data on the instance block storage volume so that data remains encrypted at rest. This must be a simple, self-service option when the instance is provisioned.		
	· The block and object storage services must offer GSCL the self-service ability from both management console and Command Line Interface to opt into provider-enabled server side encryption (SSE) for objects or object hierarchies within the storage service.		
	· Large instance support: Providers must offer GSCL instances with a large number of processor cores and memory for processor- or memory intensive use cases. The provider must be able to provide instances that support at 128 vCPUs and 3072 GB of RAM.		
	· Cloud provider should offer a dashboard that displays up-to-the minute information on service availability across multiple regions.		
	· Cloud provider should offer 365 days' worth of Service Health Dashboard (SHD) history.		
	· Cloud provider should offer a service acts like a customized cloud expert and helps provision resources by following best practices.		
	· Monitoring tools that will enable collection and tracking metrics, collection and monitoring log files, set alarms, and automatically react to changes in the provisioned resources. The monitoring tools should be able to monitor resources such as compute and other resources to gain system-wide visibility into resource utilization, application performance, and operational health.		

	· Able to define guidelines for provisioning and configuring cloud resources and then continuously monitor compliance with those guidelines. Ability to choose from a set of pre-built rules based on common best practices or custom rules (e.g., ensure Storage volumes are encrypted, Compute instances are properly tagged, and Elastic IP addresses (EIPs) are attached to instances) and continuously monitor configuration changes to the cloud resources and provides a new dashboard to track compliance status.		
	· Provide Audit Trail of the account activity to enable security analysis, resource change tracking, and compliance auditing		
	· CSP should offer a fully managed service in India that makes it easy to identify potentially fraudulent online activities such as online payment fraud and the creation of fake accounts.		
	· CSP should provide in India, a single location to track migration tasks across multiple cloud native tools and partner solutions certified on the cloud to provide visibility into migration.		
	· CSP should offer a fully managed service in India, that lets Guwahati Smart City Ltd easily create and publish interactive dashboards that include ML Insights. The dashboards should be accessible from any device, and embedded into your applications, portals, and websites.		
	· Web Application Firewall (Layer 7): Protection from attacks by filtering based on rules that create. Filter web requests based on IP addresses, HTTP headers, HTTP body, or URI strings, which allows to block common attack patterns, such as SQL injection or cross-site scripting that could affect application availability, compromise security, or consume excessive resources. Features like protection against Web visibility, east of deployment and maintenance, integrated security.		
	· DDoS Protection: Managed DDoS protection service that defends against most common, frequently occurring network and transport layer DDoS attacks that target web site or applications. When used with Content Delivery Network and global DNS service, should provide comprehensive availability protection against all known infrastructure (Layer 3, 4 and 7) attacks. Should provide always-on detection and automatic inline mitigations, minimize application downtime and latency.		
	· Identity and Access Management: Service that properly separates users by their identified roles and responsibilities, thereby establishing least privilege and ensuring that users have only the permissions necessary to perform their assigned tasks.		

	· Managed Threat Detection Service: Continuously monitor for malicious or unauthorized behaviour to help protect accounts and workloads. It should monitor for activity such as unusual API calls or potentially unauthorized deployments that indicate a possible account compromise. The service should also detect potentially compromised instances or reconnaissance by attackers.		
	· Appropriately configure the security groups in accordance with the Client's networking policies.		
	· Regularly review the security group configuration and instance assignment in order to maintain a secure baseline.		
	· Secure and appropriately segregate / isolate data /application by functionality using DMZs, subnets etc		
	· Ensure that the cloud infrastructure and all systems hosted on it, respectively, are properly monitored for unauthorized activity.		
	· Properly implementing anti-malware and host-based intrusion detection systems on their instances, as well as any required network-based intrusion detection systems in accordance with the Client's Security policies.		
	· Review the audit logs to identify any unauthorized access to the Client's systems.		

5.44 Geographical Information Systems (GIS)

The GIS platform integrated with a city surveillance system can enhance inter-departmental coordination and communication by providing a common operating picture for all stakeholders involved in public safety and emergency response. This can lead to faster response times and better decision-making during critical situations.

An indicative list of use cases which the Master System Integrator (MSI)/ Implementation Agency (IA) will be required to implement is given below. As and when the system expands, and more applications get added the Master System Integrator (MSI)/ Implementation Agency (IA) is required to be open to all such subsequent additions. Exact definition of the use cases shall be finalized as SRS(Software Requirement Specification) stage.

S.no.	Function	Use Case	Display Information	Stakeholder
1	Video camera surveillance Mapping	Show location , attributes and working condition of all assets viz. Cameras	Location coordinates, working condition with whole attribute information display on click with live feed on GIS /Web GIS Map.	Department officials
2	Video camera surveillance Mapping	Video camera site location optimisation and analysis for planning	Display of IFOV on click at any location with opening angle and viewing distance on 3D GIS/ Web GIS Map environment.	Department officials, City Planners

3	Video camera surveillance and viewing Analytics	Significant location Gap Analysis	IFOVs of all installed camera assets with a buffer of view adjustment with all significant high security locations in the city for surveillance coverage analytics	Department officials, City Planners
4	Video camera surveillance and viewing Analytics	Camera view link optimisation for tracking (Live GPS)	Linking of live GPS location of app based Services with camera (IFOV) for on the fly live view display of camera feed. It will be used for tracking /Geo-fencing of App Based Vehicles services.	Department officials, City Planners, Surveillance department (police)
5	Video camera surveillance and viewing Analytics	Camera view link optimisation for tracking(Speed)	Linking of moving asset with respect to speed and camera location (IFOV) for on the fly live view display of camera feed.	Department officials, City Planners, Surveillance department (police)
6	Environment sensor analytics	Display of location of all environment sensor	Display location and data retrieved from all environmental sensor and display bar graphs and charts in near real time updates on click.	Department officials, City Planners, Citizen
7	Environment sensor analytics	Sensor data based alert generation	Display of sensor environment factor data in spatio-temporal genre and generation of alert to citizen within effective area (buffer) of the sensor.	Department officials, City Planners, Citizen
8	Environment sensor analytics	ITMS based integration for re-routing of traffic	Red flag from environment sensor to be displayed on dashboard and can be integrated with ITMS to reroute traffic (using network analysis) in more polluted areas	Department officials, City Planners, Citizen
9	Environment sensor analytics	Temperature based Heat island mapping	Display of a high temperature density map of the city using temperature data from the sensors for identification of urban heat islands on GIS Map/Web GIS Map.	Department officials, City Planners,
10	Environment sensor analytics	Visualisation of Sensor locations and its information on web GIS map	Location coordinates, working condition with whole attribute information display on Web GIS Map	Department officials, City Planners,
11	Environment sensor analytics	Visualisation of sensor impact area and colour as per sensor value on web GIS Map	Visualisation of Sensor Impact Area Using Impact area Buffer and Change of Buffer colour as per Change in environments sensor value	Department officials, City Planners,
12	Environment sensor analytics	Environmental Sensor site location optimisation and analysis for planning	Identify senor location using Web GIS Software using various parameters like Population density. Industrial area etc	Department officials, City Planners,

COTS 3D GIS Platform with Geo Analytics Software Platform Specification Compliance

Sl. No.	Specification	Compliance
1	COTS GIS platform with 16 core licenses for 3D GIS	
2	The proposed deployed COTS 3D GIS Enterprise Platform should be Industry standard COTS GIS platform. The proposed deployed 3D GIS platform should have all functions of GIS and Image feature extraction, geo-processing, image mosaicking, Photogrammetry, sub setting, classification (supervised, unsupervised) change detection, AI/ML based object Detection components in a single installed software only. The platform should also have advance modules like network analysis, terrain analysis, 3D analysis, change Detection, Photogrammetry module, Raster GIS analysis, SAR processing and 3D analysis.	
3	The Proposed solution should be an integrated solution only having GIS, 3D Analytic and Image Processing components in single COTS Enterprise software. The overall proposed solution should be of Single GIS Platform only	
4	The single integrated platform of GIS platform should have both GIS and Image analysis components, which going to be deployed at site. It should support 64 bits. It should based on a Services Oriented Architecture (SOA). The Enterprise GIS software must be OGC certified and must have the capability to serve and consume OGC complied web services including WMS, WFS, WCS, CSW, INSPIRE, etc. Licensing policy should not be restricted by hardware/ period or sites. OEM undertaking should be submitted for further customization of application based on GIS and Image processing Custom based web application, as per project needs of present and future. No restriction during hardware upgrade/ scaling in future.	
5	Server deployed Software should run as a native 64-bit application and should support Windows 64- bit and Linux 64 bits.	
6	The deployed Integrated enterprise platform should have capabilities like geo-processing and analysis, spatial and statistics analysis and Image analysis functions. It should support server end Geo processing and Image analysis tools such as supervised classification, Enhancement, Vegetation Indices, buffer, clip, erase. Provision should be available by server for sending the request using the web client and display the processed data on web using OGC certified services.	
7	The web GIS application should open on any browser and should support cross platform. It should have RestAPI for integration with other applications	
8	The Integrated 3D Enterprise platform should provide a map centric for managing geospatial content of organization. It should serve as project centric approach to Create, Access, Analyze, Manage and disseminate geo-spatial content with capability of user management and role-based access control.	

9	3D Enterprise Platform should have rich display and navigation tools like zoom in, zoom out, fixed zoom in, fixed zoom out, pan, real time pan, bookmark, Geo link multiple views, swipe, flicker, search by location, cursor location value, etc.	
10	Ability for 3D representation of the city or town with LOD1 to LOD4 level details as required. The 3D platform should have functionality for 3D analysis tools such as Measurement (Distance, Area, etc.), Dynamic based View shed, Line Profile, Line of Sight, Dynamic Contour, Flooding simulation, Dynamic Buffer generation of all geometry types. Capability to create slope & Aspect from terrain model, dynamic water, Dynamic River course, sub-merge analysis, Volumetric analysis. The software should have capability to create skyline based on observer position and distance. Model Cut tool for the visualization of object from different directions,	
11	The 3D enterprise software should support draping of vector and raster: WMS, WMTS, KML/KMZ. Facilities to view Shape File, DGN, GPX & Geo-tiff, TIF. Provision to process and display CEOS SLC and Hybrid Polarimetric data of SAR, DTED, DEM. It should support various data such as Terrain (DEM, Tiff, DTED etc..), 3D Building and animation file i.e CZML Collada - *.dae, *.obj, *.gltf. Photogrammetry Meshes data derived from UAV. Display of model generated form Drone, Satellite Stereo Pairs, LiDAR, Point Clouds (LiDAR data *.las, *.laz). Support of Vector data (GeoJSON, KML, Shape etc.), OGC (WMS, WFS, WCS, etc.), Capable of consume multiple third party OGC map services for visualization	
12	It should have capability to import / export data in various formats like .dwg,dxf, .dgn, .shp (shape files), coverage file, .mif (MapInfo), .gml, .kml, .gpx. , Geo PDF GeoJSON, H4, H5 formats, MBtiles etc. Should support ODBC compliance interface with industry standard RDBMS like PostGRE SQL, Oracle, SQL server, Access etc.	
13	The deployed GIS platform should provide a complete set of drawing & editing tools in order to enable the user to draw & modify any or parts of various geographical objects (point, line and polygon) on the map. Provision for finding invalid geometry and Polygon Topology error	
14	The deployed 3D enterprise Platform should have capabilities like geo-processing and analysis, spatial and statistics analysis and Image processing functions in a single window. It should have out of box Geo processing and Image analysis functions like Clip, Erase, Spatial Join, Relate, Buffer, clip, erase, intersection, dissolve, union, polyline to polygon, summarize, polygon auto numbering based on line feature and direction, Image classification(supervised, unsupervised), Image segmentation , Recode, Change detection module, Photogrammetric module, Resolution Merge, Radiometric correction , Enhancement , Layer stacking, Georeferencing ,Collage Image, Mosaicking, High pass, Low Pass filter, Fast Fourier transformation,3D viewer with 3D based analytic tools and AI / ML based Object identification as out of box functions.	
15	Software should have the facility for reports generation, customized map layout, high resolution printing in different formats (jpg, pdf) with desired map scale and customized templates.	

16	Should have capability to store the applied legend, color , symbology and further applied in other GIS projects. Further, provision should be there to export and import the custom annotation and labelling pattern from one project to other. Thematic mapping like Bivarte, Multibivarte, chart mapping should be available as out of box. Geocoding and Reverse Geocoding should be available.	
17	Single deployed Platform should must support Time aware data for Trends / Time Series Analysis. Provision should be there for Online and Offline GPS integration.	
18	It should network analysis module to perform Routing analysis, Service Area Analysis, Dynamic segmentation etc. Capabilities like Dynamic Labelling and Rule based Labelling should be available	
19	The software should have function to perform different operations like: mathematical, logical, string operations on the field of table of vector layer or selected objects of vector.	
20	The software should allow visualization of data in 2D/3D in enterprise application. Provision should be available to host the 3d project from to browser mode. Facilities to import Satellite images, LIDAR, Building model. The system should have facilities to store the 3d model which can be used in future without doing any pre-processing.	
21	The 3D GIS Enterprise platform should have out of box provision to generate / create feature on 3d enviourment of all geometry types. Facilities for creation on 2d and 3d symbol should be there. Additionally, provision to share the 3d scenes is also required.	
22	It should have module for terrain analysis and 3D analysis to create/ view - slope/aspect, hillshade, elevation profile, topographic normalize, line of sight and viewshed analysis.	
23	It should have algorithm for surface generation such as heat maps, Linear, IDW and Krigging.	
24	The proposed software should support HRSI (High Resolution Satellite Imagery) and low resolution satellite images (panchromatic & multispectral) such as IKONOS, Quick bird, Geoeye, Worldview, CARTOSAT, EROS, LISS-IV, LISS-III, AWIFS, RISAT-1 & 2, KALPANA-1, INSAT3A, INSAT3D, PROVA-V,CEOS,ECW,JP2000, Sentinel, Radarsat, etc..	
25	The platform should have capability to process optical satellite data, microwave image data, and Metrological.	
26	It should have enhancement algorithm such as Linear, Logarithmic, Histogram Equalize, Histogram Matching, Density Slice, Gaussian, Squire root, Tone Balancing etc..	
27	The software should have image transformation module such Vegetation Index, Principal Component Analysis (PCA), Inverse PCA, Pan sharpening, Wavelet fusion, etc.	

28	The3D enterprise platform should be capable to process the temporal or time series image data. To identify encroachment and monitor urban sprawl, software should provide change detection capabilities as out of box tools such as Basic Change Detection, Advance Change Detection, Auto Change Detection and Site Monitoring. The advance change detection capability should allow to ingest multiple input images to find the change. It should also handle the multi resolution satellite image along with mis-registration. It should have capability of Object Library Creation for Object Identification and Automatic Feature Extraction (AFE).	
29	It should be out of box functions for generation of reports and pie charts maps like bubble, time series, scatterplot matrix. Trees map, box plot, Data plot map.	
30	The platform should have photogrammetric extension which should have facilities for automatic stereo model by using stereo data from sensors like cartosat , worldview , superview , Astrium , Geoeye by using RPC /RPB information. Also, provision should be there for auto mosaicking of stereo tiles by using sensor information.	
31	Provision should be there to create DSM, DTM and Ortho rectify Images from stereo pair. Also provision should there to generate the accuracy report of stereo model.	

Software Specification- Desktop GIS:

Sl. No.	Functional Description	Compliance Status
COTS GIS Desktop		
GIS Functions		
1.	User should be able to create multiple views in single project using the capability of multiple document interface (MDI) of the proposed software.	
2.	The application framework of the software should be such that it should have Dockable/Floating Toolbars, Dockable and Auto Hiding Windows, Unicode Support for Multilanguage Attributes, Drag and Drop to Rearrange Tools/Toolbars, Create New Toolbars or Menus without Programming, Extend the Applications with Add-ins built with .NET, Java, or Python, Build New GIS Components with .NET or Java or other development platforms.	
3.	The user should be able to create layer as per the data model defined by the authority or concerned stakeholders along with the modification in table structure as per the requirement of project.	
4.	Provision for defineding of map projection system and geodetic datum is required to set all the maps in a common projection and scale.	
5.	The proposed software should have capability to create custom projection system using 3 to 7 parameters.	
6.	Display of coordinates on map click is required to readout the co-ordinate in any projection i.e. multi projection coordinate readout.	
7.	The proposed software should have facility to click on any feature of the map and return a select set of attributes for feature.	
8.	User should be able to perform geo-processing functions such buffer generation, clip, erase, intersection, dissolve, union, polyline to polygon, etc. for various type of GIS analysis. It should have facility to perform the spatial intersection analysis like plot area with buffer zone to calculate road-widening impact on adjacent land.	

9.	The Software should be able to import / export data from / to various formats like .dwg, dxf, .dgn, .shp (shape files), coverage file, .mif (MapInfo), .mdb (GeoMedia), .gml, .kml, .gpx. , Geo PDF GeoJSON, GeoRSS, etc.	
10.	Software should have functionality to export GeoPDF and MBTiles file	
11.	The proposed software should have function to process tabular data such as .xlsx, .csv, .dbf, etc.	
12.	GPS functions which allow the user to mark locations on a georeferenced map based on the inputs from a GPS device.	
13.	Support of Coordinate Geometry (COGO) description for GIS objects creation and store in GIS database.	
14.	Facility to define joins between the two tables (graphic / non-graphic) of the database to get integrated information in the table and perform GIS analysis.	
15.	The proposed software should provide facility to exchange the GIS Data with other platform applications like Microsoft Word, and Excel to use GIS data and generate reports like graph and charts.	
16.	Software should have rich display and navigation tools. It should have zoom in, zoom out, fixed zoom in, fixed zoom out, pan, real time pan, bookmark, Geo link multiple views, swipe, flicker, search by location, cross hair, cursor location value, numeric dump, query cursor etc. It should have support of continuous panning i.e. real time pan.	
17.	Software should allow the user to perform undo / redo operations during editing of GIS maps.	
18.	The software should have capability for geo-referencing of vector and raster data both.	
19.	Facility to capture the geometry from the layout maps, creating maps by maintaining the coincident geometry i.e. when a new polygon is captured simply by selecting an existing polygon to digitize the common boundary thereby ensuring no slivers or gaps between adjacent area features like parcels.	
20.	The software should provide a complete set of drawing & editing tools in order to enable the user to Draw & Modify any or parts of various geographical objects (point, line and polygon) on the map.	
21.	The software should have capability to remove the topological errors from vector data such as road network, drainage network, canals, building, etc.	
22.	The software should have the ability to add data from internet or intranet to the existing map data using OGC services.	
23.	The software should allow user to legend template of geographic data that store symbology for displaying features.	
24.	The proposed software should have capability of thematic map mapping. User should be able to apply color and symbology using the attribute attached with the layer based on single, quantile and unique values functions.	
25.	In the proposed software, user should be able to perform labelling activity using the attribute information of the layer. Therefore, a rich annotation tool should be available in the software such as add label, edit label, move label, rotate label, remove all label, etc.	
26.	User should be able to define the rules for displaying the labels on map by defining the class using the attribute to be displayed and can set the priority for displaying the multiple labels of single layer.	
27.	The software should have a provision of hyper linking the GIS feature as well as its attribute fields with existing documents, URLs, Images, drawing files or scanned maps related to that feature.	
28.	User should be able to create version for history tracking.	
29.	Query builder tool should be available with the software to perform simple and complex queries.	
30.	The customized application should provide the user facility to make dynamic queries on GIS GUI. The application should allow users to store and retrieve standard queries used by them in day to day operation.	
31.	Software should have various query tools for queries based on attributes, location, etc.	

32.	Software should have support of various plots and charts such as Bubble chart, Box plot, Tree map, Cord diagram, scatter plot matrix, Area graph, Line and Bar graph, schematic diagram, etc.	
33.	Software should have map composition / layout tool for printing spatial data at different scales and at adjustable print quality.	
34.	Software should allow users to export results to various file formats like EMF, BMP, TIFF, JPEG, PDF, etc.	
Image Processing Functions		
35.	The proposed software should support HRSI (High Resolution Satellite Imagery) and low resolution satellite images (panchromatic & multispectral) such as IKONOS, Quick bird, Geoeye, Worldview, CARTOSAT, EROS, LISS-IV, LISS-III, AWIFS, RISAT-1, KALPANA-1, INSAT3A, INSAT3D, PROVA-V, etc..	
36.	The software should have capability to process optical satellite data as well as microwave image data.	
37.	The software should support images with More than 8 bits, 11 bit, 16 bits, and 24 bits per band.	
38.	The software should support image format such .tif, geotiff, .img, .pix, .hdr, .h4, .h5, DTED, DEM, CEOS, .bmp, .jpeg, Netcdf, Grid File, etc.	
39.	The software must have the user-friendly tool for re-projecting geospatial data (raster and vector) from pre-assigned projection to the other projection system as per the user's requirement.	
40.	Software must provide the functionality for clipping the area of interest from raster data using user defined extent, extent defined through inquire box, and polygon layer.	
41.	The software should have the functionalities for splitting the image in the tiles based upon user defined parameters. It should support mosaicking of images by geographic coordinates based mosaicking method as well as pixel based mosaicking method.	
42.	The software should have the Geometric Correction tool for assigning geographic or projected coordinates and to remove the geometric distortion in the image. It should also provide the functionalities for Atmospheric correction for Haze reduction, and DN to Reflectance conversion.	
43.	The software should have Layer stacking tool to create composite multispectral satellite image from a number of spectral bands of same spatial resolution.	
44.	The software must have image enhancement tools to permanently apply enhancement on the imageries for further processing. Some of the basic enhancement tools such as Linear, Logarithmic, Histogram Equalize, Histogram Matching, Density Slice, Gaussian, Squire root, Tone Balancing etc., must be available for the on the fly image viewing and interpretation purpose.	
45.	The software is expected to have the Image filtering tool with various filtering algorithm such as Convolution, Texture, Adaptive, Crisp, Laplacian, Statistical, FFT, etc.	
46.	The software should have image transformation modules e.g., Principal Component Analysis (PCA), Inverse PCA, De-correlation Stretch, Water Index (NDWI, MNDWI, NDMI,NDSI,NDMI) and various vegetation indices along with LAI, FAPAR, etc., for information enhancement. It should have the tools for image fusion using various image fusion algorithms like Pan sharpening, Wavelet, Brovery multiplicative, and HIS etc. for spatial resolution enhancement of the image.	
47.	The software should have the module for Natural Color image generation using NIR, Red and Green band of high-resolution multispectral image data. This module should have capability to stretch the natural color image into 8 bit.	
48.	The software must support image classification modules such as supervised and unsupervised classification along with image segmentation.	
49.	The software must have tools for the accuracy assessment such as contingency matrix, signature separability, etc.	
50.	The software should be capable to process the temporal or time series image data. The software should provide change detection module such as Basic Change Detection, Advance Change Detection, Auto Change Detection and Site Monitoring. The advance change detection module	

	should be capable to ingest multiple input images to find the change. It also handles the multi resolution satellite image along with mis-registration.	
51.	It should support various methods of advance change detection such as single band differencing, cross correlation, Image regression, Image ratioing, PCA, Change Vector Analysis (CVA), Magnitude Differencing, Vegetation Index Differencing, Tasseled Cap, Chi-Square, Unsupervised Change Detection, etc.	
52.	The software should have capability of Object Library Creation for Object Identification and Automatic Feature Extraction (AFE) based on the object library.	
53.	The software should have AI/ML based object detection/identification module. The module should have facility to create/update training model for single or multiple type of object present in specified satellite/resolution images. The module should have latest algorithm for object detection such as Faster RCNN.	
54.	The software should have functions like Linear Algebraic Combination, Change resolution, Bit Conversion, etc.	
55.	The software should have function called Dynamic threshold for analyzing change detection using image. This function is used to categorize the pixels in input image based on the threshold value.	
56.	The software should have raster catalog and vector catalog tool for raster and vector data management.	
57.	Network Analysis: The software should have network analysis module to find the shortest and Optimum path using the topologically corrected road network.	
58.	Terrain Analysis: The software should have tools for terrain analysis and 3D analysis. The module should be able to create slope/aspect, relief map, elevation profile, painted relief, line of sight and, viewshed analysis. It should also support the “cut and fill analysis” and topographic normalization using DEM data. The software should have algorithm for surface generation such as Linear, IDW, Kriging, Multilevel B Spline, etc.	
59.	Tracking Analysis: The software should have capabilities to animate the temporal GIS data using the time stamp information available as attribute.	
60.	Software should support fully automatic raster to vector conversion tools.	
61.	SAR Data Processing: The software should have support of RISAT, ALOS, SENTINEL, TERRA-SAR, and RADARSAT. The software should have various tools for SAR data processing such Calibration, amplitude & intensity image generation, phase calculation, hybrid polarimetric parameter calculation, hybrid image decomposition, radar vegetation index calculation and other data analysis tools such as EM Clustering, BOX CAR Classifiers, Ship Detection, Wake Detection, Radon Filter and Canny Filter, etc.	
62.	Meteorological Data Processing: The software should have tools for meteorological data processing module such T-Phi gram generation, satellite Image prediction and wind vector generation using sounder, imager and WVW INSAT data.	
3D Functions		
63.	The software should have capability to create 3D scenes and flythourgh model using various effect, animation and various analytics functions.	
64.	The 3D software should have capability to handle huge size of data and should have support of GPU acceleration for smooth handling of GIS data.	
65.	The 3D software should be compatible on Desktop, Web and Mobile environment.	
66.	The software should have 3d analysis tools such as Measurement (Distance, Area, etc.), Dynamic based View shed, Line Profile, Line of Sight, Dynamic Contour, Flooding, Buffer, etc.	
67.	The 3D module should have capability of land & surface interpolation to create slope & Aspect from DEM.	

68.	The software should have functions of water preservation such as dynamic water, dynamic river, sub-merge analysis, surface discharge, etc.	
69.	Volumetric calculation tool should be available with the software. Also, user should be able to mark the cross section by considering height to calculate the volume.	
70.	Should have support of variance analysis of terrain data and terrain excavation.	
71.	The software should have functions to perform shadow analysis as per the almanac information.	
72.	Should have support of indoor, outdoor, over ground and underground visualization.	
73.	The software should have big data analytics tools like honeycomb & grid diagram, wind direction, etc.	
Photogrammetry Functions		
74.	The software should have various tools for SAR data processing such Calibration, amplitude & intensity image generation, phase calculation, hybrid polarimetric parameter calculation, hybrid image decomposition, radar vegetation index calculation and other data analysis tools.	
75.	Software should support RPC model for DEM generation.	
76.	Software should have preprocessing module so that user can mosaic the tiles of images using TIL file available with raw stereo data.	
77.	Software should have modules for point cloud generation using inputs such as stereo pair image, RPC file, seed DEM, GCPs and other parameters.	
78.	The software must have the tool for DSM to DTM or tool for object and ground image generation.	
79.	The software should have tool for ellipsoid height to geoid height conversion.	
80.	The software should have DEM editing tools for gap or Void fill using Multi-level B-Spline, Gap using Spline, or Stepwise Resampling algorithm.	
81.	Should have module for ortho-rectification of satellite image using, DEM and bundle block adjustment as input.	
82.	The software should have tools for calculating the position accuracy of generated out put such as DEM and Ortho Images.	

5.45 Estimated MPLS network Plan and bandwidth requirement

S.No.	Locations	Estimated	Remarks
1.	Cameras	5 Mbps	The quantities and bandwidth mentioned in this table are indicative only. Bidder shall re- evaluate the bandwidth as per the solution requirement and propose accordingly.
2.	Other field Location- VMD, Sensors etc	5 Mbps	
3.	Viewing Centre	500 Mbps	
4.	Command & Control Centre/Data Centre	5 GBPS	
5.	Data Recovery –Cloud	16 GBPS	

Trenching for last mile connectivity			
Sl. No.	Description	Technical Compliance (Yes/ No)	Remark
1	SI shall exercise due care that soil from trenching intended to be loose for back filling is not mixed with loose debris. While trenching, SI should not cause damage to any underground installations belonging to others agencies and any damage caused should be made good at his own cost and expense.		

2	The SI should provide sufficient width in the trench at all such places, where it is likely to cave in due to soil conditions without any extra payment.		
3	A minimum free clearance of 15 cm. should be maintained above or below any existing underground installations. No extra payment will be made towards this.		
4	In order to prevent damage to HDPE Pipe/PLB Blowing Type/Pre-installed rope over a period of time, due to the growth of trees, roots, bushes, etc., the SI shall cut them if encountered in the path of alignment of trench without any additional charges with proper permission by Competent Authority.		
5	In large borrow pits, excavation shall be done not less than 165 cms. In depth and both sides of borrow pit shall be excavated more than 165 cms in depth to keep gradient of bed less than 15 degree with horizontal.		
6	If not possible as stated in sub clause above, alignment of trench shall be changed to avoid borrow pit completely.		

6. BILL OF MATERIAL (BoM)

Refer Vol-IV for Capex and Opex details

7. **Location details**

Refer Annexure_Location details