Metropolitan Transport Corporation (Chennai) Ltd.

Pallavan House, Anna Salai, Chennai-600 002

Request for Proposal for selection of System Integrator to "Design, Supply, Implement, Commission, Operate & Manage the Safe City Solution" as a part of Nirbhaya Safe City Project for Metropolitan Transport Corporation

RFP No. : 17/44017/Proj/MTC/2020

Due Date :14.09.2020

SAFE CITY

Request for Proposal

Volume 2: Scope of Work

1 Contents

1 Scope of Project Work 4
1.1 Vision 4
1.2 Background 4
1.3 Brief Description of Scope 5
1.3.1 Mobile Surveillance System 5
2 Detailed Scope of Work 8
2.1 Overview of Phase I 8
2.1.1 Section 1 – Project Planning 8
2.1.2 Section 2 – Design of Safe City Solution 9
2.1.3 Section 3 – Supply, Installation, Testing & Commissioning of solution 12
2.1.4 Section 4 – Final Acceptance Testing 14
2.1.5 Section 5 - Training & Capacity Building 17
2.1.6 Section 6 – Solution Stabilization & Go-Live 20
2.2 Overview of Phase II 20
2.2.1 Detailed Phase-II Requirements 20
2.2.2 Section 1 – Operation & Maintenance Services 20
2.2.3 Section 2 – Facility Management Services 22
2.2.4 Section 3 – Knowledge Transfer & Exit Management 26
3 Service Level Agreement (SLA) 29
3.1.1 Implementation SLAs 29
3.1.2 Operation & Maintenance SLAs 30
4 Project Implementation Timelines 33
5 Functional and Technical Requirements 34
5.1 Command & Control Centre 34
5.1.1 Functional Specifications 34
5.1.2 Technical Specifications 65
5.2 Data Centre 80
5.2.1 Data Centre Service Specification 80
5.2.2 Smart Data Centre Infrastructure (On-Premises or On-Cloud) – guidelines . 100
5.3 CCTV Monitoring Systems (VMS) for 6 MTC Officers 181
5.3.1 Minimum Technical Specifications 181
5.4 CTV Monitoring Systems (VMS) – TAB with Mobile Application for 50 MTC Staffs 183
5.4.1 Minimum Technical Specification 183
5.5 CCTV Surveillance System for Women Safety in MTC Depots & Terminals (66) 184
5.5.1 Information security policy, including policies on backup 184
5.5.2 Surveillance Equipment – Functional Requirements 184
5.5.3 Minimum Technical Specifications 185
5.6 CCTV Surveillance System for Women Safety in 2800 MTC Buses 192
5.6.1 Information security policy, including policies on backup 192
5.6.2 Surveillance Equipment – Functional Requirements 192

5.6.3 Minimum Technical Specifications 193
5.7 Network 201
6 Common guidelines / comments regarding the compliance of IT / Non-IT Equipment / Systems to be procured 210
7 Payment Terms & Payment Schedule 212
7.1 Payment Terms 212
7.2 Payment Schedule 212
8 Annexures 213
8.1 Annexure 1 – Matrix for Scope of Work 213
8.2 Annexure 2 –: Indicative list of locations 216

1 Scope of Project Work

The selected System Integrator shall have the overall responsibility for design, supply, install, build, implement, and maintain the surveillance system for Chennai Safe City Project for a period of three years (from Go-Live) which involves implementation, operation and maintenance.

The surveillance system involves setting up of an intelligent system comprising of IP based security cameras installed across minimum 2800 Metropolitan Transport Corporation (MTC) Buses which travels throughout Chennai city and 66 Numbers of Depots & Terminals. The system will have the ability to monitor, detect, alert and record any attempts of violence & abuse against women and children.

The servers and storage system of surveillance data and analysis will be housed in the Data Centre which would be setup to cater to the requirements of the solution.

The System Integrator should provide turn-key solution for all the components as envisaged by the Metropolitan Transport Corporation (MTC) and include any missing item (s) notwithstanding the detailed Bill of Material (BOM) given in this RFP for the successful end to end implementation.

The System Integrator is to implement a TURNKEY solution for safe city surveillance system and integration with other systems as mentioned in the scope of RFP adhering to the requirements as detailed by Metropolitan Transport Corporation (MTC) in this RFP scope.

1.1 Vision

The vision of the project is to implement a comprehensive women and child centric video based proactive surveillance system. The project envisages to provide more eyes on the MTC Buses to act as an effective deterrent for crimes against women and children. The following are the key objectives of this initiative: Secure environment for women and children travelling in MTC Bus, Terminals & Depots by installation of surveillance cameras

1.2 Background

The Metropolitan Transport Corporation (formerly known as Pallavan Transport Corporation), sometimes known as the MTC, is the agency that operates the public bus service in Chennai, India. The MTC had a scheduled fleet of 3600+ buses, on a daily basis carries 6.0 million passengers to and from, which is half the population of Chennai. In March 22, 2016, the Union Transport Ministry reported that Chennai had the most crowded buses in the country with 1300 passengers per bus in each direction per day. During peak hours, in some routes, a bus with capacity to accommodate 80 persons carries twice the number of people due to the extensiveness of the system. It has an operating area of 3,929 square kilometres.

The envisaged Women and Child safety-centric solution will include installation of cameras in the MTC Buses which run across the Chennai City frequently used by women/children where

video surveillance can assist law enforcement agencies in prevention and detection of incidents compromising their safety. Furthermore, in case of an emergency, this project aims to provide Metropolitan Transport Corporation (MTC) with adequate Command and Control Centre (CCC) capabilities to address the emergency promptly. The project will involve deployment of video and communication software for identifying persons involved in harassment of women and children inside buses.

The proposed project will include setting up of a network of IP based Surveillance Cameras in Buses, Depots & Terminals; app based mobile device viewing (TABS); viewing stations for MTC Officers and a master control station i.e., Command and Control Centre (CCC). The video feeds from the Cameras would be monitored and analyzed at the CCC of Metropolitan Transport Corporation (MTC). System Integrator may also be required to transmit the Video feeds to any other CCC run by government agencies (like Chennai Smart City, GCC, GCP, etc.) in the future.

The architecture envisages that the video feeds of the surveillance camera installed inside the Buses, Deports and Terminals to be stored in a Data Centre in the Metropolitan Transport Corporation (MTC). The video feeds would be viewed on a large video wall installed at the Command and Control Centre. The Command and Control Centre will be a fully integrated system with upgraded software for video analytics (future scope) and generate actionable information and alerts. All analyzed data and actionable information / alerts would then be passed on for necessary action from the Command and Control Centre to the Dispatch Section of the Dial-100 system.

MTC shall select the System Integrator through competitive bidding on evaluation of both Technical and Financial suitability of the solution proposed by the SI for providing the complete solution, involving but not limited to hardware, software, maintenance and workforce to make the system complete in all aspects. The Solution proposed to be implemented will have the following components:

1. Mobile Surveillance Solution
    a. Cameras
    b. Video Management System
    c. Command and Control Centre (CCC)
    d. Smart Data Centre (Hardware + Software)

1.3 Brief Description of Scope

1.3.1 Mobile Surveillance System

The vision of the Mobile Surveillance System is to have an integrated view of images from camera based surveillance system installed inside the Buses, Depots & Terminals in Chennai City. The system would be useful in monitoring and capturing events through the cameras and transmitting the same to CCC. The proposed system provides numerous advantages highly useful for maintenance of public order. Some of the key benefits are

- Real time monitoring
- Remote access.
- Situational Awareness for better decision making
- Improved Event Management

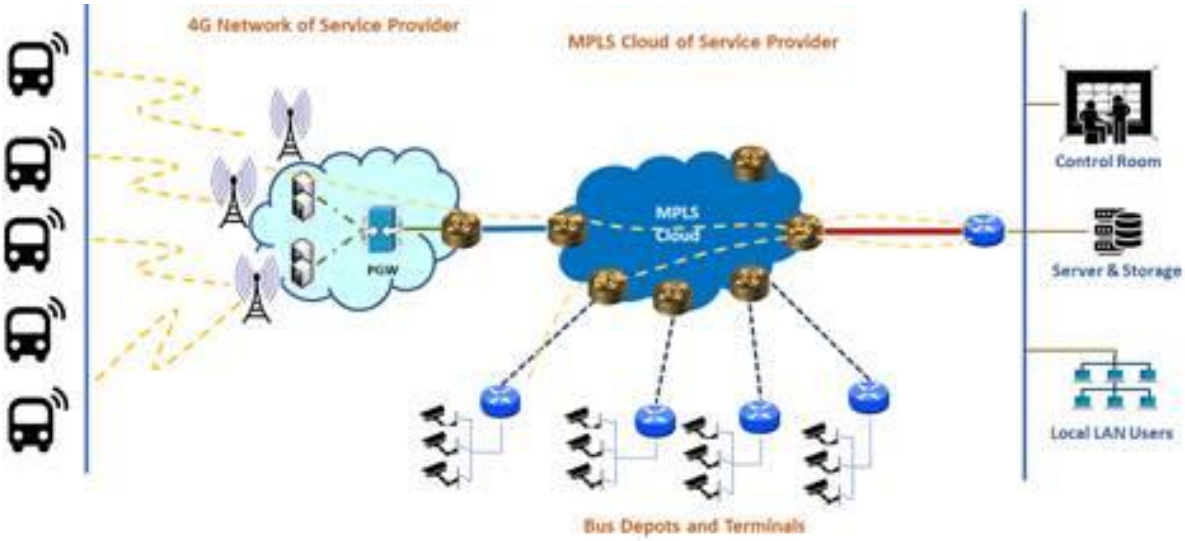
1.3.1.1 Cameras

The proposed mobile surveillance system will involve setting up of fixed IP Cameras inside the Buses, Depots and Terminals in the City of Chennai. The video surveillance data from various cameras deployed will be stored and monitored at the Command and Control Centre. The Mobile Surveillance System shall have provision for local storage of the video footage. The cameras shall also periodically send status, health and availability information back to the data center.

1.3.1.2 Network Connectivity

The surveillance system at Depots and Terminals is to be connected through dedicated network connectivity on High Availability mode. For the mobile Surveillance System (cameras inside the bus), the connectivity can be provisioned using 4G/5G. The Network shall be designed to meet the minimum SLA prescribed in this tender. Indicative bandwidth requirements are provided below:

- From Cameras inside the Bus to Data Centre – 4G connectivity.
- From Cameras inside the Bus Depots and Terminals to Data Centre - connectivity of minimum 20 mbps of MPLS bandwidth on high availability as per the proposed camera solution
- Minimum Estimated Bandwidth to Command & Control Centre – Dedicated connectivity – minimum 3 Gbps bandwidth depending on live view of number of cameras



1.3.1.3 Command and Control Centre

The vision of the Command and Control Centre (CCC) is to have an integrated view of all the surveillance initiatives undertaken by the Metropolitan Transport Corporation (MTC) to serve as a decision support engine for MTC personnel in day-to-day operations or during exigency situations. This dynamic response to situations, both proactive and re-active will truly make the surveillance operations, pertaining to the safety of women and children, “SMART”. Managing the complete incident life cycle is a critical element in CCC solutions. It requires the ability to detect performance anomalies i.e. KPIs, current status, leading indicators etc. that often serve as a precursor to an incident and continues with Situational Awareness, Situation Management and investigation / learning. The investigation / learning phase facilitates continuous improvement that improves all aspects of the incident handling process.

1.3.1.4 Smart Data Centre / Disaster Recovery Solution (H/w + S/w)

All the Safe City Data Centre, Data recovery and CCC application will be hosted in the Data Centre. Video and other relevant data will be stored centrally at the data centre. The data centre will have IT compute infrastructure, storage, network and security components. The data centre may be located in Chennai.

In case of a disaster or failure of the data center, video feed shall automatically switch to the Disaster Recovery Center and the Disaster Recovery Centre shall take over the function of the Data Centre .In normal situation, the data in data center shall be replicated in Disaster Recovery centre automatically in real time. The Disaster Recovery Centre (DRC) will also have IT compute infrastructure, storage, network and security components. The DRC shall be located anywhere in India on a different seismic zone. The DC/DR should be at a MeitY empaneled Cloud Service Provider and should be located within India.

2 Detailed Scope of Work

The following activities to be undertaken by the System Integrator (SI)

2.1 Overview of Phase I

The phase-1 will cover the work of the SI from the date of issue of LOA till the date of issue of commissioning certificate for the successful roll out of the Chennai Safe City solution.

2.1.1 Section 1 – Project Planning

The success of the project depends on the proper project planning and management. At the onset, the SI shall plan the project implementation in detail and should provide a micro level view of the tasks and activities required to be undertaken in consultation with MTC. An indicative list of planning related documentation that the SI should make at the onset is as follows:

- **Project Schedule:** A detailed week-wise timeline indicating various activities to be performed along with completion dates and resources required for the same
- **Manpower Deployment List:** A list needs to be provided with resources who will be deployed on the project along with the roles and responsibilities of each resource.
- **Infra Deployment List:** List and number of all infra (including but not limited to servers, storage, network components and software licenses) other than manpower that may be required.
- **Communication Plan**: Detailed communication plan indicating what form of communication will be utilized for what kinds of meeting along with recipients and frequency.
- **Progress Monitoring Plan:** Detailed Daily, Weekly, Monthly Progress Report formats along with issue escalation format. The format will be approved by MTC to the successful bidder before start of the project.
- **Standard Operating Procedures (SOPs):** Detailed Standard Operating Procedures for all the events and incidents to be developed and customized based on the Project scope and the functional requirement of the RFP. The SOPs will be approved by MTC to the successful bidder before the project implementation.
- **Risk Mitigation Plan:** List of all possible risks and methods to mitigate them.
- **Escalation Matrix & Incident Management:** A detailed list of key contact persons with contact details with escalation hierarchy for resolution of issues and problems. This has to be via an Incident Management system.
- **Traceability Matrix**: Chorological requirement matrix which capture the original requirements and subsequent changes with clear audit trail which shall used as reference during the for compliance checks in the Final Acceptance Testing.

2.1.2 Section 2 – Design of Safe City Solution

- The system Integrator should design, develop, implement, integrate and test the complete components as per the BOM provided in this RFP Vol I.
- Conducting site survey, obtaining necessary permissions, developing system requirements, standard operating procedures etc.
- Assessment of IT Infrastructure and Non-IT Infrastructure requirements, assessment of business processes, assessment of software requirements, assessment of integration requirement, assessment of connectivity requirement at all the field locations, DC and CCC.
- Formulation of solution architecture, detailed design of safe city solutions for the field location, DC and CCC, development of test cases (Unit, System Integration and User Acceptance), SOP documentation

2.1.2.1 Surveillance Solution Design Functional Architecture

Various components of the project, including expected system users, are as below and also depicted in the component architecture diagram below. The component architecture is indicative in nature and is given in the RFP to bring clarity to prospective bidders on the overall scope of project and its intended use. The successful bidder shall carry out the detail requirement analysis and finalize the technical architecture in consultation with authority and its consultants.

A. **Network Layer** - The secured network layer will serve as the backbone for the project and provide connectivity to gather data from field infra and communicate to the data centre / disaster recovery centre / control centre / field offices. The network bandwidth will be provided by Bidder; however, the selected bidder will have to size the bandwidth required for the overall solution, and supply and install the edge devices to utilize the network.

B. **Data Centre Layer** -The data centre layer will house centralized computing power required to store, process and analyse the video feeds and data to decipher actionable information. This layer includes servers, storage, ancillary network equipment elements, security devices and corresponding management tools. A disaster recovery site, which includes servers, storage, network equipment and security management systems will be used in case of fall back mechanism for the data centre.

C. **External Database / Application layer** – The database of various infrastructure such as surveillance camera, e-Governance applications in the City/State, etc., gets routed from this layer

D. **Control Centre Layer**: Big Data analysis, Dashboards, SOP and EMS, etc. enable administrators to get a holistic view of city conditions, and make informed decisions.

E. **User Layer**: All the stakeholders of this solution including direct & indirect beneficiaries would be part of this layer. They interact with CC solution through this layer with proper authentication.

F. **Cross-Functional Vertical Security Layer** - As multiple field devices are connected through a network, security of the entire system becomes of paramount significance and the SI will have to provide: Infrastructure security, Network security, Identity and Access Management, and Application security.

The system shall also provide the below capabilities for sustained functioning of safe city solution.

- **Scalability** - Important technical components of the architecture must support scalability up to 5000 MTC Buses to provide continuous growth to meet the growing demand of MTC. The system should also support vertical and horizontal scalability so that depending on changing requirements from time to time, the system may be scaled upwards. There must not be any system-imposed restrictions on the upward scalability in number of cameras or other edge devices. Main technology components requiring scalability are storage, bandwidth, computing performance (ICT Infrastructure), Software/application performance and advancement in camera features.
- **Availability** - The architecture components should be redundant and ensure that there is no single point of failure in the key solution components. Considering the high sensitivity of the system, design should be in such a way as to be resilient to technology sabotage. To take care of remote failure, the systems need to be configured to mask and recover with minimum outage. The Bidder shall make the provision for high availability for all the services of the system. Redundancy has to be considered at the core / data centre components level.
- **Security** - The architecture must adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft, natural disasters etc. Successful Bidder must make provisions for security of field equipment as well as protection of the software system from hackers and other threats. Using Firewalls and Intrusion Prevention Systems such attacks and theft should be controlled and well supported (and implemented) with the security policy. Virus and worm attacks should be well defended with gateway level Anti-virus system, along with workstation level Anti-virus mechanism. There should also be an endeavour to make use of the SSL/VPN technologies to have secured communication between Applications and its end users. Furthermore, all the system logs should be properly stored & archived for future analysis and forensics whenever desired. MTC may carry out the security audit of the entire system in approx. 3 months of Acceptance / operationalization through a Third-Party Auditor (TPA) once every 6 months and SI will have to bear the charges. The following guidelines need to be observed for security:

    - Build a complete audit trail of all activities and operations using log reports, so that errors in system – intentional or otherwise – can be traced and corrected.
    - The most appropriate level of security commensurate with the value to that function for which it is deployed must be chosen
    - Access Controls must be provided to ensure that the system is not tampered or modified by the system operators or unauthorized persons.
    - Implement data security to allow for changes in technology and business needs.

Field equipment installed through this Project would become an important public asset. During the implementation phase of the Project the SI shall be required to repair / replace any equipment if stolen/damaged. Appropriate insurance cover must be provided to all such field equipment. The SI shall also provide the same in price bid

- **Manageability** - Ease of configuration, ongoing health monitoring, and failure detection are vital to the goals of scalability, availability, and security and must be able to match the growth of the environment.
- **Interoperability** - The system should have capability to take feed from cameras installed by private / Govt. at public places, digitize (if required) & compress (if required) this feed & store as per requirements. Also system should have integration capabilities between various IT systems as indicated in scope of work. The system can integrate with social media platforms for social media monitoring. It may be noted that most of the systems deployed by these large private / public/community establishments use open standards. Bidder may carry out further study on the same.
- **Open Standards** - Systems should use open standards and protocols to the extent possible.
    - The Successful Bidder will be required to review the Technical Architecture suggested in the Tender and finalize the detailed architecture for the overall system, incorporating findings of site survey exercise. The network so envisaged should be able to provide real time data to the safe city Command and Control Centre / Data Centre / Field Offices and Tablets for select officials. All the components of the Technical Architecture should be of best industry standards.

2.1.2.2 Change Request during Design & Implementation

The SI shall design the solution dove tailed to the specific needs inline with proposed design and specifications proposed in their technical proposal to this RFP. Incase of any need for any changes in the design due to

- Any prevailing site & physical constraints
- Value proposition to better the requirements of the project

The same would be evaluated and put up by the SI during the design stage to the department. All such changes proposed due to external dependencies or value propositions would need to be presented shall have

- Technical superiority of the already proposed solution by the SI
- Successfully proven track record
- Commercial implementation

The department would constitute a Change Request Review committee would review the technical soundness, commercial implications and then would put its final recommendations to the authority for final decisions. This process would be in-sync would the Change-Request Management Process prescribed in the Phase II of this RFP.

The same vendor / OEM used during proof of concept shall also be used for the respective components during implementation

2.1.3 Section 3 – Supply, Installation, Testing & Commissioning of solution

2.1.3.1 Command and Control Centre

Scope of work for Command and Control Centre will include design and deployment of applications like ICCC Application, Video Management System (VMS), etc. Installation of hardware such as workstations, video wall, screens, printers, etc. and physical infrastructure including, lighting, fire detection and suppression, fixtures, cabling etc. System Integrator shall setup the ICT, and non-ICT infrastructure for Command and Control Centre including Building at the space available (Approximately 2264 Square Feet) at the MTC premises. The System Integrator shall do the site visit to estimate his work scope including demolition of existing Building, Civil Work envisaged, interiors and finishing.

The SI needs to create a CCC (to be approved by MTC) and shall arrange for all the necessary furniture like chairs, computer desks and other required IT components such workstation monitors, network connectivity to initiate the go-live.

2.1.3.1.1 CCC Site Preparation with Civil, Interior, Electrical & Network Works

The System Integrator shall build the identified site for commissioning of CCC as per TIA 942 standards used for building critical ICT based infrastructure. SI shall also ensure that and also bear all expenses for getting solution infrastructure certified by governing bodies such CEIG (for electrical work), pollution department and other statutory clearance for having the CCC in the building if required.

Floor layout design options shall be prepared by SI and presented to MTC for final decision making. Based on the approval of the same, SI shall work on detailed drawings for other interior, electrical & network layouts / drawings.

The design of CCC shall include the IT design (functional architecture, network topology, bandwidth sizing, compute & storage sizing, BOM with make & model) and Non-IT design (civil, interior, electrical, building safety/security control systems, BOM with make & model) and get the same approved by the authority. Subsequent to approval of the same, the site preparation shall be carried out towards successful commissioning before targeted commissioning period.

2.1.3.1.2 Commissioning of Video Wall for CCC Solution

The SI shall provide Video Wall of minimum 40Ft x 7Ft. In similar lines, the SI needs to propose the design for the approved site.

2.1.3.2 Data Centre / Disaster Recovery Services

The SI shall plan to host the Data Centre / Disaster Recovery Infrastructure on cloud environment. The SI shall, as per their strategy, adopt Infrastructure as a Service (IaaS) or choose collocate exclusive server/storage ear-marked for this project in the cloud environment. SI shall only use Ministry of IT, GoI's empaneled cloud service providers for the DC-DR cloud services of this project. It should be located within India. The DC-DR shall be designed in such a way that it supports the Business Continuity planning prescribed in section 2.1.3.6

The SI shall commission entire network connectivity from field location, to the destination as outlined above through the DC/DR cloud. The SI shall ensure that they DC/DR cloud shall comply with ISO 27001 certifications and ensure complete security compliance and prescribed service levels in this RFP.

2.1.3.3 Field level Components

- SI shall provide all the necessary field components required for the complete solution. The indicative BOM is provided in RFP Vol I.
- SI shall provide Power (provisioning of power including one-time charges and energy meter) and Network (Last mile including bandwidth - Internet & Intranet) at the field locations and CCC, DC / DR and viewing locations.
- SI has to mount the cameras required for this project ensuring future scalability. The SI has to submit the design to MTC for the approvals. After the confirmation from the authority, SI can install the Cameras at the respective locations.
- MTC shall appoint a team to accompany the SI during the joint site survey. It is the responsibility of the SI to organize the electrical and network service provider during the site survey.
- The location and direction of the cameras shall be finalized after the consultation with the MTC.
- SI shall provide last mile connectivity at all the field locations, DC/DR, CCC, Depots and Terminals. For the Backbone connectivity for the entire project, SI can propose their own network or any other network service provider.

2.1.3.4 Surveillance System

IP Surveillance cameras will be installed inside the MTC Bus, Depots and Terminals. SI shall present the design criteria / assumption for camera positioning, commissioning for different possible scenarios.

2.1.3.5 Connectivity

- SI is required to provide the data connectivity for all components on IP based protocol to the CCC and DC/DR. This would include 4G/5G on the Buses, Broadband Connectivity at Depots and Terminals and finally dedicated leased line at CCC.

- The SI would be responsible to design the network solution with adequate capacity and redundancy to meet the Service level requirements mentioned in the RFP.
- All the connectivity provided under this project should be secure and reliable
- Network throughput requirement (Both Internet & Intranet) should be adequate
- Backup requirement should be adequate

Detailed planning of hardware deployment and configuration should be submitted to the Authority. The configuration planning should include following details.

- Network architecture planning including
- VLAN configuration planning
- IP address planning
- Subnet planning and routing planning
- Firewall configuration planning
- Backup methodology
- Backup links between CCC & DC/DR

2.1.3.6 Business Continuity Planning

The CCC solution shall be designed on High Availability mode even during disaster situations with the following objectives

- Record/Resource Point Objective (RPO) : near to zero data loss
- Record/ Resource Time Objective (RTO) : 15 minutes

SI shall design the connectivity & infrastructure accordingly to meet this MTC requirement & Prescribed SLA.

2.1.4 Section 4 – Final Acceptance Testing

After successful installation of equipment in accordance with the requirements in the Tender, the Successful Bidder would need to carry out Final Acceptance Testing in 2 different phases

i. Unit Testing
ii. Integration Testing.

These tests would be carried out based on the test cases developed and validated by MTC. Apart from the functional testing of the entire system components, the testing would also verify following aspects:

- Configuration Testing (to ensure that all the components are configured properly)
- Security Testing (to review & evaluate security controls)

Final acceptance certificate shall be issued by MTC to the Successful Bidder after successful testing in a real time condition for trouble-free operation. The date on which final acceptance

certificate is issued for final phase shall be deemed date of the successful commissioning of the Project.

MTC shall consider implementation of 99 percent core infra components and 97 percent of cameras in the project as a sufficient condition for the Project Go-Live. Any delay by the Successful Bidder in the performance of its contracted obligations shall render the Successful Bidder liable to the imposition of appropriate liquidated damages or termination, unless agreed otherwise by Authority.

2.1.4.1 System Documents, User Documents

The Successful Bidder will provide documentation, which should follow the ITIL (Information Technology Infrastructure Library) standards. This documentation should be submitted as the Project undergoes various stages of implementation. Indicative list of documents include but not limited to:

- **Project Commencement Documentation**: Project Plan in giving out micro level activities with milestones & deadlines.
- **Cabling Layout:** SI shall submit the detailed cabling layout including cable routing, telecommunication closets and telecommunication outlet/ connector designations. The layout shall detail locations of all equipment and indicate all wiring pathways.
- **Equipment Manuals**: Original Manuals from OEMs.
- **Installation Manual**: For all systems and field infra
- **Training Material**: Training Material will include the presentations used for trainings and also the required relevant documents for the topics being covered. Training registers should be submitted for same.
- **User Manuals**: For all systems and field infra, required for operationalization of the system.
- **System Manual:** For all systems and field infra, covering detail information required for its administration.
- **Standard Operational Procedure (SOP) Manual**: The Bidder shall be responsible for preparing SOP Manual relating to operation and maintenance of each and every service as mentioned in this Tender. The draft process (SOP) document shall be formally signed off by MTC before completion of Final Acceptance Test. This SOP manual will be finalized by the Bidder within 2 months of operationalization of each phase, in consultation with the Authority and formally signed off by the Authority.

Note: The SI will ensure proper upkeep and updating of all documentation and manuals during the contractual period. The ownership of all documents, supplied by the SI, will be with MTC. Documents shall be submitted in two copies each in printed (duly hard bound) & in soft copy formats (indexed and searchable).

2.1.4.2 Compliance to Standards & Certifications

1. For a large and complex set up such as the Project, it is imperative that the highest standards applicable are adhered to. In this context, the SI will ensure that the entire Project is developed in compliance with the applicable standards.
2. During project duration, the SI will ensure adherence to prescribed standards as provided below:

S.No	Component/Application/System	Prescribed Standard
1.	Information Security	ISO 27001
2.	IT Infrastructure Management	ITIL specifications
3.	Service Management	ISO 20000 specifications
4.	Project Documentation	IEEE/ISO/CMMi (where applicable) specifications for documentation
5.	Cameras	CE, BIS, UL (Non-multilisted)

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

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

4. While writing the source code for application modules the SI should ensure high-quality documentation standards to improve the readability of the software module. An illustrative list of comments that each module contained within the source file should be preceded by is outlined below:

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

5. Apart from the above SI needs to follow appropriate coding standards and guidelines inclusive of but not limited to the following while writing the source code -

   - Proper and consistent indentation

- Inline comments
- Structured programming
- Meaningful variable names
- Appropriate spacing
- Declaration of variable names
- Meaningful error messages

6. Quality Audits
   MTC at its discretion, may also engage independent auditors to audit any/some/all standards/processes. The SI shall support all such audits as per calendar agreed in advance. The result of the audit shall be shared with the SI who has to provide an effective action plan for mitigations of observations/non-compliances, if any.

2.1.5 Section 5 - Training & Capacity Building

The proposed solution is critical to meet the objectives of the safe city initiative. Hence, it is imperative that necessary change management workshops/awareness camps are conducted for the stakeholders. The SI shall prepare the necessary content and conduct the change management workshop for the staff and the officers in batches.The selected System Integrator would be required to provide training on various aspects to enable effective use of the new system to achieve the envisaged outcomes.

1. The purpose of this section is to define the scope of work for training and capacity building to be implemented at various levels of MTC
2. The SI‘s scope of work also includes preparing the necessary documentation and learning aids required for successful delivery of such trainings.
3. The details provided in this section are indicative and due to the complex nature of the project, the number of training sessions and team size may increase over and above those proposed
4. Further the SI has to provide cost for additional and optional training sessions in its financial proposal in case more trainings are required. SI has to conduct such additional training sessions on MTC‘s request.
5. SI will develop a training and capacity building strategy that will also include a detailed plan of implementation
6. SI will get the Training and capacity building strategy including training material finalized with MTC before starting the training programs.
7. SI will prepare all the requisite audio/visual training aids that are required for successful completion of the training for all stakeholders. These include the following for all the stakeholders:
   a. Training manuals for MTC personnel and stakeholder departments
   b. Computer based training modules
   c. Video (recorded sessions) for CCC operations, back-end modules, business intelligence, dynamic reporting, etc.
   d. Presentations

e. User manuals
f. Operational and maintenance manuals for the required modules
g. Regular updates to the training aids prepared under this project

8. SI must plan all the training and its material keeping, defined and agreed SOPs as prime focus.
9. SI will maintain a copy of all the training material on the knowledge portal and access will be provided to relevant stakeholders depending on their need and role. The access to training on the portal would be finalized with MTC. SI has to ensure the following points:
    a. For each training session, the SI has to provide the relevant training material copies to all the attendees.
    b. The contents developed shall be the property of MTC with all rights
10. SI has to ensure that the training sessions held are effective and that the attendees would be able to carry on with their work efficiently. For this purpose, it is necessary that the effectiveness of training sessions is measured. The SI will prepare a comprehensive feedback form that will capture necessary parameters on measuring effectiveness of the training sessions. This form will be discussed and finalized with MTC.
11. After each training session, feedback will be sought from each of the attendees on either printed feedback forms or through a link available on the web portal. One member of the stakeholder group would be involved in the feedback process and he/she has to vet the feedback process. The feedback received would be reported to MTC for each training session.
12. For each training session, the SI will categorize the feedback on a scale of 1 to 10, where 10 will denote excellent and 1 will denote unsatisfactory.
13. The training session would be considered effective only after the cumulative score of the feedback (sum of all feedback divided by number of attendees) is more than threshold score decided by MTC.

2.1.5.1 Preparation of Training material

a) Training Plan: The selected System Integrator would be required to prepare a detailed training plan covering at least the trainings to be conducted, targeted audience, location, dates for training, duration and training content. The training plan would be submitted to the Department as per timelines mentioned in this RFP for feedback and approval from the Department.
b) Training Materials: The following minimum training materials will be required to be prepared by the selected System Integrator to facilitate the training of users:

Method of training	Brief description	Training Artifacts	Training Material Languages
Class room training (Hands-on training)	This approach can be adopted for departmental users.	• IT infrastructure and dummy data for hands-on training • Participant handouts • Online and Paper-based tests to evaluate the quality of learning and Training • Provision for online and paper-based feedback submission	• English • Tamil
Self-learning	This will be useful for both the departmental users and for stakeholder departments to learn system operations in the new application. This would include several self-learning methods for enablement of easy learning and adoption of the system	• Downloadable Computer Based toolkits, PPTs & videos on system operations and usage • FAQs • Online help modules with search by keywords, topic etc. • Online tests that may be taken up by the participant after completing the learning to evaluate his learning • Online forms to submit feedback on the quality of training material	• English • Tamil

Approval for training materials prepared should be obtained from MTC **at least 2 weeks** before delivery of the training program.

2.1.5.2 Staffing and Training

The selected System Integrator must ensure that the deployed trainers:

- possess needed skills and experience in the specific domains and are fully aware of the deployed systems and have a prior experience of training personnel in the Government sector
- are fluent in speaking and writing in English and Tamil

2.1.6 Section 6 – Solution Stabilization & Go-Live

After the successful demonstration of the Final Acceptance Testing of the solution (hardware & software), the solution is put for reliability, consistency & accuracy test for period of one month. During this stabilisation period, the solution shall successfully comply to the minimum Service Levels Prescribed.

During the Stabilisation period, through a designated agency, MTC shall assess the compliance to the SLA on a periodic basis.

Upon satisfactory compliance of the prescribed Service Levels as defined above, the CC solution shall be ready to be LIVE. Subsequently a Go-Live date is mutually agreed with MTC, taking into consideration – the number of residual days left in the quarter – when the solution is declared ready for Go-Live.

2.2 Overview of Phase II

The System Integrator shall operate, maintain and manage the safe city solution on 24x7 basis over a period of three years from the date of issue of commissioning certificate.

2.2.1 Detailed Phase-II Requirements

The SI shall provide Operation, Maintenance and Management services (phase II services) for the Safe City solution commissioned for a period of 3 years from the date of issue of Commissioning Certificate as per the Service Level Agreement (SLA) and as per the scope of terms & conditions in the tender.

The phase II services to be provided is as given below, but not limited to:

- The phase II services to be provided as per the approved requirements. During the phase II operation, MTC reserves the right to amend the tasks as per requirement.
- The phase II services shall cover the services to be provided through the CCC, and maintenance of all applications.

2.2.2 Section 1 – Operation & Maintenance Services

2.2.2.1 Post Implementation Services

Success of the Project would rely on how professionally and methodically the entire Project is managed once the implementation is completed. From the Systems Integrator perspective, this is a critical phase since the quarterly payments are linked to the SLA's in the post implementation phases. System Integrator, thus, is required to depute a dedicated team of professionals to manage the Project and ensure adherence to the required SLAs.

2.2.2.2 Post Implementation Scope for the Operation and Maintenance Phase:

- Deploying manpower for solution maintenance and monitoring support which includes change request management, bug tracking and resolution, production support, performing version and patch updates
- Annual technical support for all hardware and software components for the O & M period.
- Preventive, repair maintenance and replacement of hardware and software components as applicable under the warranty and AMC services during the contract period
- Provide a centralized Helpdesk and Incident Management Support till the end of contractual period
- Recurring refresher trainings for the users and Change Management activities
- Conducting DR testing through regular mock drills

2.2.2.3 Provision of the Operational Manpower to view the feeds at CCC

MTC personnel will be trained and deployed as CCC operators by the SI. In addition to that, SI shall provide suitable manpower to monitor the feeds at Control Centre and support MTC in operationalisation of the Command and Control Centre. The exact role of these personnel and their responsibilities would be defined and monitored by MTC personnel.

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

- Shall be at least graduates
- Shall be without any criminal background / record
- MTC 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.
- System Integrator shall replace any person, if not found suitable for the job.

All the manpower should undergo training from the System Integrator for at least 15 working days on the working of Control Centre. Training should also cover dos & don'ts and will have a few of the below mentioned:

- Sessions from MTC officers on right approaches for monitoring the feeds & providing feedback to Police Personnel / Surveillance System and other components.
- Each person shall have to undergo compulsory 1 day training every month
- Operational Manpower shall work in 3 shifts, with no person being made to see the feeds for more than 8 hours at a stretch.

Detail operational guideline document shall be prepared during implementation which shall specify in detail the responsibilities of these resources and their do's & don'ts.

MTC reserves the right to include or exclude this scope of providing operational manpower in the project or include it partly at the time of signing of the contract or during execution of the contract.

2.2.3 Section 2 – Facility Management Services

2.2.3.1 Application Monitoring and Administration

- Monitoring all the applications on a day-to-day basis to ensure application availability and reliability.
- Monitor application to ensure that the application does not suspend, hang etc.
- Monitor components, including but not limited to, Application servers, Web Servers, Middleware and other application servers on an ongoing basis to ensure smooth functioning of the applications.
- Expertise in the application to have the ability to troubleshoot problems, monitor erratic behaviour through the application logs
- Configuration reviews to isolate bottlenecks and bring out parameters affecting the performance.
- Performance monitoring of the application and facilitating performance tuning.
- Maintenance of application response time logs.
- Manage patch upgrade as and when required with minimal downtime.
- Ensure configuration management and backups of patch to facilitate rollback in case of problems.
- Asset Management Services

2.2.3.2 Managed Services

Managed Services shall include a range of services related to the infrastructure services at the CCC, DC & near DR, and management of all the applications. Following services shall form a part of managed services:

2.2.3.3 Monitoring and Management Services

The system integrator shall provide the following monitoring and management services at the DC/DR and CCC.

- Server Monitoring, Administration & Management Services
- Database Administration & Management Services
- Storage Administration & Management Services
- Backup & Restore Services
- Security Administration Services.

2.2.3.4 Server Monitoring, Administration & Management Services

The activities shall include but not limited to:

- Configuration of server parameters, operating systems administration and tuning.

- Operating system administration, including but not limited to management of users, processes, resource contention, preventive maintenance and management of updates & patches to ensure that the system is properly updated.
- Re-installation in the event of system crash/failures.
- Maintenance of a log of the performance monitoring of servers including but not limited to monitoring CPU, disk space, memory utilization, I/O utilization, etc.
- Event log analysis generated in all the sub systems including but not limited to servers, operating systems, databases, applications, security devices, messaging, etc.
- Ensuring that the logs are backed up and truncated at regular intervals.
- Periodic health check of the systems, troubleshooting problems, analysing and implementing rectification measures.
- Identification, diagnosis and resolution of problem areas and maintenance of assured SLA levels.
- Implementation and maintenance of standard operating procedures for maintenance of the infrastructure.
- Management of the user names, roles and passwords of all the relevant subsystems, including, but not limited to servers, applications, devices, etc.
- System administration activities shall include tasks including but not limited to setting up the servers, executing hardware and software updates when necessary.

2.2.3.5 Database Administration & Management Services

The activities shall include but not limited to:

- End-to-end management of database on an ongoing basis to ensure smooth functioning of the same.
- Management of changes to database schema, disk space, storage, user roles.
- Conduct code and configuration reviews to provide tuning inputs to relevant stakeholders for improving the application performance or resolve bottlenecks, if any.
- Performance monitoring and tuning of the databases on a regular basis including, preventive maintenance of the database as required.
- Management of database upgrade or patch upgrade as and when required with minimal downtime.
- Regular backups for all databases in accordance with the backup and archive policies and conduct recovery whenever required with appropriate permissions

2.2.3.6 Storage Administration & Management Services

The activities shall include but not limited to:

- Installation and configuration of the storage system.
- Management of storage environment to maintain performance at desired optimum levels.

- Development of storage management policy, configuration and management of disk array, SAN fabric / switches, NAS, tape library, etc.
- Configuration of SAN shall include activities such as management of storage space, volume, RAID configuration, LUN, zone, security, business continuity volumes, NAS, performance, etc.

2.2.3.7 Backup and Restore Services

The activities shall include but not limited to:

- Backup of operating system, database and application as per stipulated policies.
- Monitoring and enhancement of the performance of scheduled backups, schedule regular testing of backups and ensure adherence to related retention policies.
- Ensuring prompt execution of on-demand backups of volumes, files and database applications whenever required by department or in case of upgrades and configuration changes to the system.
- Real-time monitoring, log maintenance and reporting of backup status on a regular basis. Prompt problem resolution in case of failures in the backup processes.
- Media management including, but not limited to, tagging, cross-referencing, storing, logging, testing, and vaulting in fire proof cabinets.
- Physical security of the media stored in cabinets.
- Ongoing support for file and volume restoration requests
- A backup of all transactions shall be done so that in case of any disaster / emergency at the Data Centre, the DR will have all the data.
- SI shall be responsible for supply, install, test & commission of the backup storage of the archival of data.

2.2.3.8 Security Administration Services

The activities to be carried out under security administration shall include, but not limited to:

- Addressing the ongoing needs of security management including, but not limited to, monitoring of various devices / tools such as firewall, intrusion detection, content filtering and blocking, virus protection, and vulnerability protection through implementation of proper patches and rules.
- Root domain administration by creating the root and sub-domains and setting the root level security policies such as authentication mechanisms (single/multi factor), password policies such as password length, password complexity, password expiry, account lockout policy, certificate policies, IPSEC policies, etc.
- Maintaining an updated knowledge base of all the published security vulnerabilities and virus threats for related software and microcode, etc.
- Ensuring that patches / workarounds for identified vulnerabilities are patched / blocked immediately.

- Respond to security breaches or other security incidents and coordinate with respective OEMs in case of a new threat is observed to ensure that workaround / patch is made available for the same.
- Provide a well-designed access management system, security of physical and digital assets, data and network security, backup and recovery etc.
- Maintenance and management of security devices, including, but not limited to maintaining firewall services to restrict network protocols and traffic, detecting intrusions or unauthorized access to networks, systems, services, applications or data, protecting email gateways, firewalls, servers, from viruses.
- Ensuring that the security policy is maintained and updates to the same are made regularly as per ISO 27001, ISO 20000 and BS 15000 guidelines

2.2.3.9 Network management & Monitoring Services

The activities shall include but not limited to:

- The SI shall ensure the management of network environment to maintain performance at optimum levels on a 24 x 7 basis.
- The SI shall monitor and administer the network connectivity provided for CCC, DC/DR and field locations.
- The SI shall create and modify VLAN, assignment of ports to appropriate application traffic.

2.2.3.10 Change Management

- Tracking the changes in hard / soft configurations, changes to applications, changes to policies, applying of upgrades / updates / patches, etc.
- Plan for changes to be made - draw up a task list, decide on responsibilities, coordinate with all the affected parties, establish and maintain communication between parties to identify and mitigate risks, manage the schedule, execute the change, ensure and manage the port change tests and documentation.
- SI shall be responsible for making any changes demanded by MTC anytime during the contract period. The SI needs to adequately plan & deploy to carry out the change in the agreed timeline without any additional charge
- In case of any additional requirement which mandates additional developmental activities in any of the applications, then SI shall do the same as per requirements of MTC without any additional charge. Therefore SI shall plan to deploy adequate resources during the Phase II – Operation & Maintenance phase as well.

2.2.3.11 Change request

The system Integrator shall ensure that the change requests for any of the components (Hardware / Software) are deployed after carrying out the following technical tasks to ensure smooth roll out of the change request.

- Functional Testing: Ensuring that the Hardware/ Software functionality meets the functional and technical requirements of the project.
- Performance Testing: Ensuring that the Hardware/ Software meets expressed performance requirements.
- Security Testing: Testing for exploitable application security weaknesses that undermine the application security or the security of the infrastructure.

2.2.3.12 Periodic Security and Performance Testing & Conformance

SI shall conduct Security and Performance testing by the CERT-IN empaneled TPA (preferred to use the same TPA) agency approved by MTC. Any approved Change Request in any of the components (Hardware/ Software) would call for Vulnerability, security & performance audit. The SI shall also plan to conduct, in half-yearly basis

- Audit of application vulnerability
- Security for both application & compute
- Performance load testing for application & network connectivity assessment

In case of any degradation identified in this periodic assessment the SI needs to highlight proactive measures to mitigate the same. Any Non-conformance & vulnerability aspects identified by the TPA during this exercise need to be immediately mitigated & closed before 2 weeks of succeeding quarter. In case of any default there would penalty levied as per SLA & Tender conditions

2.2.3.13 SLA monitoring

The Service Level mentioned in the RFP needs to be captured, analyzed & reported to the MTC. The consultant & department nodal officers shall review the SLA reports & ratify the same on a quarterly basis. Based on the ratification of SLA/performance reports, the payments would be estimated i.e. after deducting any penalties and the same would be released to SI.

2.2.4 Section 3 – Knowledge Transfer & Exit Management

i. This sets out the provisions, which will apply on expiry or termination of the Master Service Agreement, the Project Implementation, Operation and Management SLAs.
ii. In the case of termination of the Project Implementation and/or Operation and Management, the Parties shall agree at that time whether, and if so during what period, the provisions of this Schedule shall apply.
iii. The Parties shall ensure that their respective associated entities carry out their respective obligations set out in this Exit Management Schedule.

2.2.4.1 Cooperation and Provision of Information

During the exit management period:

i. The SI will allow the MTC or its nominated agency access to information reasonably required to define the then current mode of operation associated with the provision of the services to enable the MTC to assess the existing services being delivered.

ii. Promptly on reasonable request by the MTC , the 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 System integrator or sub-contractors appointed by the SI). The MTC shall be entitled to a copy of all such information. Such information shall include details pertaining to the services rendered and other performance data. The SI shall permit the MTC or its nominated agencies to have reasonable access to its employees and facilities, to understand the methods of delivery of the services employed by the SI and to assist in appropriate knowledge transfer.

2.2.4.2 Confidential Information, Security and Data

i. The SI will promptly on the commencement of the exit management period supply to the MTC or its nominated agency the following:

- Information relating to the current services rendered and customer and performance data relating to the performance of sub-contractors in relation to the services;
- Documentation relating to Intellectual Property Rights;
- Documentation relating to sub-contractors;
- All current and updated data as is reasonably required for purposes of MTC or its nominated agencies transitioning the services to its Replacement SI in a readily available format nominated by the MTC or its nominated agency;
- All other information (including but not limited to documents, records and agreements) relating to the services reasonably necessary to enable MTC or its nominated agencies, or its Replacement SI to carry out due diligence in order to transition the provision of the Services to MTC or its nominated agencies, or its Replacement System integrator (as the case may be).

ii. Before the expiry of the exit management period, the SI shall deliver to the MTC or its nominated agency all new or up-dated materials from the categories set out in Schedule above and shall not retain any copies thereof, except that the SI shall be permitted to retain one copy of such materials for archival purposes only.

2.2.4.3 Knowledge Transfer of Certain Agreements

On request by the MTC or its nominated agency, the SI shall effect such assignments, transfers, licences and sub-licences to MTC, or its Replacement SI in relation to any equipment lease, maintenance or service provision agreement between SI and third party lessors, vendors, and which are related to the services and reasonably necessary for the carrying out of replacement services by the MTC or its nominated agency or its Replacement SI.

2.2.4.4 General Obligations of the SI

i. SI shall provide all such information as may reasonably be necessary to effect as seamless a handover as practicable in the circumstances to the MTC or its nominated agency or its Replacement SI and which the SI has in its possession or control at any time during the exit management period.
ii. For the purposes of this Schedule, anything in the possession or control of any SI, associated entity, or sub-contractor is deemed to be in the possession or control of the SI.
iii. SI shall commit adequate resources to comply with its obligations under this Exit Management Schedule.

2.2.4.5 Exit Management Plan

i. SI shall provide the MTC or its nominated agency with a recommended exit management plan ("Exit Management Plan") which shall deal with at least the following aspects of exit management in relation to the Master Service Agreement (MSA) as a whole and in relation to the Project Implementation, and the Operation and Management SLA.
   - A detailed program of the transfer process that could be used in conjunction with a Replacement SI including details of the means to be used to ensure continuing provision of the services throughout the transfer process or until the cessation of the services and of the management structure to be used during the transfer;
   - Plans for the communication with such of the SI's sub-contractors, staff, suppliers, customers and any related third party as are necessary to avoid any material detrimental impact on the MTC 's operations as a result of undertaking the transfer;
   - (If applicable) proposed arrangements for the segregation of the SI's networks from the networks employed by MTC and identification of specific security tasks necessary at termination;
   - Plans for provision of contingent support to MTC, and replacement SI for a reasonable period after transfer.
ii. SI shall re-draft the Exit Management Plan annually thereafter to ensure that it is kept relevant and up to date.
iii. Each Exit Management Plan shall be presented by the SI to and approved by the MTC or its nominated agencies.
iv. The terms of payment as stated in the Terms of Payment Schedule include the costs of the SI complying with its obligations under this Schedule.
v. In the event of termination or expiry of MSA, and Project Implementation, each Party shall comply with the Exit Management Plan.
vi. During the exit management period, the SI shall use its best efforts to deliver the services.
vii. Payments during the Exit Management period shall be made in accordance with the Terms of Payment Schedule.
viii. This Exit Management plan shall be furnished in writing to the MTC or its nominated agencies within 90 days from the Effective Date of this Agreement.

3 Service Level Agreement (SLA)

- Service Level Agreement (SLA) shall become the part of contract between MTC and the successful bidder. SLA defines the terms of the successful bidder's responsibility in ensuring the timely delivery of the deliverables and the correctness of the same based on the agreed Performance Indicators as detailed in this section.
- The successful bidder has to comply with service level requirements to ensure adherence to project timelines, quality and availability of services, throughout the period of this contract i.e. during implementation phase and for a period of three (3) years. The successful bidder has to supply appropriate software/hardware/ automated tools as may be required to monitor and submit reports of all the SLAs mentioned in this section.
- For purposes of the SLA, the definitions and terms as specified in the document along with the following terms shall have the meanings set forth below:
    - **"Total Time"** - Total number of hours in the quarter (or the concerned period) being considered for evaluation of SLA performance.
    - **"Uptime"** – Time period for which the specified services/ outcomes are available in the period being considered for evaluation of SLA. Formulae for calculation of Uptime: Uptime (%) = {1-[(Downtime)/(Total time- scheduled maintenance time)]}*100
    - **"Downtime"**- Time period for which the specified services/ components/ outcomes are not available in the concerned period, being considered for evaluation of SLA, which would exclude downtime owing to Force Majeure & Reasons beyond control of the successful bidder.
    - **"Scheduled Maintenance Time"** - Time period for which the specified services/ components with specified technical and service standards are not available due to scheduled maintenance activity. The successful bidder is required to take at least 10 days prior approval from the Authority for any such activity. The scheduled maintenance should be carried out during non-peak hours (like post mid-night, and should not be for more than 2 hours. Such planned downtime would be granted max 2 times a year.
    - **"Incident"** - Any event / abnormalities in the service being rendered, that may lead to disruption in normal operations and services to the end user.
    - **"Response Time"** - Time elapsed from the moment an incident is reported in the Helpdesk over phone or by any applicable mode of communication, to the time when a resource is assigned for the resolution of the same.
    - **"Resolution Time"** - Time elapsed from the moment incident is reported to Helpdesk either in person or automatically through system, to the time by which the incident is resolved completely and services as promised are restored.

3.1.1 Implementation SLAs

These SLAs shall be used to evaluate the timelines for completion of deliverables that are listed in the deliverable.

Delay (Weeks)	Penalty (INR)
For every one week of delay for Go-Live Date	0.1% of total CAPEX of the undelivered portion for every week of delay
For every one week of delay beyond 10 weeks from Go-Live Date	0.2% of total CAPEX of the undelivered portion for every week of delay, subject to the total cumulative penalty capped at 10% of CAPEX

In case the penalties for the selected bidder reaches 10% of the CAPEX value in the form of penalty, cumulative of penalties for all elements, at any point of time during the implementation phase, MTC reserves the right to invoke the termination clause.

3.1.2 Operation & Maintenance SLAs

- These SLAs shall be used to evaluate the performance of the services on quarterly basis.
- Penalty levied for non- performance as per SLA requirements shall be deducted through subsequent payments due from MTC.
- The upper limit of penalty would be capped at 10% of the OPEX value for each quarter. In case the calculated penalty crosses 10% penalty of the OPEX value in 2 subsequent quarters, MTC reserves the right to invoke the termination clause.
- Uptime definition: All devices have to be working and deliver the desired results. The no. of hours that the particular device/ equipment does not work will be treated as down time. Uptime shall be calculated as Uptime (%) = {1-[(Downtime)/ (Total time- scheduled maintenance time)]}*100. For ex, if 10 nos. of cameras are deployed at various locations, and 2 cameras does not work for 5 Hrs, the total non-working device hours will be 10 unit hours (and the uptime would be {1-((2*5)/(10*30*24)}, 10 being the number of units, for 30 days on 24 hours basis.
- The penalties would be levied for every unit down time hour

3.1.2.1 SLA and Penalty for Response and Resolution time

In any circumstances the total cumulative penalty derived from SLA non-compliances that may be levied on the SI shall be capped to 10% of OPEX of Price Bid.

<table>
<tr><th>S.No</th><th>Parameter</th><th>Penalty</th></tr>
<tr><td>1.</td><td>Core Infrastructure:
Centralized Infrastructure availability & Performance degradation of all the hardware, software, network connectivity, surveillance Solution, Portal, etc. that are deployed by the SI</td><td>
<table>
<tr><th>Uptime per each Camera level</th><th>Penalty (%)</th></tr>
<tr><td>> 99.9 %</td><td>Nil</td></tr>
<tr><td>>98% & less than 99.9%</td><td>1% on the OPEX payable</td></tr>
<tr><td>For Every 0.5% drop from <98%</td><td>Additional 2% on the OPEX payable, CAPPED at 10% of OPEX</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>S.No</th><th>Parameter</th><th>Penalty</th></tr>
<tr><td></td><td>SLA Period of Measurement hours: 24x7x1 month</td><td></td></tr>
<tr><td>2.</td><td>Field Infra Critical : (camera service)
Service Availability/functionality & Performance degradation of all the hardware, software, network connectivity (Depots & Terminals only), etc.

SLA Period of Measurement hours: 24x7x1 month</td><td>
<table>
<tr><th>Uptime per each Camera level</th><th>Penalty (%)</th></tr>
<tr><td>> 99 %</td><td>Nil</td></tr>
<tr><td>>98% & less than 99%</td><td>1% on the OPEX payable</td></tr>
<tr><td>For Every 0.5% drop from <98%</td><td>Additional 2% on the OPEX payable, CAPPED at 10% of OPEX</td></tr>
</table>
</td></tr>
</table>

3.1.2.2 SLA for Business Continuity Planning

S.No	Parameter	Metric	Frequency	Penalty
1.	Data Loss	Near to zero	At all times	For loss of every 5 MB of data, 0.2% on OPEX payable capped to 10% OPEX
2.	Returning to Business-as-usual	RTO <= 15 minutes	At all times	For loss of every 1 minute delay of RTO above 15 minutes, 0.2% on the OPEX payable capped to 10% OPEX

3.1.2.3 SLA for Change Requests or enhancements

- For every week delay from T (mutually agreed timeline for change request between SI & Authority before commencing the CRM), a Penalty for Change Request for Low, Medium & High criticality of changes shall be 0.05%, 0.075% & 0.1% of OPEX respectively.
- For every week delay in providing replacement of Key Resources (as per Vol. I) from the approved date of exit of the key resource from the project, shall attract a penalty of INR 5000 per day per resource
- For every solution Security-breach / Vulnerability attack with severity level of 1, 2, 3 & 4 (as defined in section 3.1.2.4) then a penalty of 2%, 1.5%, 1%, and 0.5% of OPEX respectively and in case of similar attacks of more than three attacks may lead to termination of contract.

S.No	Parameter	Metric	Frequency	Penalty
1.	Criticality of Change – Low	< T, where T is the timeframe for completion of the Change request	Weekly per Occurrence	For every week delay from T (mutually agreed timeline for change request between SI & Authority

S.No	Parameter	Metric	Frequency	Penalty
		as agreed upon by Authority and successful bidder		before commencing the CRM), a Penalty for Change Request for Low, Medium & High criticality of changes shall be 0.05%,.075% & 0.1% of OPEX respectively
2.	Criticality of Change – Medium	< T, where T is the timeframe for completion of the Change request as agreed upon by Authority and successful bidder	Weekly per Occurrence	
3.	Criticality of Change – High	< T weeks, where T is the timeframe for completion of the Change request as agreed upon by Authority and successful bidder	Weekly per Occurrence	
4.	Resource Replacement	Within 7 days of exit of resource (in case of Authority initiated or supplier initiated)	Per Occurrence	For every week delay in providing replacement of Key Resources (as per Vol. I) from the approved date of exit of the key resource from the project, shall attract a penalty of INR 5000 per day per resource
5.	Application Security	Cyber Crime / Hacking / Data Theft / Fraud attributable to the SI	Per Occurrence	"Depending on the type of incident and its impact, a Penalty of 10% on the "Section I total OPEX "or in case of severe issue (as defined by Authority) such breach may lead to termination clause of contract"

3.1.2.4 Definitions

- Severity 1: Control Centre down for more than 70% users (OR) VMS down for more than 70% cameras / 70% users
- Severity 2: Control Centre down for more than 30% users (OR) VMS down for more than 30% cameras / 30% users
- Severity 3: Control Centre down for more than 10% users (OR) VMS down for more than 10% cameras / 10% users
- Severity 4: Minor functionality issues with Control Centre (OR) VMS
- Response Time: Response time is defined as the time the support vendor takes to respond from the time that ticket was raised.
- Resolution Time: Resolution time is defined as the time the vendor takes to resolve the issue or provide acceptable workaround for the issue

3.1.2.5 Conditions for No Penalties

Penalties shall not be levied on the Bidder in the following cases:

- There is a force majeure event effecting the SLA which is beyond the control of the successful bidder. Force Majeure events shall be considered in line with the clause mentioned RFP.
- The non-compliance to the SLA has been due to reasons beyond the control of the successful bidder.

Theft cases by default / vandalism would **NOT** be considered as "beyond the control of bidder". Hence, the Bidder should be taking adequate anti-theft measures, spares strategy, Insurance as required to maintain the desired Required SLA. But some theft will be handled on case to case to basis

4 Project Implementation Timelines

The implementation timelines for the project components are as given below.

- T = Date of signing of Contract Agreement
- G= Go-Live Dates for surveillance solution

S.No	Milestone	Timelines
1.	Solution Design Sign-off	T + 30 days
2.	Supply of all ICT & Non-ICT infrastructure for the Solution	T + 120 Days
3.	Installation of all ICT & Non-ICT infrastructure for the Solution	T+ 210 Days
4.	Unit Testing by System Integrator	T + 240 Days
5.	Final Acceptance Testing	T+ 270 Days
6.	Solution stabilization & Go-Live	G = T + 300 Days
7.	Operations & Maintenance Phase for a period of 3 years	G+12 Quarters
8.	36th month – Project Closures Exit Management	G+ 12th Quarter

5 Functional and Technical Requirements

5.1 Command & Control Centre

5.1.1 Functional Specifications

5.1.1.1 Functional Specifications of the Application Software

Various functional requirements of the CCC application System are given in the table below:

S.No	Functions	Minimum Specifications
1.	Solution & Platform	The Command & Control solution should be implemented and complied to the industry open standards based Commercial-of-the-shelf (COTS) products.
2.		The CCC shall embody the following characteristics: i. Client/server architecture ii. Support multi-site, multiple-hierarchy deployment iii. Provide clear scalability iv. Central administration capability v. Support local redundancy and high availability options vi. Employ encrypted communications over TCP/IP LAN's and WAN's vii. Capable of running in a virtual environment viii. Provide a mechanism to define key performance indicators, trends, leading indicators and visualize the indicators on a web based configurable dashboard infrastructure ix. Provide a mobile portal to allow viewing of incidents and relevant details x. Display a configurable indication of overall situation and threat level xi. Provide communication capability to include email, text, telephone, intercom, mass notification, and application-based messages xii. Support a mobile app for field personnel, which enables its users to receive incident details (including: photos and videos) and a comprehensive set of GIS capabilities, to ensure collaborative response aligned with the Command & Control room's operator xiii. Support the simulation of events, such as alarms, for training purposes.
3.		Software (Application, Database and any other) must not be restricted by the license terms of the OEM from scaling out on unlimited number of cores and servers during future expansion.

S.No	Functions	Minimum Specifications
4.		System must provide a comprehensive API (Application Programming Interface) or SDK (Software Development Kit) to allow interfacing and integration with existing systems.
5.		The solution should be network and protocol agonistic and provide option to connect legacy system through APIs with either read, write or both options. It should connect diverse on premise and/or cloud platforms and makes it easy to exchange data and services between them.
6.		The system shall allow seamless integration with all of the department's existing and future initiatives (e.g. open source intelligence)
7.		The platform should be able to integrate with any type of sensor platform being used for the urban services irrespective of the technology used. The platform should also allow the manufacturers of the sensors to develop integrations themselves using SDKs without affecting the northbound applications and existing integrations
8.	Convergence of Multiple feeds / services	System need to have provision that integrates various services and be able to monitor them and operate them. The solution should provide option to integrate existing deployed solution by City and also need to provide scalability option to implement new use cases. System should have capability to source data from various systems implemented in Chennai (being implemented as part of this project or other projects) to create actionable intelligence
9.	Industry Standards for the CCC	The solution should adhere to the industry standards for interoperability, data representation & exchange, aggregation, virtualization and flexibility
10.		IT Infrastructure Library (ITIL) standards for Standard Operations Plan & Resource Management
11.		Geo Spatial Standards like GML & KML etc.
12.		Business Process Model and Notation (BPMN) or equivalent for KPI Monitoring.
13.	CCC Operations	The solution shall provide a unified viewing and management GUI that enables operators to manage situations in a consistent manner, regardless of underlying integrated systems.
14.		The Solution shall process events automatically, perform correlations, prioritization and rule based calculations based on a predefined business logic.
15.		The Solution shall facilitate the management of situations, as opposed to individual alarms

S.No	Functions	Minimum Specifications
16.		The Solution shall have facilities to support routine management, such as scheduler, tour management tool, intercom and messaging and allow seamless escalation from routine to emergency management.
17.		The Solution shall have applications to support the complete operational cycle of Planning, Responding and Debriefing.
18.		The Solution shall support the planning and activation of dynamically adapting response plans to real time varying situations.
19.		The Solution shall have an at-a-glance operational status view that will indicate all exceptions such as alarms, outstanding events that still require attention, and escalations.
20.	Incident Management Requirements	The system must provide Incident Management Services to facilitate the management of response and recovery operations:
21.		Define conditional tasks with pre-configured branching options for presentation to users and with procedures and response plans which change dynamically based on users' selections
22.		Define automatic procedure tasks that initiate actions, including i. sending messages ii. displaying video iii. popping up pre-configured GIS map views iv. adjusting incident's details, such as editing incident name or raising the severity level v. inserting another procedure into action
23.		Define key performance indicators, trends, leading Indicators for visualization on a web-based configurable dashboard
24.		configure and monitor service levels and trigger actions for monitored key performance indicators
25.		Should support for multiple incidents with both segregated and/or overlapping management and response teams.
26.		Should support Geospatial rendering of event and incident information.
27.		Should support plotting of area of impact using polynomial lines to divide the area into multiple zones on the GIS maps.
28.		GIS map functions shall include 2D and 3D views, synchronized, displaying the same objects and areas, and easily switched from one view to the other
29.		The GIS map function shall provide the ability to track movements, real-time and historical, and status of all location-based technologies, including GPS and RFID
30.		The GIS map function shall further support the following:

S.No	Functions	Minimum Specifications
		i. layer types capable of being toggled on/off per pre-defined rule ii. saving of multiple GIS map views for later on-demand or automatic popup iii. customization and real time activation of multiple-level drill downs by linking objects placed on map layers to other GIS view iv. definition and drawing of zones of arbitrary shapes and sizes and rendering as layers
31.		An operator shall be able to perform below on GIS map views i. place of predefined objects on map locations to include cameras, alarm points, vehicles, and people ii. add points, polylines, and polygons to maps to identify multiple locations related to an incident iii. place or directly open incidents on a map iv. filter display multiple locations related to an incident
32.		Should support incorporation of resource database for mobilizing the resources for response.
33.		Should provide facility to capture critical information such as location, name, status, time of the incident and be modifiable in real time by multiple authors with role associated permissions (read, write). Incidents should be captured in standard formats to facilitate incident correlation and reporting.
34.		The system must identify and track status of critical infrastructure / resources and provide a status overview of facilities and systems
35.	Integrated User Specific & Customizable Dashboard	Should provide integrated dashboard with an easy to navigate user interface for managing profiles, groups, message templates, communications, tracking receipts and compliance
36.		Should provide current status (snapshot) of organization's facilities, departments and a holistic perspective of incidents and situations, including incident handling time, number of false alerts, and number of active and closed incidents
37.		i. Collects major information from other integrated City sensors/platforms. ii. Should allow different inputs beyond cameras, such as, PC screen, web page, and other external devices for rich screen layout iii. Multi-display configurations iv. Use of GIS tool which allows easy map editing for wide area monitoring (Google map / Bing map / ESRI Arc GIS map / Any Open Source Map).

S.No	Functions	Minimum Specifications
38.		Should provide dashboard filtering capabilities that enable end-users to dynamically filter the data in their dashboard based upon criteria, such as region, dates, product, brands, etc. and capability to drill down to the details
39.	Integration with Social Media & Open Source Intelligence	Should provide integration of the Incident Management application with the social media. Should provide analytics based on the social media feed collected from the open source intelligence and collate with the surveillance inputs to alert the responders for immediate action on the ground.
40.		Should extract messages and display it in an operational dashboard.
41.		Should be able to correlate the extracted message from social media with existing other events and then should be able to initiate an SOP.
42.		Should be able to identify critical information and be able to link it to an existing SOP or a new SOP should be started.
43.		Should provide notifications to multiple agencies and departments (on mobile) that a new intelligence has been gathered through open source/social media.
44.	Device Status, Obstruction Detection and Availability Notification	Should provide icon based user interface on the GIS map to report non-functional device.
45.		Should also provide a single tabular view to list all devices along with their availability status in real time.
46.		Should provide User Interface to publish messages to multiple devices at the same time.
47.	Event Correlation	Command & Control Centre should be able to correlate two or more events coming from different subsystems (incoming sensors) based on time, place, custom attribute and provide correlation notifications to the operators based on predefined business and operational rules in the configurable and customizable rule engine.
48.	Standard Operations Procedures (SOP)	Command & Control Centre should provide for authoring and invoking un-limited number of configurable and customizable standard operating procedures through graphical, easy to use tooling interface.
49.		Standard Operating Procedures should be established, approved sets of actions considered to be the best practices for responding to a situation or carrying out an operation.
50.		The solution shall provide a visual environment to design business workflow processes that map business rules into a set of workflows to provide automatic responses.

S.No	Functions	Minimum Specifications
51.		The users should be able to edit the SOP, including adding, editing, or deleting the activities.
52.		The users should be able to also add comments to or stop the SOP (prior to completion).
53.		There should be provision for automatically logging the actions, changes, and commentary for the SOP and its activities, so that an electronic record is available for after-action review.
54.		The SOP Tool should have capability to define the following activity types:
55.		**Manual Activity** - An activity that is done manually by the owner and provide details in the description field.
56.		**Automation Activity** - An activity that initiates and tracks a particular work order and select a predefined work order from the list.
57.		**If-Then-Else Activity** - A conditional activity that allows branching based on specific criteria. Either enter or select values for Then and Else.
58.		**Notification Activity** - An activity that displays a notification window that contains an email template for the activity owner to complete, and then sends an email notification.
59.		**SOP Activity** - An activity that launches another standard operating procedure.
60.	Key Performance Indicator	The CCC shall allow definition of key performance indicators, trends, leading Indicators and visualize the indicators on a web based configurable dashboard infrastructure.
61.		The CCC shall allow configuration and monitoring of service levels for key performance indicators and triggering of actions towards the incident management system when those service levels are breached
62.		**Green** indicates that the status is acceptable, based on the parameters for that KPI, no action is required.
63.		**Yellow** indicates that caution or monitoring is required, action may be required.
64.		**Red** indicates that the status is critical and action is recommended.
65.	Reporting Requirements	Command & Control Centre should provide easy to use user interfaces for operators such as Click to Action, Charting, Hover and Pop Ups, KPIs, Event Filtering, Drill down capability, Event Capture and User Specific Setup
66.		The solution should generate Customized reports based on the area, camera or periodic or any other customer reports as per choice of the administrators

S.No	Functions	Minimum Specifications
67.		The CCC shall provide a repository of built-in relevant reports, including: i. Incident Reports-Detailed incident reports shall include an incident summary, all the tasks associated with the incident, relevant snapshots, and maps. ii. Periodic Reports iii. Maintenance Reports iv. Statistical Reports
68.		The CCC shall have a built-in reporting engine that will allow on demand or automatic report generation, configurable by the Administrator and with customization options
69.	Collaboration among Stakeholders	The CCC shall enable stakeholder collaboration where incidents/tasks triggered automatically or manually by control room operators are distributed to the correct owners in incident/task context, such collaboration to include: i. allowing departments to work autonomously ii. allowing logical locations or project groups to work autonomously iii. allowing inter-department collaboration
70.		Collaboration shall include content such as markups, comments, tasks, and forms.
71.	Asset Management	The system shall provide the capability to define, search, and locate assets of various types, including vehicles, buildings, and people.
72.		Asset management shall be fully integrated with the events correlation/ workflows / rules engine and shall allow defining various triggers based on specific assets, asset types, asset groups and assets attributes.
73.		i. The system shall enable assets to be displayed on maps with their corresponding GIS locations and unique icons. ii. The context menu associated with an asset's map icon shall allow direct dialing of a phone number, if available.
74.	Communication Requirements	The solution should adhere to the below mentioned communication requirements.
75.		The system shall allow email messages based on templates to be initiated by users in response to incidents or invoked by rules-based automatic actions.
76.		Provide the capability to invite using information provided during the location of those individuals or roles, invite them to collaborate and to share valuable information.

S.No	Functions	Minimum Specifications
77.		The System shall support on-demand or automatic outgoing call initiation. i. Calling capability shall be available via GIS map icons. ii. SIP protocol shall be supported.
78.		Provide a single web based dashboard to send notifications to target audiences using multiple communication methods including voice-based notification on PSTN/Cellular, SMS, Voice mail, E- mail and Social Media
79.		The solution should provide Dispatch Console integration with various communication channels. It should provide rich media support for incidents, giving dispatchers the power to consolidate information relating to an incident and instantly share that information among responder teams. It should assess the common operating picture, identify & dispatch mobile resources available near the incident location. Augment resources from multiple agencies for coordinated response.
80.	Authentication	Use authentication information to authenticate individuals and/or assign roles.
81.	Events and Directives control	Should provide the capability for the events that are produced from a sub- system and are forwarded to the Command & Control Centre. Events could be a single system occurrence or complex events that are correlated from multiple systems. Events could be ad hoc, real-time, or predicted and could range in severity from informational to critical. At the Control Centre, the event should be displayed on an operations dashboard and analyzed to determine a proper directive.
82.		Directives issued by the Command & Control Centre should depend on the severity of the monitored event. Directives will be designed and modified based on standard operating procedures, as well as state legislation. A directive could be issued automatically via rules, or it could be created by the operations team manually.
83.	Alert & Notification Requirements	The system should provide the software component for the message broadcast and notification solution that allows authorized personal and/or business processes to send messages to target audience (select-call or global or activation of pre-programmed list) using multiple communication methods including SMS, Voice (PSTN/Cellular), Email and Social Media.
84.	Security & Access Control	Provide Role based security model with Single-Sign-On to allow only authorized users to access and administer the alert and notification system.

S.No	Functions	Minimum Specifications
85.	Internet Security	Provide comprehensive protection of web content and applications on back-end application servers, by performing authentication, credential creation and authorization.
86.	Authorization	Comprehensive policy-based security administration to provide all users specific access based on user's responsibilities. Maintenance of authorization policy in a central repository for administration purposes.
87.	User group	Should provide support to enable assignment of permissions to groups, and administration of access control across multiple applications and resources. Secure, web-based administration tools to manage users, groups, permissions and policies remotely
88.	Flexible single sign-on (SSO)	SSO to Web-based applications that can span multiple sites or domains with a range of SSO options.
89.	Authentication	Support LDAP authentication mechanism
90.	Rule Engine &Optimization	Should have ability to respond to real-time data with intelligent &automated decisions
91.		Should provide an environment for designing, developing, and deploying business rule applications and event applications.
92.		The ability to deal with change in operational systems is directly related to the decisions that operators are able to make
93.		Should have at-least two complementary decision management strategies: business rules and event rules.
94.		Should provide an integrated development environment to develop the Object Model (OM) which defines the elements and relationships
95.	Mobile Module – 2 -way communication for Field personnel	i. Create an incident from the field ii. View incidents and relevant incident information including location and attachments iii. Exchange comments with the control room operators and other users iv. Support incident management at offline mode with ability to sync information when reconnect with network

5.1.1.2 Functional Requirement for Knowledge Management Solution

Common Knowledge Management solution for Chennai Safe City Initiative, to create knowledge repository.

5.1.1.2.1 Archival of Knowledge Content

- Allow creation of a central knowledge repository of documents that can be accessed by all officials based on their roles and privileges.
- Allow to add description with the uploading documents / knowledge content.
- Should have a well-defined workflow that allows processes for knowledge creation, approval and archival for re-use.
- Should allow multiple / bulk file upload
- Should have folder wise categorization
- Should allow to upload and archive documents of any format including tiff, jpeg, pdf, PDF/A, audio, video etc.
- Should allow categorization of Knowledge into different categories like personnel, financial, legal etc.
- Should allow multimedia content archiving / sharing.

5.1.1.2.2 *Knowledge Content Collaboration*

- Should allow only authorized employees to locate, update and share documents
- Should allow authorized users to post questions / answers.
- Should provide an online discussion forum to hold conversation on posted topics.
- Should allow documents to be stored and modified with proper versioning.
- Should support Individual/group/section/office specific centralized information repository to store knowledge content.
- Should allow collaborative working on the knowledge content.
- Should keep a track of different document versions modified by different users
- Should have an add-on feature of rating the content.
- Should have capability to attach citations and synopsis with the respective knowledge content.
- Should provide the capability to subscribe for the knowledge content, category, so that the users get notifications once any new document, content is getting uploaded for the respective category or knowledge source.
- Should allow users to share the documents on Social media platforms such as Facebook, Twitter etc.
- Should have online chat facilities, where users can initiate a discussion with concerned expert or group of users and can send messages, documents and interact on common platform.
- Discussion forum should have an administrator who can add, edit and delete discussions post.
- Should have functionality to define the To-Do list for the tasks to be done.

5.1.1.2.3 *Strong Searching Capabilities*

- Provides facility for index based content search
- Support content searching using content categories, sub categories, Title, author, File/Content types
- Should allow to search for contents based on Keywords, Tags, From/To Date etc.

- Supports automatic full text indexing for Text based search

5.1.1.2.4 *Notification & Messaging*

- Should allow users to mail knowledge content to users / departmental officials.
- Should have feature to send the notifications to a user about his/her content being approved / rejected.
- Should have an intelligent feature to either email knowledge content on a specific date and time.
- Should have a built in alert mechanism (Email and SMS) for subscribed documents.

5.1.1.2.5 *Architecture & Scalability*

- Should be built using Enterprise Content Management framework
- Should be COTS based solution and platform independent and support for all major operating systems such as Windows, Linux etc. on server side with or without virtualization.
- Multi-tier architecture having web-based solution and support for clustering
- Supports separate Document/Image server for better management of documents and store only metadata information in database.
- Proven Scalability for thousands of users
- Support for de-centralized/distributed architecture
- Store billions of documents in repository

5.1.1.2.6 *Viewing & Annotations*

- Support for viewing and annotating on image documents through inbuilt viewer through web and mobile devices
- Inbuilt viewer for viewing scanned documents and facilitates zoom- in/zoom-out, zoom percentage and other image operations like Invert, rotate etc.
- Support view of multipage document having capability to download and view document page by page
- Support view & annotation of PDF/A format documents using inbuilt viewer (open ISO standard for long term archival of documents)
- Provides facility of putting text and image annotations on scanned document.

5.1.1.2.7 *Reporting & Dashboards*

- Should have dashboard and reporting capability for viewing the reports such as knowledge content added by users, number of documents per category, content pending to be approved etc.

5.1.1.2.8 *Compliance with Open Standards*

- Should compliant to ODMA and WebDAV standards

- Supports interoperability through CMIS compliance
- Workflows of the proposed Knowledge Management System should compliant to open standards such as BPMN, BPEL, WFMC.
- Should compliant to records and metadata management standards such as DoD 5015.15, ISO 15489, Dublin Core

5.1.1.2.9 Document Management Security

Knowledge Management system should allow for multiple permission levels such as:

- At Folder level – All rights (system, group, and user) are assigned at folder level.
- At system level – Set global access rights at the overall system level.
- At the group level – The most efficient way to manage security rights is defining the access rights at group level wherein users who are part of the specific groups will be able to perform operations accordingly.
- At the user level – Set permissions for Individual users.

Apart from this, Knowledge Management System should also have various other key security features having support for:

- Defining multiple levels of access rights (Delete/ Edit/ View/ Print/ Copy or Download).
- Define system privileges like Create/Delete Users, Define indexes etc.
- Support for Digital certificate
- Facility to define password policy with extensive password validations like passwords must be of minimum 8 characters which shall be alphanumeric, locking of user-id after three un- successful attempts, password expiry, password history so that passwords are not same as previous passwords etc.
- Extensive Audit-trails at document, Folder and for highest levels for each action done by user with user name, date and time
- Encryption of documents and metadata

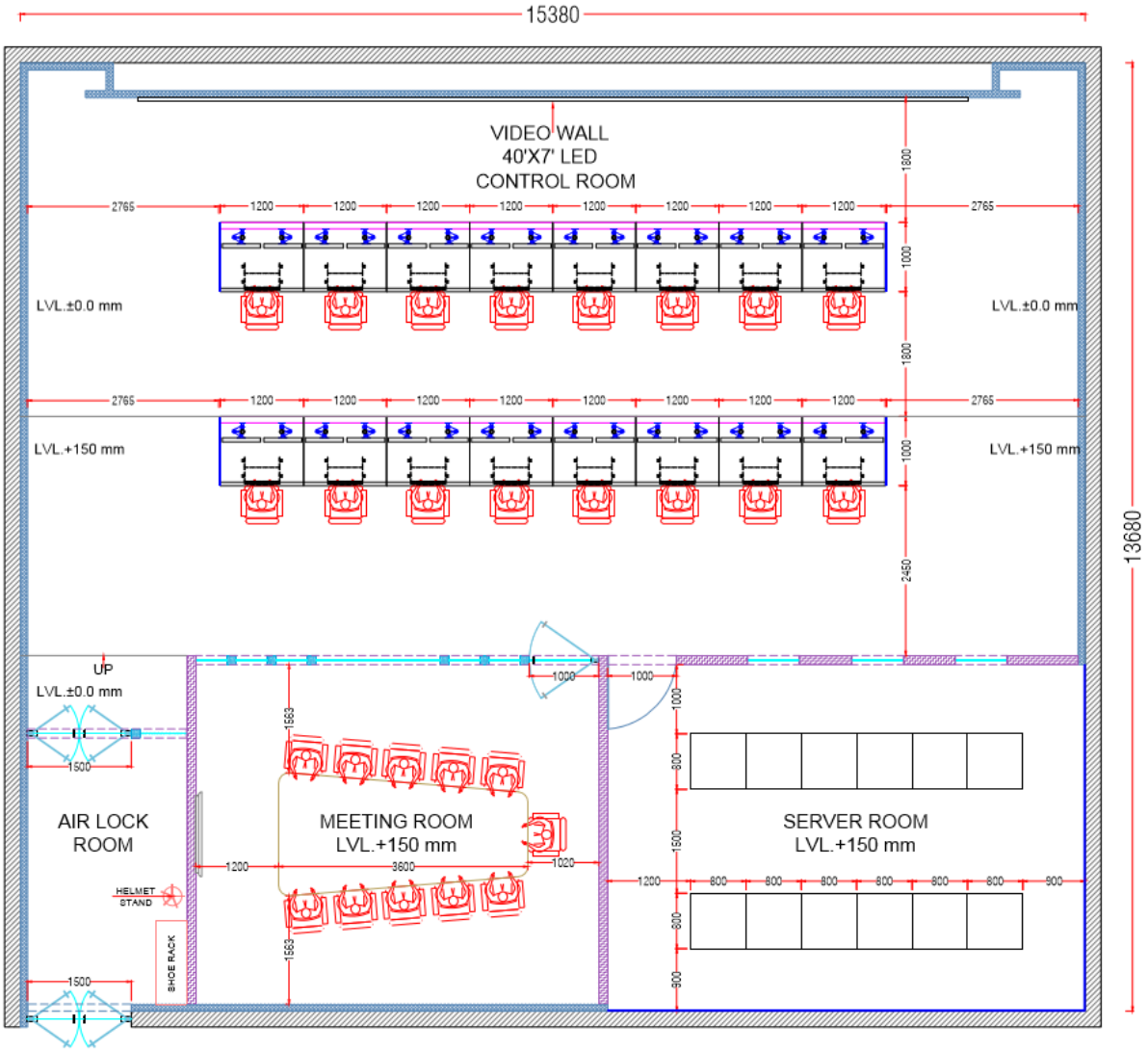
5.1.1.2.10 Application Integration Capability

- Support for web services, Java based API, and URL-based integration
- Integration based on standards such as XML
- Active Directory/LDAP integration

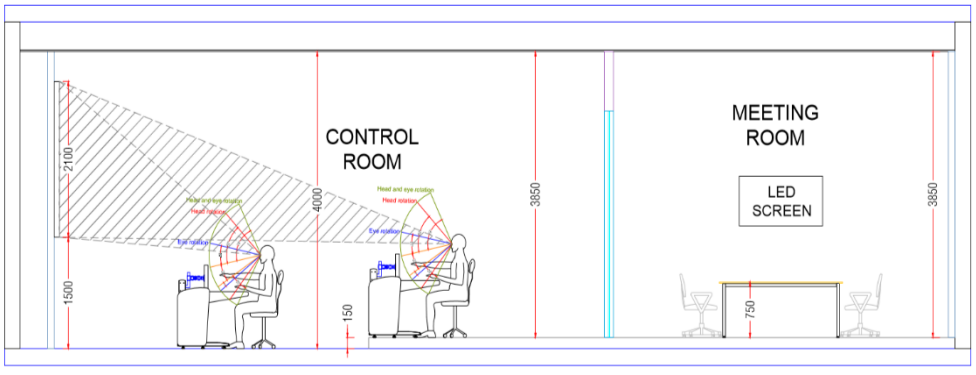
5.1.1.3 Functional Specifications of Non-IT components at CCC

Proposed specifications for various Non-IT components, required at Command & Control Centre and the Edge Level, are given in this section. It is essential that Fire Proof material be used as far as possible and Certification from Fire Department be taken for Command & Control Centre before Go Live.

Indicative CCC Layout



LEGEND	
SYMBOL	NAME
	BRICK WALL
	METAL PANELING
	METAL PARTITION
	GLASS PARTITION
	PAINT
	METAL RAFTER



NOTE: UNLESS OTHERWISE MENTIONED ALL DIMENSIONS ARE IN MILIMETERS

5.1.1.3.1 *Civil and Architectural work*

A. Command and Control Centre Building

- CCC Building- 2264 Sq. Ft., however bidders are strongly advised to do site visit to understand the requirements and design the usage for built up areas as required
- SI shall be responsible for making the facility fit for the intended purpose. The work shall be done in accordance to the drawings approved by the statutory authorities
- Scope includes Site Planning, Demolition of existing structures, developing required specifications, preparing Good for Construction (GFC), coordinated drawings and construct the CCC in accordance with the same.
- The scope shall also include preparation of as-built drawings before handing over the work to the Client, maintaining the Quality assurance & Quality control (QA&QC) including control, corrective actions, reporting and arranging for regular inspections by all concerned
- The Scope of Work includes but is not limited to the following in relation to the design, construction, of the CCC
    - Prepare Design Basis Report based on the design intent and submit for approval
    - Carry out Structural Design based on approved Civil Structural Design Criteria
    - Submit Structural stability certificate for all structures and components from government authority at his own cost
    - Proof checking by accredited agencies at bidders cost before submitting for the approval of the Client
    - Soil Testing, Site Topographic Survey and Geotechnical Investigations as deemed necessary must be performed by the SI.
    - Site Clearing, Site Grading, and Excavation
    - Piling, foundation & substructure works
    - Implement Anti termite treatment / Water proofing / Insulation works
    - Superstructure RCC works
    - Masonry
    - Plastering/Painting/Façade/External Finishes
    - Structural Steel work
    - Ancillary PCC / RCC works including equipment foundations / pedestals, etc.

B. False Ceiling (at Command & Control Centre)

- **Safety** - Ceiling system shall be seismic zone 3 or better tested and certified from government approved test laboratory on the name of Control Room Solution Provider.
- **Environmental Concern** - RoHS (Restriction of Hazardous Substances) certified (from UL/Intertek) ceiling to ensure restriction of hazardous substance.
- **Fire Safety** - The on-perforated ceiling tiles shall be Class A fire rated as per ASTM E-84 (from UL/Intertek)to ensure that the material does not provoke fire and does not generate smoke."

- **Quick & Easy Maintenance** - UL 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.
- **Acoustics** - The tiles are designed to provide acoustics and ensure that no echo is generated in the control room. Ceiling has acoustical properties as the perforated tiles have 0.3 NRC according to IS:8225-1987, ISO: 354-1985 and ASTM 423-90.

C. Furniture and Fixture

- **Maintainability Feature -** UL Certified design feature of High-density Poly Urethane Foam moulded on industrial grade aluminium core to form 50mm deep tapered edge to be installed on worktop. The Edge shall be mechanically replaceable within 30 minutes in case of damage or wear without opening or removing the worktop. Valid UL audit Certificate to be enclosed with the bid.
- **Quality & Durability -** The proposed console must be UL Listed product. Valid certificate to be enclosed with the bid. The Control Room Turnkey Solution Provider should have Trade Mark registration certificate issued by the Government of India for the console offered in the Tender. This is to ensure that the offered product is an engineered solution.
- **Environmental Concern -** Also, the Control Room Turnkey Solution Provider must be FSC Certified Company. Valid certificate to be enclosed with the bid.
- **Operator's Health -** The entire console must be Greenguard gold certified from last 1 year. Valid certificate to be enclosed with the bid.
- **Up gradation -** For quick & easy installation , maintenance and retrofitting it is recommended to define the Monitor Arm Assembly as mentioned below:-
    - UL certified design feature of Monitor Arm Assembly shall have auto-lock, push & add/remove die-cast aluminium extendible arms of 150mm each with tool less addition/deletion feature to cater future requirements. Tool less addition / deletion in less than a minute. UL certificate to be enclosed along with the bid.
- **Quick & Easy Maintenance -** UL 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."

D. Partitions (wherever required as per approved drawing)

- **Safety -** ""Wall panelling system shall be seismic zone 3 or better tested and certified from government approved test laboratory on the name of Control Room Turnkey Solution Provider.
- **Acoustic -** Minimum 15% of the tiles shall have at least 10,000 micro-perforations per square meter to achieve NRC of 0.6 Sound Absorption Coefficient by diffuse field

method; IS: 8225-1987 “Measurement of Sound Absorption Coefficient in Reverberation Room” (Equivalent to ISO: 354-1985 and ASTM 423-90).

- **Environmental Concern -** RoHS (Restriction of Hazardous Substances) certified (from UL/Intertek) wall paneling to ensure restriction of hazardous substance.
- **Fire Safety -** ASTM E84 certificate (From UL / intertek) for control room wall tiles to be submitted to ensure that the material does not provoke fire and does not generate smoke.""
- **Easy replacement -** UL Certified Design feature of Modular wall Paneling tile having secure locking arrangement for equidistant mounting. Locking arrangement to 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 UL audit Certificate to be submitted along with the technical bid
- **Load bearing capacity-** UL Certified Design feature of Load bearing capacity of Paneling:- Paneling structure shall have load carrying capacity of 300 Kg to hold any display unit on clamp having minimum length of 750mm. Valid UL audit Certificate to be submitted along with the technical bid."
- Fire Rated Wire Glass minimum 6 mm thick for all glazing in the partition wall complete. (External windows not included in this).
- All doors should be minimum 1200 mm (4 ft.) wide.

E. Flooring

- False flooring systems shall be provided with calcium silicate floor tiles with acoustic laminate finish on the top. Calcium silicate floors are resistant to fire and acoustic laminate offers wide range of colours and has acoustic property to add ergonomic value to ambience of the control room.
- Top finish material shall be bio-degradable, acoustical in nature and must not emit any harmful VOCs, should be durable in nature and resistant to scratches.
- Top finish of acoustic Laminate shall reduce impact sound by 14dB (ISO 717-2)). It shall be twinlayer linoleum built up from 2 mm acoustic laminate.

F. Painting

- Fire retardant paint of pre-approved make and shade to give an even shade over a primer coat as per manufacturers’ recommendations after applying painting putty to level and plumb and finishing with 2 coats of fire retardant paint. Base coating shall be as per manufacturer’s recommendation for coverage of paint.
- For all vertical Plain surface.
- For fire-line gyp-board ceiling.
- POP punning over cement plaster in perfect line and level with thickness of 10 – 12 mm including making good chases, grooves, edge banding, scaffolding pockets etc.
- Fire retardant coating on all vertical surfaces, furniture etc. as per manufacturer’s specification.

5.1.1.3.2 *PVC Conduit*

- The conduits for all systems shall be high impact rigid PVC heavy-duty type and shall comply with I.E.E regulations for standardized conduit 1.6 mm thick as per IS 9537/1983.
- All sections of conduit and relevant boxes shall be properly cleaned and glued using appropriate epoxy resin glue and the proper connecting pieces, like conduit fittings such as Mild Steel and should be so installed that they can remain accessible for existing cable or the installing of the additional cables.
- No conduit less than 20mm external diameter shall be used. Conduit runs shall be so arranged that the cables connected to separate main circuits shall be enclosed in separate conduits, and that all lead and return wire of each circuit shall be run to the same circuit.
- All conduits shall be smooth in bore, true in size and all ends where conduits are cut shall be carefully made true and all sharp edges trimmed. All joints between lengths of conduit or between conduit and fittings boxes shall be pushed firmly together and glued properly.
- Cables shall not be drawn into conduits until the conduit system is erected, firmly fixed and cleaned out. Not more than two right angle bends or the equivalent shall be permitted between draw or junction boxes. Bending radius shall comply with I.E.E regulations for PVC pipes.
- Conduit concealed in the ceiling slab shall run parallel to walls and beams and conduit concealed in the walls shall run vertical or horizontal.
- The chase in the wall required in the recessed conduit system shall be neatly made and shall be of angle dimensions to permit the conduit to be fixed in the manner desired. Conduit in chase shall be held by steel hooks of approved design of 60cm centre the chases shall be filled up neatly after erection of conduit and brought to the original finish of the wall with cement concrete mixture 1:3:6 using 6mm thick stone aggregate and course sand.

5.1.1.3.3 *Wiring*

- PVC insulated copper conductor cable shall be used for sub circuit runs from the distribution boards to the points and shall be pulled into conduits. They shall be stranded copper conductors with thermoplastic insulation of 650 / 1100 volts grade. Color code for wiring shall be followed.
- Looping system of wring shall be used, wires shall not be jointed. No reduction of strands permitted at terminations.
- Wherever wiring is run through trunking or raceways, the wires emerging from individual distributions shall be bunched together with cable straps at required regular intervals. Identification ferrules indicating the circuit and D.B. number shall be used for sub main, sub circuit wiring the ferrules shall be provided at both end of each sub main and sub-circuit.
- Where, single phase circuits are supplied from a three phase and a neutral distribution board, no conduit shall contain wiring fed from more than one phase in any one room in

the premises, where all or part of the electrical load consists of lights, fans and/or other single phase current consuming devices, all shall be connected to the same phase of the supply.

- Circuits fed from distinct sources of supply or from different distribution boards or M.C.B.s shall not be bunched in one conduit. In large areas and other situations where the load is divided between two or three phases, no two single-phase switches connected to difference phase shall be mounted within two meters of each other.
- All splicing shall be done by means of terminal blocks or connectors and no twisting connection between conductors shall be allowed.
- Metal clad sockets shall be of die cast non-corroding zinc alloy and deeply recessed contact tubes. Visible scraping type earth terminal shall be provided. Socket shall have push on protective cap.
- All power sockets shall be piano type with associated switches of same capacity. Switch and socket shall be enclosed in a M.S sheet enclosure with the operating knob projecting. Entire assembly shall be suitable for wall mounting with Bakelite insulators connected on the live wire and neutrals of each circuit. It shall also be continuous everywhere having no fuse or switch installed in the line excepting at the main panels and boards. Each power plug shall be connected to each separate and individual circuit unless specified otherwise. The power wiring shall be kept separate and distinct from lighting and fan wiring. Switch and socket for light and power shall be separate units and not combined one.
- Balancing of circuits in three phases installed shall be arranged before installation is taken up. Unless otherwise specified not more than ten light points shall be grouped on one circuit and the load per circuit shall not exceed 1000 watts.

5.1.1.3.4 *Earthing*

- All electrical components are to be earthed by connecting two earth tapes from the frame of the component ring and will be connected via several earth electrodes. The cable arm will be earthed through the cable glands. Earthing shall be in conformity with provision of rules 32, 61, 62, 67 & 68 of Indian Electricity rules 1956 and as per IS-3043. The entire applicable IT infrastructure in the Control Rooms shall be earthed.
- 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. State shall provide the necessary space required to prepare the earthing pits.
- All metallic objects on the premises that are likely to be energized by electric currents should be effectively grounded.
- The connection to the earth or the electrode system should have sufficient low resistance in the range of 0 to 25 ohm to ensure prompt operation of respective protective devices in event of a ground fault, to provide the required safety from an electric shock to personnel & protect the equipment from voltage gradients which are likely to damage the equipment.

- Recommended levels for equipment grounding conductors should have very low impedance level less than 0.25 ohm.
- The Earth resistance shall be automatically measured on an online basis at a pre-configured interval and corrective action should be initiated based on the observation. The automatic Earthing measurements should be available on the UPS panel itself in the UPS room.
- There should be enough space between data and power cabling and there should not be any cross wiring of the two, in order to avoid any interference, or corruption of data.
- The earth connections shall be properly made .A small copper loop to bridge the top cover of the transformer and the tank shall be provided to avoid earth fault current passing through fastened bolts, when there is a lighting surge, high voltage surge or failure of bushings.
- A complete copper mesh earthing grid needs to be installed for the server farm area, every rack need to be connected to this earthing grid. A separate earthing pit need to be in place for this copper mesh.
- Provide separate Earthing pits for Servers, UPS & Generators as per the standards.

5.1.1.3.5 *Cable Work*

- Cable ducts should be of such dimension that the cables laid in it do not touch one another. If found necessary, the cable shall be fixed with clamps on the walls of the duct. Cables shall be laid on the walls/on the trays as required using suitable clamping/ fixing arrangement as required. Cables shall be neatly arranged on the trays in such manner that a crisscrossing is avoided and final take off to switch gear is easily facilitated.
- All cables will be identified close to their termination point by cable number as per circuit schedule. Cable numbers will be punched on 2mm thick standard strips and securely fastened to the cables. In case of control cables all covers shall be identified by their wire numbers by means of PVC ferrules. For trip circuit identification additional red ferrules are to be used only in the switch gear / control panels, cables shall be supported so as to prevent appreciable sagging. In general distance between supports shall not be greater than 600mm for horizontal run and 750mm for vertical run.
- Each section of the rising mains shall be provided with suitable wall straps so that the same can be mounted on the wall.
- Whenever the rising mains pass through the floor they shall be provided with a built-in fire proof barrier so that this barrier restricts the spread of fire through the rising mains from one section to the other adjacent section.
- Neoprene rubber gaskets shall be provided between the covers and channel to satisfy the operating conditions imposed by temperature weathering, durability etc.
- Necessary earthing arrangement shall be made alongside the rising mains enclosure by means of a GI strip of adequate size bolted to each section and shall be earthed at both ends. The rising mains enclosure shall be bolted type.
- The space between data and power cabling should be as per standards and there should not be any criss-cross wiring of the two, in order to avoid any interference, or corruption of data.

5.1.1.3.6 *Water Leak Detection*

The water leak detector shall be installed to detect any seepage of water into the critical area and alert the Security Control Room for such leakage. It shall consist of water leak detection cable and an alarm module. The cable shall be installed in the ceiling & floor areas around the periphery.

- Water Leak Detection system should be for the Server and Network room Areas to detect and monitor water flooding below the floor of the DC.
- Water Leak Detection System should be wire based solution with alarm; the wire needs to be laid in DC surrounding the AC units, which is the probable source of water leakage.

Supply Voltage:	230Vac @ 50Hz
Supply current	50mA max.
Output	12A @ 250Vac
Response time	<1 sec. after exposure
Electrical	Terminals for 0.5-2.5² cable
Ambient:	
Temperature	*-10 to 50°C*
RH	*0-80% non-condensing*
Material	PVC Twisted pair with stainless 316 elements
Dimension	3.5mm dia. Maximum cable run 200m (Including detection cable)

5.1.1.3.7 *Gas Based Fire Suppression System*

The Clean Agent Fire Suppression system cylinder, CCOE, Nagpur approved seamless cylinders, discharge hose, fire detectors and panels and all other accessories required to provide a complete operational system meeting applicable requirements of NFPA 2001 Clean Agent Fire Extinguishing Systems, NFPA 70 National Electric Code, NFPA 72 National Fire Alarm Code or ISO standards must be considered to ensure proper performance as a system with UL/FM approvals and installed in compliance with all applicable requirements of the local codes and standards.

- The Clean Agent system considered for Total flooding application shall be in compliance with the provisions of Kyoto Protocol.
- Care should be taken that none of the Greenhouse Gases identified in the Kyoto Protocol is used for fire suppression application.
- The minimum criterion for the selection of the Clean Agent will be on the following parameters
    - Zero Ozone Depleting Potential.
    - Global Warming Potential not exceeding one.
    - Atmospheric Lifetime not exceeding one week.

- The clean agent fire suppression system with FK-5-1-12 and Inert Gas based systems are accepted as a replacement of HCFC and HFC as per Kyoto Protocol.
- The Clean Agent considered for the suppression system must be suitable for manable occupied areas with NOAEL Level (No observable adverse effect level) of 10% as compared to the design concentration to ensure high safety margin for the human who might be present in the hazard area.
- The minimum design standards shall be as per NFPA 2001, 2004 edition or latest revisions.
- Care shall be given to ensure proper early warning detection system with minimum sensitivity of 0.03% per foot obscuration as per NFPA 318 & NFPA 72 to ensure that one gets a very early warning to investigate the incipient fire much before the other detectors activate the fire suppression system automatically.
- All system components furnished and installed shall be warranted against defects in design, materials and workmanship for the full warranty period which is standard with the manufacturer, but in no case less than five (5) years from the date of system acceptance
- Additionally, Portable Extinguishers (CO_2 or Halon based Extinguishers are not acceptable) shall be placed at strategic stations throughout the Data Centre. **OR** Fire suppression system shall deploy FM-200 (ETG-5) or NOVEC-1230 based gas suppression systems with cross-zoned detector systems for all locations. These detectors should be arranged in a manner that they activate the suppression system zone wise to cater to only the affected area.
- Illuminated Signs indicating the location of the extinguisher shall be placed high enough to be seen over tall cabinets & racks across the room. Linear heat detection cable should be placed along all wire pathways in the ceiling. This should not directly trigger the suppression system—rather; it should prompt the control system to sound an alarm
- The OEM (/ Bidder) shall give a Certificate stating that their FM-200 system is approved by UL / FM / VdS / LPC/CNPP for use with Seamless Steel Cylinders (Component as well as System Approval).
- The OEM (/ Bidder) shall also provide a Letter that the OEM has FM-200 Flow Calculation software suitable for Seamless Steel cylinder bided for as per the Bill of materials and that such Software shall be type approved by FM / UL / VdS / LPC.
- The Storage Container offered shall be of Seamless type, meant for exclusive use in FM-200 systems, with VdS/FM/UL/LPC/CNPP component approval. Welded cylinders are not permitted.
- The Seamless storage cylinder shall be approved by Chief Controller of Explosives, Nagpur and shall have NOC from CCoE, Nagpur for import of the same. Documentary evidence to be provided for earlier imports done by the bidder.
- The FM-200 valve should be Differential Pressure Design and shall not require an Explosive / Detonation type Consumable Device to operate it.
- The FM-200 Valve operating actuators shall be of Electric (Solenoid) type, and it should be capable of resetting manually. The Valve should be capable of being functionally

tested for periodic servicing requirements and without any need to replace consumable parts.

- The individual FM-200 Bank shall also be fitted with a manual mechanism operating facility that should provide actuation in case of electric failure.
- The system flow calculation is to be carried out on certified software, suitable for the Seamless Steel Cylinder being offered for this project. Such system flow calculations shall be also approved by VdS / LPC/ UL / FM.
- The system shall utilize 25 Bar / High pressure (362 psi) technology that allows for a higher capacity to overcome frictional losses and allow for higher distances of the agent flow; and also allow for better agent penetration in enclosed electronic equipment such as Server Racks/ Electrical Panels etc.
- The designer shall consider and address possible Fire hazards within the protected volume at the design stage. The delivery of the FM-200 system shall provide for the highest degree of protection and minimum extinguishing time. The design shall be strictly as per NFPA standard NFPA 2001.
- The suppression system shall provide for high-speed release of FM-200 based on the concept of total Flooding protection for enclosed areas. A Uniform extinguishing concentration shall be 7% (v/v) of FM-200 for 21 degree Celsius or higher as recommended by the manufacturer.
- The system discharge time shall be 10 seconds or less, in accordance with NFPA standard 2001.
- Sub floor and the ceiling void to be included in the protected volume.
- The FM-200 systems to be supplied by the bidder must satisfy all requirements of MTC having jurisdiction over the location of the protected area and must be in accordance with the OEM's product design criteria.
- The detection and control system that shall be used to trigger the FM-200 suppression shall employ cross zoning of photoelectric and ionization smoke detectors. A single detector in one zone activated, shall cause in alarm signal to be generated. Another detector in the second zone activated, shall generate a pre-discharge signal and start the pre-discharge condition.
- The discharge nozzles shall be located in the protected volume in compliance to the limitation with regard to the spacing, floor and ceiling covering etc. The nozzle locations shall be such that the uniform design concentration will be established in all parts of the protected volumes. The final number of the discharge nozzles shall be according to the OEM's certified software, which shall also be approved by third party inspection and certified such as UL / FM / VdS / LPC.
- The Cylinder shall be equipped with differential pressure valves and no replacement parts shall be necessary to recharge the FM-200 containers.
- FM-200 shall be discharged through the operation of an Electric (solenoid) operated device or pneumatically operated device, which releases the agent through a differential pressure valve.
- The bidder shall provide all documentation such as Cylinder Manufacturing Certificates. Test and Inspection Certificates and Fill Density Certificates.

- The FM-200 discharge shall be activated by an output directly from the `FM-200' Gas Release control panel, which will activate the solenoid valve. FM-200 agent is stored in the container as a liquid. To aid release and more effective distribution, the container shall be super pressurized to 600 psi (g) at 21°C with dry Nitrogen.
- The releasing device shall be easily removable from the cylinder without emptying the cylinder. While removing from cylinder, the releasing device shall be capable of being operated, with no replacement of parts required after this operation.
- Upon discharge of the system, no parts shall require replacement other than gasket, lubricants, and the FM-200 agent. Systems requiring replacement of disks, squibs, or any other parts that add to the recharge cost will not be acceptable.
- The manual release device fitted on the FM-200 Cylinder(s) shall be of a manual lever type and a faceplate with clear instruction of how to mechanically activate the system. In all cases, FM-200 cylinders shall be fitted with a manual mechanical operating facility that requires two-action actuation to prevent accidental actuation.
- FM-200 storage cylinder valve shall be provided with a safety rupture disc. An increase in internal pressure due to high temperature shall rupture the safety disc and allow the content to vent before the rupture pressure of the container is reached. The # contents shall not be vented through the discharge piping and nozzles.
- FM-200 containers shall be equipped with a pressure gauge to display internal pressure.
- Brass Discharge nozzles shall be used to disperse the `FM-200'. The nozzles shall be brass with female threads and available in sizes as advised by the OEM system manufacturer. Each size shall come in two styles: 180° and 360° dispersion patterns.
- All the Major components of the FM-200 system such as the Cylinder, Valves and releasing devices, nozzles and all accessories shall be supplied by one single manufacturer under the same brand name.
- Manual Gas Discharge stations and Manual Abort Stations, in conformance to the requirements put forth in NFPA 2001 shall be provided.

Release of FM-200 agent shall be accomplished by an electrical output from the FM- 200 Gas Release Panel to the solenoid valve and shall be in accordance with the requirements set forth in the current edition of the National Fire Protection Association Standard 2001.

5.1.1.3.8 *Fire Alarm System*

Fire can have disastrous consequences and affect operations of a Control Room. The early detection of fire for effective functioning of the Control Room.

A. System Description

- The Fire alarm system shall be a single loop addressable fire detection and alarm system. It must be installed as per NFPA 72 guidelines.
- Detection shall be by means of automatic heat and smoke detectors (multi sensor) located throughout the Control Room (ceiling, false floor and other appropriate areas where fire can take place) with break glass units on escape routes and exits.

B. Control and indicating component

- The control panel shall be a microprocessor based single loop addressable unit, designed and manufactured to the requirements of UL/EN54 Part 2 for the control and indicating component and UL/EN54 Part 4 for the internal power supply.
- All controls of the system shall be via the control panel only.
- The system status shall be made available via panel mounted LEDs and a backlit 8 line x 40-character alphanumeric liquid crystal display.
- All system controls and programming will be accessed via an alphanumeric keypad. The control panel will incorporate form fill menu driven fields for data entry and retrieval.
- The system will include a detection verification feature. The user shall have the option to action a time response to a fire condition. This time shall be programmable up to 10 minutes to allow for investigation of the fire condition before activating alarm outputs. The operation of a manual call point shall override any verify Control Centre.

C. Manual Controls

- Start sounders
- Silence sounders
- Reset system
- Cancel fault buzzer
- Display test
- Delay sounder operation
- Verify fire condition
- Disable loop

D. Smoke detectors

Smoke detectors shall be of the optical or ionization type. Devices shall be compatible with the CIE conforming to the requirements of UL/EN54 Part 7. The detectors shall have twin LEDs to indicate the device has operated and shall fit a common addressable base.

E. Heat detectors

- Heat detectors shall be of the fixed temperature (58° C) or rate of temperature rise type with a fixed temperature operating point.
- Devices shall be compatible with the CIE conforming to the requirements of UL/ EN54 Part 5 the detectors shall have a single LED to indicate the device has operated and shall fit a common addressable base.
- All bases shall be compatible with the type of detector heads fitted and the control system component used. Each base shall comprise all necessary electronics including a short circuit isolator.
- The device shall be automatically addressed by the CIE on power up of the loop without the need of the insertion of a pre-programmed EPROM or setting of DIL switches.
- Detector bases shall fit onto an industry standard conduit box.

- Addressable Manual Call points must also be provided
- Control & Monitor module must be provided for integration with 3rd party systems.

F. Audible Alarms –

Electronic sounders shall be colored red with adjustable sound outputs and at least 3 sound signals. The sounders should be suitable for operation with a 24V DC supply providing a sound output of at least 100dBA at 1 meter and 75 dBA min, for a bed head or sounder base type device. The sounder frequency shall be in the range of 500Hz to 1000Hz.

G. Commissioning

The fire detection and alarm system will be programmable and configurable via an alpha numeric keypad on the control panel.

5.1.1.3.9 Aspirating Smoke Detection System

This specification covers the requirements of design, supply of materials, installation, testing and commissioning of Aspirating Smoke Detection System. The system shall include all equipment's, appliances and labor necessary to install the system, complete with high sensitive LASER-based Smoke Detectors with aspirators connected to network of sampling pipes.

A. Codes and standards

- The entire installation shall be installed to comply one or more of the following codes and standards
  - NFPA Standards, US
  - British Standards, BS 5839 part :1

B. Approvals

- All the equipment's shall be tested, approved by any one or more:
- LPCB (Loss Prevention Certification Board), UK
- FM Approved for hazardous locations Class 1,Div 2
- UL (Underwriters Laboratories Inc.), U
- ULC (Underwriters Laboratories Canada), Canada
- Vds (Verband der Sachversicherer e.V), Germany

C. Design Requirements

- The System shall consist of a high sensitive LASER-based smoke detector, aspirator, and filter.
- It shall have a display featuring LEDs and Reset/Isolate button. The system shall be configured by a programmer that is either integral to the system, portable or PC based.
- The system shall allow programming of:

- Multiple Smoke Threshold Alarm Levels.
- Time Delays.
- Faults including airflow, detector, power, filter block and network as well as an indication of the urgency of the fault.
- Configurable relay outputs for remote indication of alarm and fault Conditions.

- It shall consist of an air sampling pipe network to transport air to the detection system, supported by calculations from a computer-based design modeling tool.
- Optional equipment may include intelligent remote displays and/or a high-level interface with the building fire alarm system, or a dedicated System Management graphics package.
- Shall provide very early smoke detection and provide multiple output levels corresponding to Alert, Action, and Fire 1 & 2. These levels shall be programmable and shall be able to set sensitivities ranging from 0.025 – 20% obscuration / meter.

D. Displays on the Detector Assembly

- The detector will be provided with LED indicators.
- Each Detector shall provide the following features: Alert, Alarm, Fire 1 and Fire 2 corresponding to the alarm thresholds of the detector/Smoke Dial display represents the level of smoke present, Fault Indicator, Disabled indicator

E. Sampling Pipe

The pipe shall be identified as Aspirating Smoke Detector Pipe along its entire length at regular intervals not exceeding the manufacturer's recommendation or that of local codes and standards.

F. Installation

- The Contractor shall install the system in accordance with the manufacturer's recommendation.
- Where false ceilings are available, the sampling pipe shall be installed above the ceiling, and Capillary Sampling Points shall be installed on the ceiling and connected by means of a capillary tube.
- Air Sampling Piping network shall be laid as per the approved pipe layout. Pipe work calculations shall be submitted with the proposed pipe layout design for approval.
- The bidder shall submit computer generated software calculations for design of aspirating pipe network, on award of the contract.

5.1.1.3.10 *Access Control System*

The Access Control System shall be deployed with the objective of allowing entry and exit to and from the premises to authorized personnel only. The system deployed shall be based on Biometric Technology. An access control system consisting of a central PC, intelligent controllers, power supplies and all associated accessories is required to make a fully

operational on-line access control system. Access control shall be provided for entry / exit doors. These doors shall be provided with electric locks and shall operate on fail-safe principle. The lock shall remain unlocked in the event of a fire alarm or in the event of a power failure. The fire alarm supplier shall make potential free contacts available for releasing the locks in a fire condition especially for staircase and main doors. Entry to the restricted area shall be by showing a proximity card / facial recognition near the reader and exit shall be using a push button installed in the secure area. The system shall monitor the status of the doors through magnetic reed contacts. The system should be designed and implemented to provide following functionality:

- Controlled Entries to defined access points
- Controlled exits from defined access points
- Controlled entries and exits for visitors
- Configurable system for user defined access policy for each access point
- Record, report and archive each and every activity (permission granted and / or rejected) for each access point.
- User defined reporting and log formats
- Fail safe operation in case of no-power condition and abnormal condition such as fire, theft, intrusion, loss of access control, etc.
- Day, Date, Time and duration-based access rights should be user configurable for each access point and for each user.
- One user can have different policy / access rights for different access points.

5.1.1.3.11 *Rodent Repellent*

The entry of Rodents and other unwanted pests shall be controlled using non-chemical, non-toxic devices. Ultrasonic pest repellents shall be provided in the false flooring and ceiling to repel the pests without killing them. However periodic pest control using Chemical spray can be done once in 3 months as a contingency measure to effectively fight the pest menace.

- Configuration : Master console with necessary transducer
- Operating Frequency : Above 20 KHz (Variable)
- Sound Output : 80 dB to 110 dB (at 1 meter)
- Power output : 800 mW per transducer
- Power consumption : 15 W approximately
- Power Supply : 230 V AC 50 Hz
- Mounting : Wall / Table Mounting

5.1.1.3.12 *Structured Cabling Components*

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

S.No	Parameter	Minimum Specifications
3	Certification	UL Listed and Verified

5.1.1.3.13 *Precision Air Conditioning*

The Data Centre Area shall be provided with fully redundant, microprocessor-based, gas-based, Precision Air-Conditioning system. Cool air feed to the Data Centres shall be bottom-charged or downward flow type using the raised floor as supply plenum through perforated aluminium tiles for airflow distribution. The return airflow shall be through the false ceiling to cater to the natural upwardly movement of hot air. Cooling shall be done by the Precision Air-Conditioning system only. Forced cooling using fans on the false floor is not acceptable. Air conditioning shall be capable of providing sensible cooling capacities at the design ambient temperature and humidity with adequate airflow. The Precision Air-Conditioning system shall capable to be integrated with the BMS for effective monitoring.

The SI shall assess, design, supply, transport, store, unpack, erect, and test the successful commissioning and satisfactory completion of trial operations of the Precision Air-Conditioning system for the Data Centres. The SI shall follow ASHRAE Standard for the HVAC and Ducting.

The SI shall be responsible for:

- Connecting the indoor unit with the mains electrical point
- Connecting indoor and outdoor units mechanically (with 18-gauge-hard copper piping).
- Connecting indoor and outdoor unit electrically
- Nitrogen pressure testing, triple vacuum, and final gas charging
- Connecting the humidifier feed line with the point provided
- Connecting the drain line with the point provided
- Commissioning and handing over the unit to the customer
- Operation and routine maintenance training for up to two persons nominated by the CLIENT while commissioning the units at site

Temperature Requirements

The environment inside the Primary and Secondary Data Centres shall be continuously maintained at 23 ± 1o degrees Celsius. The temperature and humidity shall be controlled at desired levels. The necessary alarms for variation in temperatures shall be monitored on a 24/7 basis and logged for providing reports.

Indicating Lamps

1. Indicating lamps assembly shall be screw type with built in resistor having non-fading color lens. LED type lamps are required.
   Wiring for Remote ON, OFF, TRIP indicating lamps is required.
   - ON indicating lamp: Red
   - OFF indicating lamp: Green

- TRIP indicating lamp: Amber
- PHASE indicating lamp: Red, Yellow, Blue
- TRIP circuit healthy lamp: Milky

Relative Humidity (RH) requirements

Ambient RH levels shall be maintained at 50% ± 5 non-condensing. Humidity sensors shall be deployed. The necessary alarms for variation in RH shall be monitored on a 24/7 basis and logged for providing reports.

Temperature and Relative Humidity Recorders

Temperature and relative humidity recorders shall be deployed for recording events of multiple locations within the Primary and Secondary Data Centres. Records of events for the past 7 days shall be recorded and presentable whenever required. Sensors shall be located at various locations within the Primary and Secondary Data Centres to record temperature and humidity automatically.

Air Quality Levels

The Primary and Secondary Data Centres shall be kept at highest level of cleanliness to eliminate the impact of air quality on the hardware and other critical devices. The Primary and Secondary Data Centres shall be deployed with efficient air filters to eliminate and arrest the possibility of airborne particulate matter which may cause air-flow clogging, gumming up of components, causing short-circuits, or blocking the function of moving parts.

Additional Points

1. The precision air conditioners shall be capable of maintaining a temperature range of 23 degrees Celsius with a maximum of ±1 degree variation and relative humidity of 50% with a maximum variation of ±5%.
2. The precision air conditioners shall have two (2) independent refrigeration circuits, each comprised of one scroll compressor, refrigeration circuit and condenser, and dual blowers for flexibility of operations and better redundancy.
3. The unit casing shall be in double-skin construction for longer life of the unit and low noise level.
4. For close control of the Data Centres temperature and relative humidity (RH) environment conditions, the controller shall have proportional integration and differential (PID).
5. The precision unit shall be air-cooled, refrigerant-based system to avoid chilled water in critical space.
6. The internal rack layout design shall follow the cold aisle and hot aisle concept as recommended by ASHRAE.
7. The refrigerant used shall be environmentally friendly HFC, R-407-C or equivalent in view of the long-term usage of the Data Centres equipment as well as the availability of spares and refrigerant.

8. The system shall include fully deployed Dynamic Smart Cooling with auto sequencing and auto power management features.
9. Thermal and computational fluid dynamics(CFD) analysis diagrams shall be provided
10. The fan section shall be designed for an external static pressure of 25 Pa. The fans shall be located downstream of the evaporator coil and be of the electronically commuted, backward, curved, centrifugal type, double-width, double-inlet, and statically and dynamically balanced. Each fan shall be direct-driven by a high efficiency direct current (DC) motor.
11. The evaporator coil shall be A-shape coil for down flow, incorporating draw-through air design for uniform air distribution. The coil shall be constructed of rifled bore copper tubes and louvered aluminium fins with the frame and drip tray fabricated from heavy gauge aluminium. Face area of coil shall be selected corresponding to air velocity not exceeding 2.5 m/sec.
12. Dehumidification shall be achieved by either reducing effective coil area by solenoid valve arrangement or using the dew point method of control. Whenever dehumidification is required, the control system shall enable a solenoid valve to limit the exchange surface of the evaporating coil, thereby providing a lower evaporating temperature.
13. The humidifier and heaters shall be built-in features in each machine individually. Humidification shall be provided by boiling water in a high-temperature, polypropylene steam generator. The steam shall be distributed evenly into the bypass airstreams of the environment control system to ensure full integration of the water vapor into the supply air without condensation. The humidifier shall have an efficiency of not less the 1.3 kg/kw and be fitted with an auto-flush cycle activated on demand from the microprocessor control system. The humidifier shall be fully serviceable with replacement electrodes. Wastewater shall be flushed from the humidifier by the initiation of the water supply solenoid water valve via a U-pipe overflow system. Drain solenoid valves shall not be used. A microprocessor shall control the humidification and heating through suitable sensors.
14. The following microprocessor controls features shall be displayed on the units:
    a. Room temperature and humidity
    b. Supply fan working status
    c. Compressor working status
    d. Condenser fans working status
    e. Electric heaters working status
    f. Humidifier working status
    g. Manual/Auto unit status
    h. Line voltage value
    i. Temperature set point
    j. Humidity set point
    k. Working hours of main component i.e. compressors, fans, heater, humidifier.
    l. Unit working hours
    m. Current date and time
    n. Type of alarm (with automatic reset or block)
    o. The last 10 intervened alarms

15. The microprocessor shall be able to perform following functions:
    a. Testing of the working of display system
    b. Password for unit calibration values modification
    c. Automatic restart of program
    d. Cooling capacity control
    e. Compressor starting timer
    f. Humidifier capacity limitation
    g. Date and time of last 10 intervened alarm
    h. Start/Stop status storage
    i. Random starting of the unit.
    j. Outlet for the connection to remote system
    k. Temperature and humidity set point calibration
    l. Delay of general alarm activation
    m. Alarm calibration
16. Following alarms shall be displayed on screen of microprocessor unit:
    a. Air flow loss
    n. Clogged filters
    o. Compressor low pressure
    p. Compressor high pressure
    q. Smoke /Fire
    r. Humidifier low water level
    s. High/Low room temperature
    t. High/Low room humidity
    u. Spare external alarms
    v. Water under floor
17. The control system shall include the following settable features:
    a. Unit identification number
    b. Start-up delay, cold start delay, and fan run on timers
    c. Sensor calibration
    d. Remote shutdown and general alarm management
    e. Compressor sequencing
    f. Return temperature control
    g. Choice of modulating output types
18. The unit shall incorporate the following protections:
    a. Single phasing preventers
    b. Reverse phasing
    c. Phase misbalancing
    d. Phase failure
    e. Overload tripping (MPCB) of all components

5.1.1.3.14 *Other Requirements*

- The Command and Control Centre will be the nodal point of availability of all online data and information related to various current and future smart elements and will be connected to other network of services in Chennai through an integration layer.
- The CCC will be established with all hardware, software and network infrastructure including switches and routers and will be maintained by the successful bidder throughout the mentioned period.
- All required Servers, Storage, Software, Firewall, Network Switches for entire project shall be installed in an integrated manner.
- The controls and displays should be mounted in ergonomically designed consoles to keep the operator's fatigue to a minimum and console's efficiency high.
- Integration with Telecom / Internet service providers would aid in automatically capturing the CDR database for person of interest
- **Security:** Under no circumstances the data accumulated and processed by Control Centre should be compromised. Hence, provisions will be made to keep all the data stored in the platform that is highly secured with required security framework implementation. The platform will be hosted in Data centre at a location decided by MTC to be provided by successful bidder. Further the platform will provide an open standards based Integration Bus with API Management, providing full API lifecycle management with governance and security.

5.1.2 Technical Specifications

5.1.2.1 LED Video wall Panel

S. No	Parameter	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
1.	Product details-			
2.	Please mention Make Model No. or Part Code			
	Module Parameters			
3.	Size	240mm (H) × 240mm (H)		
4.	Module Resolution	128(H)×128(W)		
5.	Pitch	1.875 mm		
6.	Density	284.444 pixels/m²		
7.	LED Lamps	SMD1515		
8.	Driver IC	2153 Or equivalent high refresh rate IC		
9.	Module Refresh	3840hz		
10.	Mask	Nor mask		
	Cabinet Parameters			
11.	Cabinet Resolution	256 (H) × 256 (W)		
12.	Cabinet Size	480 mm (H) × 480 mm (W)		

S. No	Parameter	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
13.	Driver Mode	Dynamic 1/32 scan, constant current driving		
14.	Cabinet Power	≤200w		
15.	Cabinet Thickness	≤73mm+5mm		
	Electrical Parameters			
16.	***Optical Ratings***			
a.	*Brightness Of White Balance*	*≥1500cd/m²*		
b.	*View Angle*	*140 degree (horizontal) 140degree(vertical)*		
c.	*View Distance*	*1m-180m*		
d.	*Gray Scale*	*65536*		
e.	*Display Color*	*3-in-1 RGB*		
f.	*Brightness Adjustment*	*100 levels*		
17.	***Power Supply***			
a.	*Operation Power*	*AC100-240V 50-60HZ Switch-able*		
b.	*Maxim Power Consumption*	*1200w/m²*		
c.	*Average Power Consumption*	*600 w/m²*		
18.	**Control System**			
a.	*Correction Scale Level*	*Clear view 18bits - A8S or A10S receiving card or equivalent*		
b.	*Screen Refresh Frequency*	*3840Hz*		
c.	*Gamma Correction*	*-5.0—5.0*		
d.	*Support Input*	*HDMI,DVI,VGA,RJ45,USB,Serial Port*		
e.	*Control Distance*	*Ethernet cable 100m, optical fiber 5km*		
f.	*Color Temperature*	*5000-9300 adjustable*		
g.	*Brightness Correction*	*dot by dot, module by module, cabinet by cabinet*		

S. No	Parameter	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
19.	**Reliability**			
a.	*Temperature*	*Storage: 0°C to 60°C* *Operation: 0°C to 55°C*		
b.	*Humidity*	*Storage:10-70% RH* *Operation:10--60% RH*		
c.	*Operating Life*	*≥100,000 hours*		
d.	*MTBF*	*≥10,000 hours*		
e.	*Continuous Working Time*	*≥72 hours*		
f.	*Protection Level*	*IP25*		
g.	*Out of Control Pixel Rate*	*0.03%*		

5.1.2.2 Video Wall Controller

S. No	Parameter	Minimum Specification	Compliance (Yes/No)	Deviations (if any)
1.	Product details-			
2.	Please mention Make Model No. or Part Code			
3.	Controller	Controller to control Video wall as per requirement along with software		
4.	Chassis	19” Rack mount		
5.	Processor	Latest Generation 64 bit Quad Core processor (3.4 Ghz) or better		
6.	Operating System	Pre-loaded 64-bit Operating System Windows / Linux / Equivalent, with recovery disc		
7.	RAM	16 GB DDR3 ECC RAM		
8.	HDD	2x500 GB 7200 RPM HDD		
9.	Networking	Ethernet Controller with RJ-45 port		
10.	Power Supply	(1+1) Redundant hot swappable		
11.	Accessories	Keyboard and Optical USB mouse		
12.	USB Ports	Minimum 4 USB Ports		

S. No	Parameter	Minimum Specification	Compliance (Yes/No)	Deviations (if any)
13.	Redundancy support	Power Supply, HDD, LAN port & Controller		
14.	Scalability	Display multiple source windows in any size, anywhere on the wall		
15.	Control functions	Brightness/Contrast/ Saturation/ Hue/ Filtering/ Crop/ Rotate		
16.	Inputs	Controller should also have at least 12 or 24 DVI/HDMI inputs for connecting workstations		
17.	Output	To connect to required Displays through HDMI/DVI		
18.	Operating Temperature	10°C to 35°C, 80 % humidity		
19.	Cable & Connections	Successful bidder should provide all the necessary cables and connectors, so as to connect Controller with Display units		
20.	Integration	Seamless integration among display unit, controller, wall management software to be ensured. Preferred to have same OEM.		

5.1.2.3 Video Wall Management Software

S.No	Parameter	Minimum Specifications	Compliance (Yes/No)	Deviations (if any)
1.	Product details-			
2.	Please mention Make Model No. or Part Code			
3.	Display &Scaling	At least 20 layers		
4.	Input Management	All input sources can be displayed on the video wall in freely resizable and movable windows		
5.	Scenarios management	Save and load desktop layouts from local or remote machines		

S.No	Parameter	Minimum Specifications	Compliance (Yes/No)	Deviations (if any)
6.	Layout Management	Support all layout from input sources, Internet Explorer, desktop and remote desktop application		
7.	Multi View Option	Multiple view of portions or regions of Desktop, multiple application can view from single desktop		
8.	Other features	SMTP support		
9.		Remote Control over LAN		
10.		Alarm management		
11.		Remote management		
12.		Multiple concurrent client		
13.		KVM support		

5.1.2.4 Workstation for CCC

S.No	Parameter	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
1.	Product details-			
2.	Please mention Make Model No. or Part Code			
3.	CPU	Quad core CPU with 8 threads or equivalent or better		
4.	Memory	8 GB DDR4 or better		
5.	Hard-Disk Drive	512 GB SSD or better		
6.	Display	2 No.s of 27”-inch LCD / LED Display		
7.	Display ports	4 Display Port / mini Display Ports		
8.	GPU	• Base clock: 1290 Mhz or better • Number of cores: 768 or better • VRAM: 4GB or better • Display connectors: DP 1.4, HDMI 2.0b, dual link-DVI multi-monitor support • Max resolution: 7680 x 4320 @ 60 Hz or better		
9.	Keyboard	Wired keyboard with 104 keys		
10.	Mouse	Wired Optical with USB interface		

S.No	Parameter	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
11.	Ports	USB Ports including 2 USB 3.0 Ports and audio ports for microphone and headphone		
12.	Cabinet	Mini Tower.		
13.	Operating system	Windows 10 64-bit operating system		
14.	Antivirus	To be provided		
15.	Network Connectivity	• RJ-45 (10/100/1000 Base-T) • Wireless 802.11 a/b/g/n/ac or better		
16.	Power Supply (SMPS)	700 W or better		

5.1.2.5 Network MFD Color Laser Printers

S. No	Parameter	Minimum Specification	Compliance (Yes/No)	Deviations (if any)
1.	Product details-			
2.	Please mention Make Model No. or Part Code			
3.	Print Speed	• Black : 16 ppm or above on A3, 24 ppm or above on A4 • Colour : 8 ppm or above on A3, 12 ppm or above on A4		
4.	Resolution	600 X 600 DPI		
5.	Memory	8 MB or more		
6.	Paper Size	A3, A4, Legal, Letter, Executive, custom sizes		
7.	Paper Capacity	250 sheets or above on standard input tray, 100 Sheet or above on Output Tray		
8.	Duty Cycle	25,000 sheets or better per month		
9.	OS Support	Linux, Windows 2000, Vista, 7, 8, 8.1		
10.	Interface	Ethernet Interface		
11.	Other requirement(s)	Shall have the ability to Scan, Send and Receive Fax		

5.1.2.6 IP Phone Specifications

S.No	Parameter	Minimum Specifications	Compliance (Yes/No)	Deviations (if any)
1.	Product details-			
2.	Please mention Make Model No. or Part Code			
3.	Display	2 line or more, Monochrome display for viewing features like messages, directory, operator name, etc.		
4.	Integral switch	10/100 mbps for a direct connection to a 10/100BASE-T Ethernet network through an RJ-45 interface		
5.	Speaker Phone	Yes		
6.	Head set	Port for Head set (Headset also to be provided)		
7.	VoIP Protocol	SIP V2		
8.	PoE	IEEE 802.3af or better		
9.	Supported Protocols	SNMP, DHCP, DNS		
10.	Codecs	G.711, G.722 including handset and speakerphone		
11.	Speaker Phone	• Full duplex speaker phone with echo cancellation • Speaker on/ off button, microphone mute		
12.	Volume control	Easy decibel level adjustment for speaker phone, handset and ringer		
13.	Phonebook/Address book	Minimum 100 contacts		
14.	Call Logs	Access to missed, received, and placed calls. (Minimum 20 overall)		
15.	Clock	Time and Date on display		
16.	Ringer	Selectable Ringer tone		
17.	Directory Access	LDAP standard directory		

5.1.2.7 Digital Calling VoIP & EPABX including 2 - PRI

The system shall support minimum 500 IP Phones with at least 100 concurrent sessions with features like –

- Provide reports for calls based on records, calls on a user basis, calls through gateways etc.
- Able to add bulk add, delete, and update operations for devices and users
- Session Initiation Protocol (SIP) Trunk support
- Centralized, configuration database, Web based management
- Lightweight Directory Access Protocol (LDAP) directory interface
- Facilities to users like Call Back, Call Forward, Directory Dial, Last number Redial, etc.
- Calling Line Identification

S.No	Description	Minimum Specification	Compliance (Yes/No)	Deviations (if any)
1.	Product details-			
2.	Please mention Make Model No. or Part Code			
3.	Technology	PCM-TDM , IP, Non-blocking		
4.	Interface	Should support all telecom interfaces in Indian Telecom Service provider offerings		
5.	Type of Interface	ISDN interface for digital, basic interface for Analog lines		
6.	No. of lines - ,ISDN PRI lines & Analog / Digital Extensions	2 PRI, 32 Extensions (IP / Analog / Digital)		
7.	Type of Extension Support	Analog , Digital and IP		
8.	Expansion of Extensions	Multiples of 8 / 16		
9.	Run Distance	Not less than 800 mtrs. on 0.5mm dia. Cable		
10.	Max. Loop resistance for analog trunk lines Extensions	2500 ohms including telephone		
11.	Requirement at the time of supply	02 ISDN PRI, 24 Analog Ports & 8 Digital extension ports. Expected to handle at least 30 external lines.		
12.	Contact centre Expansion available (Max. capacity)	It must support at least 16 Call centre Agents		

S.No	Description	Minimum Specification	Compliance (Yes/No)	Deviations (if any)
13.	Max. loop resistance for analog trunk lines	1200 ohms at –48 Volts DC		
14.	Other	• ISDN supplementary services for Digital phone • Support for digital trunk lines • Working on 230v AC mains and DC voltage • Support for ACD call centre with CTI and advanced call routing		
15.	Design of EPABX System	Modular with universal slots, Wall/Rack mountable		
16.	Conferencing	5 party conferencing to be provided (to be configurable dynamically)		

5.1.2.8 Online UPS (100 KVA)

S. No	Parameter	Minimum Specification	Compliance (Yes/No)	Deviations (if any)
1.	Product details-			
2.	Please mention Make Model No. or Part Code			
3.	Capacity	Adequate capacity to cover all above IT Components at respective location		
4.	Output Wave Form	Pure Sine wave		
5.	Input Power Factor at Full Load	>0.90		
6.	Input	Three Phase 3 Wire for over 100 KVA		
7.	Input Voltage Range	305-475VAC at Full Load		
8.	Input Frequency	50Hz +/- 3 Hz		
9.	Output Voltage	400V AC, Three Phase for over 100 KVA UPS		

S. No	Parameter	Minimum Specification	Compliance (Yes/No)	Deviations (if any)
10.	Output Frequency	50Hz+/- 0.5% (Free running); +/- 3% (Sync. Mode)		
11.	Inverter efficiency	>90%		
12.	Over All AC-AC Efficiency	>85%		
13.	UPS shutdown	UPS should shutdown with an alarm and indication on following conditions 1) Output over voltage 2) Output under voltage 3) Battery low 4) Inverter overload 5) Over temperature 6) Output short		
14.	Battery Backup	4 hours in full load		
15.	Battery	VRLA (Valve Regulated Lead Acid) SMF (Sealed Maintenance Free) Battery		
16.	Indicators & Metering	Indicators for AC Mains, Load on Battery, Fault, Load Level, Battery Low Warning, Inverter On, UPS on Bypass, Overload, etc. Metering for Input Voltage, Output Voltage and frequency, battery voltage, output current etc.		
17.	Audio Alarm	Battery low, Mains Failure, Over temperature, Inverter overload, Fault etc.		
18.	Cabinet	Rack / Tower type		
19.	Operating Temp	0ºC to 50ºC		

5.1.2.9 Indoor Fixed Dome Cameras for internal surveillance with storage

S. No	Parameter	Minimum Specification	Compliance (Yes/No)	Deviations (if any)
1.	Product details-			
2.	Please mention Make Model No. or Part Code			

S. No	Parameter	Minimum Specification	Compliance (Yes/No)	Deviations (if any)
3.	Video Compression	H.264 / H.265 or better		
4.	Video Resolution	1080p or better		
5.	Frame rate	Min. 25 fps		
6.	Image Sensor	1/3" Progressive Scan CCD / CMOS		
7.	Lens Type	Varifocal, IR Correction Full HD lens compatible to camera imager		
8.	Lens#	Auto IRIS 2.8-10mm		
9.	Multiple Streams	Dual streaming with 2nd stream at minimum 720P at 30fps at H.264 individually configurable		
10.	Minimum Illumination	Colour: 0.1 lux, B/W: 0.01 lux (at 30 IRE)		
11.	IR Cut Filter	Automatically Removable IR-cut filter		
12.	Day/Night Mode	Colour, Mono, Auto		
13.	S/N Ratio	≥ 50 dB		
14.	Auto adjustment + Remote Control of Image settings	Colour, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, Gain Control, Auto back focus		
15.	Wide Dynamic Range	True WDR upto 80 db		
16.	Audio	Full duplex, line in and line out, G.711, G.726		
17.	Local storage	microSDXC card 128GB (Class 10) or better In the event of failure of connectivity to the central server the camera shall record video locally on the SD card automatically. After the connectivity is restored these recordings shall be automatically merged with the server recording such that no manual intervention is		

S. No	Parameter	Minimum Specification	Compliance (Yes/No)	Deviations (if any)
		required to transfer the SD card based recordings to server.		
18.	Protocol	HTTP, HTTPS, FTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, ONVIF Profile S &G		
19.	Security	Password Protection, IP Address filtering, User Access Log, HTTPS encryption		
20.	Intelligent Video	Motion Detection & Tampering alert		
21.	Alarm I/O	Minimum 1 Input & Output contact for 3rd part interface		
22.	Operating conditions	0ºC to 50°C		
23.	Casing	NEMA 4X / IP-66 rated & IK 09		
24.	Certification	UL / CE / FCC		
25.	Power	802.3af PoE (Class 0) and 12VDC/24AC		

5.1.2.10 L3 Switch

S. No	Parameter	Minimum Specification	Compliance (Yes/No)	Deviations (if any)
1.	Product details-			
2.	Please mention Make Model No. or Part Code			
3.	Ports	• 24 or 48 (as per requirements) 10/100/1000 Base-TX Ethernet ports and extra 2 nos of Base-SX/LX ports • All ports can auto-negotiate between 10Mbps/ 100Mbps/ 1000Mbps, half-duplex or full duplex and flow control for half-duplex ports.		
4.	Switch type	Layer 3		
5.	MAC	Support 8K MAC address.		
6.	Backplane	56 Gbps or more Switching fabric capacity (as per network configuration to meet performance requirements)		

S. No	Parameter	Minimum Specification	Compliance (Yes/No)	Deviations (if any)
7.	Forwarding rate	Packet Forwarding Rate should be 40.0 Mpps or better		
8.	Port Features	Must support Port Mirroring, Port Trunking and 802.3ad LACP Link Aggregation port trunks		
9.	Flow Control	Support IEEE 802.3x flow control for full-duplex mode ports.		
10.	Protocols	• Support 802.1D, 802.1S, 802.1w, Rate limiting • Support 802.1Q VLAN encapsulation, IGMP v1, v2 and v3 snooping • 802.1p Priority Queues, port mirroring, DiffServ • 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 Strict priority queuing & Sflow • Support for IPV6 ready features with dual stack • Support upto 255 VLANs and upto 4K VLAN IDs		
11.	Access Control	• Support port security • Support 802.1x (Port based network access control). • Support for MAC filtering. • Should support TACACS+ and RADIUS authentication		
12.	VLAN	• Support 802.1Q Tagged VLAN and port based VLANs and Private VLAN • The switch must support dynamic VLAN Registration or equivalent • Dynamic Trunking protocol or equivalent		

S. No	Parameter	Minimum Specification	Compliance (Yes/No)	Deviations (if any)
13.	Protocol and Traffic	• Network Time Protocol or equivalent Simple Network Time Protocol support • Switch should support traffic segmentation • Traffic classification should be based on user-definable application types: TOS, DSCP, Port based, TCP/UDP port number		
14.	Management	• Switch needs to have RS-232 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		

5.1.2.11 75'' Touch screen Smart TV for conference room

S.No	Specification	Minimum Requirements	Compliance (Yes/No)	Deviations (if any)
1.	Product details-			
2.	Please mention Make Model No. or Part Code			
3.	Type	Industrial Grade Touch Display for 24x7 operations		
4.	Screen Size	75" or better		
5.	Type	LED Backlit		
6.	Panel	IPS LCD		
7.	Aspect Ratio	16:9		
8.	Resolution	Ultra HD (4K), 3840 x 2160 or better		
9.	Brightness	300 nits or better		
10.	Orientation	Portrait and Landscape		

S.No	Specification	Minimum Requirements	Compliance (Yes/No)	Deviations (if any)
11.	Contrast Ratio	1200:1 or better		
12.	Connectors	DVI, HDMI, VGA		
13.	Network Connectivity	• RJ-45 (10/100/1000 Base-T) • Wireless 802.11 b/g/n or better		
14.	Colour Depth	16-bit colour		
15.	Input Voltage	150-240v, 50 Hz		
16.	Operating temperature	0ºC to 50ºC or better		
17.	Viewing angle	178 degree x 178 degree		
18.	Response	12ms or better		
19.	Power supply	inbuilt or external		
20.	Accessories	Accessories for Wall mount, Desktop with suitable specification for video Conferencing,1080p/30fps camera with microphone required		
21.	Certification	CE, FCC		
22.	Operating System	Android or other similar TV operating system with ability to install applications from a publically available application repository		
23.	Other requirements	Shall support casting from iOS, Android and Windows devices through Wi-Fi		

5.2 Data Centre

5.2.1 Data Centre Service Specification

5.2.1.1 Compute

S.No	Requirement	Description	Compliance (Yes/No)	Deviations (if any)
1.	Product details-			
2.	Please mention Make Model No. or Part Code			
3.	Compute instances – • General Purpose • Memory optimized • Compute optimized • Storage optimized • GPU instances	The provider should offer the following instance types – • General Purpose – optimized for generic applications and provides a balance of compute, memory, and network resources. • Memory optimized – optimized for memory applications • Compute optimized – optimized for compute applications • Storage optimized – include very fast/large amount of local storage for NoSQL databases and Hadoop • GPU – intended for graphics and general purpose GPU compute applications		
4.	Compute instances – Burstable performance	The provider should offer instances that provide a baseline level of CPU performance with the ability to burst above the baseline.		
5.	Compute instances – Dedicated	The provider should offer instances that run on hardware dedicated to a single customer.		

S.No	Requirement	Description	Compliance (Yes/No)	Deviations (if any)
6.	OS Support – Linux	The provider should be able to support following Linux distributions - (Red Hat, SUSE, Ubuntu, CentOS, and Debian)		
7.	OS Support – Windows	The provider should be able to support the latest version in the market (Windows Server 2019) and the previous version (Windows Server 2016)		
8.	Resize virtual cores, memory, storage seamlessly	Customer must be able to specify and modify server configuration (CPU, memory, storage) parameters seamlessly and without outage.		
9.	Local disk/Instance store	The service should support local storage for compute instances to be used for temporary storage of information that changes frequently.		
10.	Provision multiple concurrent instances	The service must offer self-service provisioning of multiple instances concurrently either through a programmatic interface (API/CLI) or through a management console.		
11.	Instance affinity - logical grouping of instances within a single data centre	Customer should be able to logically group instances together for applications that require low network latency and/or high network throughput.		
12.	Instance anti-affinity -two or more instances hosted in different data centres	Customer should be able to split and host instances across different physical data centres to ensure that a single physical failure event does not take all instances offline.		
13.	Auto Scaling support	The service should be able to automatically increase the number of instances during demand spikes to maintain		

S.No	Requirement	Description	Compliance (Yes/No)	Deviations (if any)
		performance and decrease capacity during lulls to reduce costs.		
14.	Bring your own image/Instance Import	Customer 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.		
15.	Export Instance Image	The 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.		
16.	Instance maintenance mitigation	The 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.		
17.	Instance failure recovery	The service must be architected in such a way to automatically restart instances on a healthy host if the original physical host fails.		
18.	Instance restart flexibility	The provider must be able to schedule events for customer's instances, such as a reboot, stop/start, or retirement. Depending on the event, customer might be able to take action to control the timing of the event.		
19.	Support for Docker containers	The service should support containers, including Docker and/or other containerization platforms.		
20.	Highly scalable, high performance	The provider should offer a highly scalable, high performance container management service.		

S.No	Requirement	Description	Compliance (Yes/No)	Deviations (if any)
	container management service			
21.	Event-driven computing that runs code in response to events	The service should be able to run customer code in response to events and automatically manage the compute resources.		
22.	License portability and support – Microsoft	The provider should offer license portability and support for Microsoft apps like SQL Server and SharePoint Server.		
23.	License portability and support – Oracle	The provider should offer license portability and support for Oracle apps like Oracle Database 11g.		
24.	License portability and support – SAP	The provider should offer license portability and support for SAP apps like HANA.		
25.	License portability and support – IBM	The provider should offer license portability and support for IBM apps like DB2 and Websphere.		
26.	Pay-as-you-go pricing	The provider should offer a simple pay-as-you-go pricing where customers can pay for compute capacity by the hour with no long-term commitments.		

5.2.1.2 Storage

S.No	Parameter	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
1.	Product details-			
2.	Please mention Make Model No. or Part Code			
3.	Controllers and Architecture	• Storage Should be Fully Symmetric and fully distributed clustered Architecture written for Scale-Out Storage operations		

S.No	Parameter	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
		• Scale out storage should be configured with minimum 8 controllers of the same type Over all storage cluster should be upgradable to min 2 x numbers of Storage controllers / Storage nodes, without any disruptions / downtime to production workflow for performance, capacity enhancement, software / firmware upgrades. • The storage cluster should support linear scalability of performance and capacity. • All storage nodes / controllers must be active for all Storage shares, contributing in performance and capacity of the system • Storage Controllers should have Intel processors.		
4.	Onboard Memory	The scale out storage must be configured with minimum 256GB globally coherent, DRAM based cache/memory.		
5.	Operating System Network Ports	Scale-Out Storage operating system should have Fully journaled, fully distributed, specialized Operating System by OEM or Software Defined Storage solution, dedicated for serving data efficiently and customized for True Scale-Out Storage. Entire data should automatically balance across proposed controllers/nodes		

S.No	Parameter	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
		within each tier without any administrative intervention		
		The scale out storage should be offered with minimum 16 x 10Gbps SFP+ ports, and should be scalable to 2x the number of offered ports		
6.	Disk support	Storage cluster should have capability to support different kinds of disks tiers likes SSD, SAS, SATA/NL-SAS drives within single file system.		
7.	Redundancy with No Single Point of Failure (SPOF)	• The Scale-Out Storage System should be able to protect the data against simultaneous three disks failure without any data loss and data unavailability • Scale-Out Storage should have self-optimizing architecture so the system does not require defragmentation, nor consistency check like “fsck” in the event of an ungraceful shutdown of the cluster to ensure higher uptime. • All data should be striped across all storage controllers in proposed storage system, so that performance of all controllers can be utilized for all read and write operations. • The backend internal connectivity between storage controllers /		

S.No	Parameter	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
		storage nodes should be using high performance Infiniband or 10 /40 GigE network with no single point of failure. • The backend internal connectivity configured between Storage controllers / Storage nodes themselves and between storage controllers / nodes and disk controllers, if configured, should be redundant and there should be "No Single Point of Failure". • Redundant and Hot replaceable modules: Controllers, Hard Disk Drive and power supplies (230V AC, 50 Hz.) • The Complete multi-controller Storage System Solution should be fully redundant, configured in High Availability mode and should NOT have any Single Point of Failure (SPOF).		
8.	Total Storage Capacity	• Scale out storage should be configured with 3 PB usable capacity with triple disk failure protection, using equal to or less than 12TB NL-SAS/SATA HDD • The storage should be scalable upto 5x the capacity as a single file		

S.No	Parameter	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
		system and a single global namespace.		
9.	Capacity/performance Expansion	• There should not be any downtime or migration activity required in the event it is needed to add additional capacity or additional performance to the storage system. • Storage solution should enable linear scalability of performance and capacity (ie X TB increase in capacity should lead to Y GBps increase in performance) • In the event of addition of storage controller/storage node to storage solution, existing data should be rebalanced across all nodes of storage controllers / storage nodes automatically. This autobalance should be done with low priority avoiding any impact to client performance. • Addition of storage controller / storage nodes should not require any complicated configuration of new controller/node. It should be done easily, seamlessly and without having any impact to user access. • Storage file system shall not require metadata performance tuning.		

S.No	Parameter	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
		• The system must be able to support policy based tiering to different storage tiers with Storage sub-system.		
10.	Protection Levels	• Storage solution should support required protection level which can protect data against simultaneous 3 disks failures • Should have capability to change the protection level on-the-fly. • Should be able to assign protection level on cluster, directory or file level.		
11.	Protocol Support	• Network protocol Support: Must provide access for a variety of operating systems using native OS protocols. Licenses if any, required for such protocol access to be provided. • Should support user security mechanisms like AD, LDAP and NIS. • Storage solution must support multiple protocols at the same time on the same piece of hardware (No separate, individually managed servers shall be required). • License should be provided for all the protocol and it should be perpetual.		

S.No	Parameter	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
12.	Client Load Balancing	Storage System should have capability to load balance client connectivity across these multiple controllers so that all clients gets distributed across all existing controllers/nodes to avoid any performance hotspot.		
13.	Heterogenous support for end user systems	Operating system support RedHat Linux, Suse Linux, Windows Servers 2003/2008 or later , Windows XP/7 or later. Unix Based operating systems like SUN solaris, HP Unix, IBM AIX		
14.	Management Interface software	Support the management, administration and configuration of the whole storage platform through a single management interface along with CLI		
15.	Security	The system must support encrypting data at rest. The system must be able to support Write Once Read Many (WORM) compliant to SEC17a-4. The system must support Role Base Access Control with Integration with Active Directory and LDAP . The system must be able to support System Auditing for system as well as supported protocols. The system must support multiple DNS.		

S.No	Parameter	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
		The system must be able to support Anti-Virus Scanning through Internet Content Adaptation (ICAP) protocol or equivalent capability to provide virus scanning functionality. The system should have file system integrity and data integrity checks built in to prevent data loss due to bit rot and other soft errors		

5.2.1.3 Networking

S.No	Requirement	Description	Compliance (Yes/No)	Deviations (if any)
1.	Product details-			
2.	Please mention Make Model No. or Part Code			
3.	Multiple network interface/instance	The service should be able to support multiple (primary and additional) network interfaces.		
4.	Multiple IP addresses/instance	The service should be able to support multiple IP addresses per instance. Use cases include hosting multiple websites on a single server and network appliances (such as load balancers) that have multiple private IP addresses for each network interface.		
5.	Ability to move network interfaces and IPs between instances	The service should support the ability to create a network interface, attach it to an instance, detach it from an instance, and attach it to another instance.		

S.No	Requirement	Description	Compliance (Yes/No)	Deviations (if any)
6.	Enhanced networking support	The service should support capabilities such as single root I/O virtualization for higher performance (packets per second), lower latency, and lower jitter.		
7.	Network traffic logging - Log traffic flows at network interfaces	The service should support capturing information about the IP traffic going to and from network interfaces.		
8.	Auto-assigned public IP addresses	The service should be able to automatically assign a public IP to the instances.		
9.	IP Protocol support	The service should be able to support multiple IP protocols, including TCP, UDP, and ICMP protocols.		
10.	Use any network CIDR, including RFC 1918	The service should be able to support IP address ranges specified in RFC 1918 as well as publicly routable CIDR blocks.		
11.	Static public IP addresses	The provider must support IP addresses associated with a customer account, not a particular instance. The IP address should remain associated with the account until released explicitly.		
12.	Auto-created default virtual private network	The service should be able to create a default private network and subnet with instances launching into a default subnet receiving a public IP address and a private IP address.		
13.	Subnets within private network	Customer should be able to create one or more subnets within private network with a single Classless Inter-Domain Routing (CIDR) block.		
14.	Subnet level filtering	The service should support subnet level filtering – Network ACLs that		

S.No	Requirement	Description	Compliance (Yes/No)	Deviations (if any)
	(Network ACLs)	act as a firewall for associated subnets, controlling both inbound and outbound traffic at the subnet level.		
15.	Ingress filtering	The service should support adding or removing rules applicable to inbound traffic (ingress) to instances.		
16.	Egress filtering	The service should support adding or removing rules applicable to outbound traffic (egress) originating from instances.		
17.	Disable source/destination checks on interfaces	The service should support the ability to disable source/destination check on network interfaces. By default, compute instances perform source/destination checks.		
18.	Configure proxy server (NAT instance) at network level	The service should support NAT instances that can route traffic from internal-only instances to the Internet.		
19.	Site-to-site managed VPN service	The service should support a hardware based VPN connection between the cloud provider and customer data centre.		
20.	Virtual Network Peering	The service should support connecting two virtual networks to route traffic between them using private IP addresses.		
21.	Multiple VPN Connections per Virtual Network	The service should support creating multiple VPN connections per virtual network		
22.	BGP for high availability and reliable failover	The provider should support Border Gateway Protocol. BGP performs a robust liveness check on the IPSec tunnel and simplifies the failover procedure that is invoked when one VPN tunnel goes down.		

S.No	Requirement	Description	Compliance (Yes/No)	Deviations (if any)
23.	Private connection to customer data centres	The provider should support direct leased-line connections between cloud provider and a customer data centre, office, or colocation environment, which in many cases can reduce network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.		
24.	DNS based global load balancing	The service should support Load balancing of instances across multiple host servers.		
25.	Load balancing supports multiple routing methods	The service should support multiple routing mechanism including round-robin, failover, sticky session etc.		
26.	Front-end Load Balancer	The service should support a front-end load balancer that takes requests from clients over the Internet and distributes them across the instances that are registered with the load balancer.		
27.	Back-end Load Balancer	The service should support an internal load balancer that routes traffic to instances within private subnets.		
28.	Health checks - monitor the health and performance of application	The service should support health checks to monitor the health and performance of resources.		
29.	Integration with Load Balancer	The service should support integration with load balancer.		
30.	Low Latency	The CSP should be able to provide a 10GB network connectivity between the servers if required.		
31.	Support for storage allocated as local disk to a single VM	The provider should offer persistent block level storage volumes for use with compute instances.		

S.No	Requirement	Description	Compliance (Yes/No)	Deviations (if any)
32.	Storage volumes > 1 TB	The provider should offer block storage volumes greater than 1 TB in size.		
33.	SSD backed storage media	The service should support solid state drive (SSD) backed storage media that offer single digit millisecond latencies.		
34.	Provisioned I/O support	The service should support the needs of I/O-intensive workloads, particularly database workloads that are sensitive to storage performance and consistency in random access I/O throughput.		
35.	Encryption using provider managed keys	The service should support encryption of data on volumes, disk I/O, and snapshots using industry standard AES-256 cryptographic algorithm.		
36.	Encryption using customer managed keys	The service should support encryption using customer managed keys.		
37.	Durable snapshots	The service should support point-in-time snapshots. These snapshots should be incremental in nature.		
38.	Ability to easily share snapshots globally	The Service should support sharing of snapshots across regions making it easier to leverage multiple regions for geographical expansion, data centre migration, and disaster recovery.		
39.	Consistent Input Output per second (IOPS)	The service should support a baseline IOPS/GB and maintain it consistently at scale		
40.	Annual Failure Rates <1%	The service should Annual Failure Rates <1%		
41.	Scalable object storage service	The provider should offer secure, durable, highly-scalable object		

S.No	Requirement	Description	Compliance (Yes/No)	Deviations (if any)
		storage for storing and retrieving any amount of data from the web.		
42.	Low cost archival storage with policy support	The provider should support an extremely low-cost storage service that provides durable storage with security features for data archiving and backup.		
43.	Support for Server-side Encryption	The service should support encryption for data at rest using 256-bit Advanced Encryption Standard (AES-256) encryption to encrypt your data.		
44.	Support for Server Side Encryption with Customer-Provided Keys	The service should support encryption using customer-provided keys. These keys should be used to manage both the encryption, as data is written to disks, and decryption, when data is accessed.		
45.	Support for Server Side Encryption with a Key Management Service	The service should support encryption using a Key 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.		
46.	Object lifecycle management	The 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.		
47.	Data Locality	The provider should provide a strong regional isolation, so that objects stored in a region never leave the region unless customer explicitly transfers them to another region.		

S.No	Requirement	Description	Compliance (Yes/No)	Deviations (if any)
48.	Object change notification	The service should be able to send notifications when certain events happen at the object level (addition/deletion).		
49.	High-scale static web site hosting	The 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).		
50.	Object Versioning	The Service should support versioning, where multiple versions of an object can be kept in one bucket. Versioning protects against unintended overwrites and deletions.		
51.	Flexible access-control mechanisms	The service should support flexible access-control policies to manage permissions for objects.		
52.	Audit logs	The 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.		
53.	Multi-factor delete	The service should support multi-factor delete as an additional security option for storage buckets		
54.	Lower Durability offering	The service should support a lower cost option for noncritical, reproducible data at lower levels of redundancy.		
55.	Parallel, multipart upload	The 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.		

S.No	Requirement	Description	Compliance (Yes/No)	Deviations (if any)
56.	CDN option for users	The provider should offer a service to speed up distribution of static and dynamic web content.		
57.	Strong Consistency	The service should support read-after-write consistency for PUT operations for new objects.		
58.	Storage gateway appliance for automated enterprise backups	The provider should offer a storage gateway appliance for seamlessly storing on-premises data to the cloud.		

5.2.1.4 Virtualisation Security

Virtualisation security design should meet security, availability, manageability, performance, and recoverability aspects on the solution design. It should be noted that some of the following Virtualisation Security Monitoring may redefined by vendors to fit their own security products and without any change in outcome as listed below:

Item	Requirement	Description	Compliance (Yes/No)	Deviations (if any)
1.	Product details-			
2.	Please mention Make Model No. or Part Code			
3.	Network Segmentation	VLANs and PVLANs should provide a simple form of network segmentation. A VLAN represents an IP address space by separating workloads		
4.	Macro-segmentation	High-level separation of objects, including but not limited to applications, clusters, and networks. Including • Segmenting production clusters, development clusters, and DMZ clusters • Segmenting applications from one another with routers and/or firewalls		
5.	Application Isolation	Construction of a security boundary around the workloads		

Item	Requirement	Description	Compliance (Yes/No)	Deviations (if any)
		of an entire application. Application isolation should be able to use both firewall features and network address translation to maintain control of traffic to any of the application workloads.		
6.	Security Policy Management (Orchestration)	Service-Defined Firewall architecture should include a centralized policy manager that can be accessed through a simplified user interface, an advanced user interface, or/and declarative API. As a security policy, • Domain – A logical construct representing a security zone and all rules and groups. • Security Policy – A structure to encompass various security elements, including firewall rules and service configurations. Security Policies include Distributed Firewall Policies, Gateway Policies, Network Introspection Policies, and Endpoint Policies. • Rule – Set of parameters that flows are evaluated against and that define which action should be taken upon match. Rules include parameters such as Source/Destination, Service, Context Profile, Logging, and Tag. • Group – Grouping construct to group the different objects statically and dynamically. Used in Source/Destination of Rules. Group inclusion includes virtual machines,		

Item	Requirement	Description	Compliance (Yes/No)	Deviations (if any)
		logical ports, IP/MAC sets, AD User Groups, and other nested groups. Dynamic inclusion for VMs can be based on tag, virtual machine name, operating system type, or computer name. • Service – Defines a combination of port and protocol. Used to classify traffic based on port/protocol. Predefined services or user-created services can be used in Rules. • Context Profile – Defines one context-aware attribute, including APP-ID and/or Domain name, as well as sub attributes such as application version or cipher set. Rules can optionally include a context profile to enable a Layer 7 firewall.		
7.	Service Insertion Tied to the Workload	• Service insertion policies for intrusion detection systems (IDS) and intrusion prevention systems (IPS) should be bound to the workload in Virtualisation. • By having a service virtual machine on each host, the deep inspection can happen prior to the egress of the host onto the physical network. • While this type of distributed model does consume more compute and storage resources, it provides a much greater advantage to the efficiency of the security architecture.		

5.2.2 Smart Data Centre Infrastructure (On-Premises or On-Cloud) – guidelines

- Any additional physical space required as per proposed design of SI, wherein some local storage is being envisaged for better data availability requirements, then minimal space (to the tune 1-2 racks space) may be provisioned at MTC post evaluating the design and need for the same. The bidder has to take care of the interior, electrical works DC/DR racks, IT Compute, Storage, Network, Security and Non IT components including power and cooling.
- Indicative list of ICT equipment to be provisioned and maintained by the SI at the DC on-premises or on-cloud.
- The DR on a cloud is required only for on-premises DC as the Cloud DC is expected to have their own DR measures.
- The DC/DR cloud shall necessarily be one of empanelled cloud services providers of MeitY GoI and shall comply with ISO27001 standards. It must be located within India.
- The Business Continuity Planning (BCP) shall be configurable as per requirements of BCP requirements prescribed in this RFP. The mass broadcasting / messaging in case of likely disaster shall be done in accordance to guidance of Transport department / Government of Tamil Nadu guidelines.

Technical Specifications for Smart Data Centre and Disaster Recovery Infrastructure Components

5.2.2.1 Data Centre TOR (Top of the Rack) Switch

S.No	Parameter	Minimum Requirement Specification	Compliance (Yes/No)	Deviations (if any)
1.	Product details-			
2.	Please mention Make Model No. or Part Code			
3.	Architecture	• The Switch should support non-blocking Layer 2 switching and Layer 3 routing • There switch should not have any single point of failure like switching fabric, support module, power supplies and fans etc. should have 1:1/N+1 level of redundancy. • Switch support on line hot insertion and removal of different parts like modules/power supplies/fan tray should not require switch reboot and disrupt the functionality of the system		

S.No	Parameter	Minimum Requirement Specification	Compliance (Yes/No)	Deviations (if any)
		• Switch should support the complete STACK of IP V4 and IP V6 services • Switch and different modules used should function in line rate and should not have any port with oversubscription ratio applied • Need to have 48 X 1G/10G Ports populated with following interfaces. • 12 x 1 G SFP; 12 RJ45 SFP & 18 Port SFP+ • 4 X 40GBE QSFP Fiber interface (Two wire Multi Mode / LC / Two wire single mode - LC Fiber interface using OM4 minimum distance of 150 mtr)		
4.	Performance Requirement	• Switch should support 12,000 IPv4/IPv6 routes entries in routing table and should support at least 2000 multicast routes • Switch should support Graceful Restart for OSPF, BGP etc. • Switch should support minimum 32 VRF instances • The switch should support Hardware based Multi-Terabit/s L3 load-balancing at wire speed using standard protocols • Switch should support up to 1.4 TBps of switching capacity including the services: ✓ Switching ✓ IP Routing (Static/Dynamic) ✓ IP Forwarding ✓ Policy Based Routing ✓ QoS ✓ ACL and Other IP Services ✓ IP V.6 host and IP V.6 routing		

S.No	**Parameter**	**Minimum Requirement Specification**	**Compliance (Yes/No)**	**Deviations (if any)**
5.	Advance Features	• Switch should support Network Virtualization using Virtual Over Lay Network • Switch should support VXLAN (RFC7348) and EVPN as draft-ietf-l2vpn-evpn-04 for supporting Spine - Leaf architecture to optimise the east - west traffic flow inside the data centre or should support in the roadmap • Switch should support Python, NetConf, XML etc.		
6.	Layer2 Features	• Spanning Tree Protocol (IEEE 8201.D, 802.1W, 802.1S • Switch should support VLAN Trunking (802.1q) and should support 4096 VLAN • Switch should support basic Multicast IGMP v1, v2, v3 • Switch should support Industry Standard Port/Link Aggregation for All Ports across any module or any port. • Switch should support Jumbo Frames up to 9K Bytes on 1G/10G Ports • Support for broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from storm due to network attacks and vulnerabilities • Switch should support Link Layer Discovery Protocol as per IEEE 802.1AB for finding media level failures		
7.	Layer3 Features	• Switch should support all physical ports to use either in Layer2 or Layer 3 mode and also should support layer 3 VLAN Interface and Loopback port Interface		

S.No	Parameter	Minimum Requirement Specification	Compliance (Yes/No)	Deviations (if any)
		• Switch should support static and dynamic routing using: ✓ Static routing ✓ OSPF V.2 using MD5 Authentication ✓ ISIS using MD5 Authentication ✓ BGP V.4 using MD5 Authentication ✓ Should support route redistribution between these protocols • Switch should recon verge all dynamic routing protocol at the time of routing update changes i.e. Non-Stop forwarding for fast re-convergence of routing protocols • Switch should be capable to work as DHCP server and relay • Switch should provide multicast traffic reachable using: ✓ PIM-SM ✓ PIM-SSM or DM ✓ IGMP V.1, V.2 and V.3 • Switch should support Multicast routing of minimum 8 way Equal Cost Multi Path load splitting. However, the SI shall do the required hard ware sizing		
8.	Quality of Service	• Switch system should support 802.1P classification and marking of packet using: ✓ CoS (Class of Service) ✓ DSCP (Differentiated Services Code Point) • Switch should support for different type of QoS features for ream time traffic differential treatment using ✓ Class- Based Weighted Random Early Detection ✓ Strict Priority Queuing		

S.No	Parameter	Minimum Requirement Specification	Compliance (Yes/No)	Deviations (if any)
		• Switch should support to trust the QoS marking/priority settings of the end points as per the defined policy • Switch should support Flow control of Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end for receiving traffic as per IEEE 802.3x		
9.	Security	• Switch should support for deploying different security for each logical and physical interface using Port Based access control lists of Layer-2 to Layer-4 in IP V.4 and IP V.6 and logging for fault finding and audit trail • Switch should support control plane i.e. processor and memory Protection from unnecessary or DoS traffic by control plane protection policy • Switch should support for stringent security policies based on time of day of Layer-2 to Layer-4 • Switch should support for external database for AAA using: • TACACS and RADIUS • Switch should support DHCP Snooping, Dynamic Arp Inspection, IP Source Guard. • Switch should support for Role Based access control (RBAC) for restricting host level network access as per policy defined		
10.	Manageability	• Switch should support for embedded RMON/RMON-II for central NMS management and monitoring		

S.No	**Parameter**	**Minimum Requirement Specification**	**Compliance (Yes/No)**	**Deviations (if any)**
		• Switch should support for sending logs to multiple centralised syslog server for monitoring and audit trail • Switch should provide remote logging for administration using: Telnet and SSH • Switch should support for management and monitoring status using different type of Industry standard NMS using: • SNMP v1,v2 and v3 • Switch should support Real time Packet Capture using Wire shark in real time for traffic analysis and fault finding • Switch should support central time server synchronisation using Network Time Protocol NTP V.4 • Switch should support for providing granular MIB support for different statistics of the physical and logical interfaces • Switch should support for predefined and customised execution of script for device mange for automatic and scheduled system status update for monitoring and management • Switch should provide different privilege for login in to the system for monitoring and management		
11.	IPv6 features	• Switch should support for IP V.6 connectivity and routing required for network reachability using different routing protocols such as: ✓ OSPF V.3 ✓ BGP with IP V.6 ✓ IP V.6 Dual Stack etc.		

S.No	Parameter	Minimum Requirement Specification	Compliance (Yes/No)	Deviations (if any)
		• Switch should support multicast routing in IP V.6 network using PIMv2 Sparse Mode • Switch should support monitoring and management using different versions of SNMP in IP V.6 environment such as: ✓ SNMPv1, SNMPv2c, SNMPv3 ✓ SNMP over IP V.6 with encryption support for SNMP Version 3.		

5.2.2.2 Servers (Application / VMS / others as required)

S.No	Parameter	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
1.	Product details-			
2.	Please mention Make Model No. or Part Code			
3.	CPU	Latest Generation x86-64 Bit, Populated with dual Multi-tasking Processors having min. 16 cores of minimum 2.8GHz each. Cache as per offered processor. Processor should be from latest announced series.		
4.	Motherboard	Intel C621 Series Chipset or latest		
5.	Memory	Adequate RAM should be configured Per core.		
6.	Memory Protection	Advanced ECC with multi-bit error protection, online spare/memory mirroring.		
7.	Hard disk drive with carrier	Min. 2 * 1.2 TB hot plug SFF SAS drives or higher		
8.	Storage Controller	12Gb/s SAS Raid Controller with RAID 0/1/1+0 and shall have at-least 1GB flash backed write cache.		

S.No	Parameter	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
9.	Networking features	Converged Network Adaptor with 50Gbps bandwidth (100Gbps bi-directional) which supports carving FlexNICs/vNIC and FlexHBA/vHBA per downlink port (minimum up to 8 sub-ports)		
10.	Blade Server Connectivity to SAN	Should be capable of supporting 32 Gbps Dual port Fiber Channel HBA internal to the Server Blade, having backward compatibility of 16Gb FC.		
11.	Bus Slots	Minimum of 2 Nos of x16 PCIe 3.0 based mezzanine/mLOM slots supporting Converged Ethernet, Ethernet and FC adapters.		
12.	Embedded system management	Blade Solution should support Gigabit out of band management port to monitor the servers for ongoing management, service alerting and reporting		
		Should support UEFI to configure and boot the servers securely		
		System should support RESTful/XML API integration		
		System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support		
13.	OS Support	Windows/ Linux		
14.	Enhanced Supportability	Solution shall provide insights, forecasting and recommendations for quicker problem resolutions including automating case creation or alternate solution on proactive support services with proactive parts dispatch for offered items of the solution.		

S.No	Parameter	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
15.	Embedded Remote Management and firmware security	System remote management should support browser based graphical remote console along with Virtual Power button, remote boot using USB/CD/DVD Drive. It should be capable of offering upgrade of software and patches from a remote client using Media/image/folder; It should support server power capping and historical reporting and should have support for multifactor authentication		
		Server should have local management port and should provide remote management functionality		
		The server should support monitoring and recording/logging of changes in hardware and system configuration. It assists in diagnosing problems and delivering rapid resolution when system failures occur		
		Remote console should provide support for AES and 3DES on browser or latest security features. Should provide remote firmware update functionality		
		Should support managing multiple servers as one via		
		Group Power Control		
		Group Power Capping		
		Group Firmware Update		
		Group Configuration		
		Group Virtual Media		
		Should support RESTful API integration		

S.No	Parameter	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
		System should support embedded remote support to transmit hardware events directly to OEM or an authorized partner for automated phone home support		
16.	Server Management	The Systems Management software should provide Role-based access control		
		Management software should support integration with popular virtualization platform management software like vCentre, and SCVMM		
		Should help provide proactive notification of actual or impending component failure alerts on critical components like CPU, Memory and HDD.		
		Should help to identify out-of-date BIOS, drivers, and Server Management agents and enable the remote update of system software/firmware components		

5.2.2.3 Blade Chassis Specifications

The blade chassis shall have the following minimum technical specifications:

S.No	Specifications	Compliance (Yes / No)	Deviations (if any)
1.	Product details-		
2.	Please mention Make Model No. or Part Code		
3.	Minimum 6U size, rack-mountable, Each Chassis should be populated with max up to 8 servers. The Chassis should be able to support compute sleds of latest generation processors and at least 2 future generations of intel processors		
4.	Dual network connectivity of 10 G speed for each blade server for redundancy shall be provided		

S.No	Specifications	Compliance (Yes / No)	Deviations (if any)
5.	Backplane shall be completely passive device. If it is active, dual backplane shall be provided for redundancy or the chassis should use no mid-plane to connect to Ethernet network in order to support future generation Ethernet technologies without the need to replace chassis.		
6.	Have the capability for installing industry standard flavors of Microsoft Windows, and Enterprise Red Hat Linux Oss as well as virtualization solution such as VMware.		
7.	DVD ROM shall be available in chassis, can be internal or external, which can be shared by all the blades allowing remote installation of software		
8.	Minimum 1 USB Ports at Blade Server or Chassis level		
9.	Two hot-plug/hot-swap, redundant 10 Gbps Ethernet or FCoE module with minimum 16 ports (cumulative), having Layer 2/3 functionality		
10.	Two hot-plugs/hot-swap redundant 16 Gbps Fiber Channel module for connectivity to the external Fiber channel Switch and ultimately to the storage device		
11.	Hot plug/hot-swap redundant power supplies to be provided, along with power cables		
12.	Power supplies shall have N+N. All power supplies modules shall be populated in the chassis.		
13.	Required number of PDUs and power cables, to connect all blades, Chassis to Data Centre power outlet.		
14.	Hot pluggable/hot-swappable redundant cooling unit		
15.	Provision of systems management and deployment tools to aid in blade server configuration and OS deployment		
16.	Blade enclosure shall have provision to connect to display console/central console for local management such as troubleshooting, configuration, system status/health display.		

S.No	Specifications	Compliance (Yes / No)	Deviations (if any)
17.	Single console for all blades in the enclosure, built-in KVM switch or Virtual KVM features over IP		
18.	Dedicated management network port shall have separate path for remote management.		

5.2.2.4 Server Virtualisation and Security

S.No	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
1.	Product details-		
2.	Please mention Make Model No. or Part Code		
3.	Virtualisation software shall provide a Virtualisation layer that sits directly on the bare metal server hardware with no dependence on a general purpose OS for greater reliability		
4.	Virtualisation solution shall have heterogeneous support for guest Operating systems like Windows client, Windows Server, Linux (at least Red Hat, SUSE, Oracle Linux, Ubuntu and CentOS, Solaris x86)		
5.	Virtualisation software should have capability to create Virtual machines with up to 128 virtual processors, 6 TB virtual RAM and 2GB Video memory in virtual machines for all the guest operating system supported by the hypervisor		
6.	Virtualisation software should be able to boot from iSCSI, FCoE, and Fibre Channel SAN		
7.	The solution should provide special integration with Storage API's providing integration with supported third-party data protection, multi-pathing and disk array solutions.		
8.	Solution should provide encrypted live migration capability across different virtualization management instances and versions and also provides seamless migration of individual VMs across different processor generation between different data-centers or from an on-premises data-center to the cloud and back, across clusters and during power cycles.		

S.No	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
9.	Virtualisation software should have the ability to live migrate VM files from one storage array to another without any VM downtime. Support this migration from one storage protocol to another (ex. FC, iSCSI, DAS)		
10.	Virtualisation software should have the provision to provide zero downtime, zero data loss and continuous availability for the applications running in virtual machines in the event of physical host failure, without the cost and complexity of traditional hardware or software clustering solutions.		
11.	The virtualisation software should provide in-built Replication capability which will enable efficient array-agnostic replication of virtual machine data over the LAN or WAN. This Replication should simplify management enabling replication at the virtual machine level and enabling RPOs as low as 5 minutes.		
12.	Virtualisation software should provide capabilities of Hot Add (CPU, Memory & devices) to virtual machines when needed, without disruption or downtime in working for both windows and Linux based VMs		
13.	Virtualisation software should provide secure boot for protection for both the hypervisor and guest operating system by ensuring images have not been tampered with and preventing loading of unauthorized components		
14.	Virtualisation software should provide integration of 3rd party endpoint security to secure the virtual machines with offloaded antivirus, antimalware solutions without the need for agents inside the virtual machines.		
15.	The solution should provide hardware as well as non-hardware accelerated 3D graphics to run Basic 3D applications in virtual machines with suspend and resume capabilities for vGPUs, to improve host lifecycle management and reduce end-user disruption.		
16.	The solution should support enforcing security for virtual machines at the Ethernet layer. Disallow		

S.No	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
	promiscuous mode, sniffing of network traffic, MAC address changes, and forged source MAC transmits.		
17.	Virtualisation software should provide software FCoE adaptor that can work with a network adaptor that support partial FCoE offload capabilities.		
18.	Virtualisation software should allow configuring each virtual machine with one or more virtual NICs. Each of those network interfaces can have its own IP address and even its own MAC address, must support NIC teaming for load sharing and redundancy.		
19.	Virtualisation manager should be highly available with out of box HA without any dependency on external shared storage or load balancer.		
20.	Hypervisor should have capability similar of Virtual Volumes which enables abstraction for external storage (SAN and NAS) devices making them Virtualisation aware.		
21.	Virtualisation software shall continuously monitor utilization across virtual machines and should intelligently allocate available resources among virtual machines		
22.	Virtualisation software should provide enhanced visibility into storage throughput and latency of hosts and virtual machines that can help in troubleshooting storage performance issues.		
23.	Virtualisation software shall be able to dynamically allocate and balance computing capacity across collections of hardware resources aggregated into one unified resource pool with optional control over movement of virtual machines like restricting VMs to run on selected physical hosts.		
24.	It should provide the ability to set constraints that restrict placement of a virtual machine to a subset of hosts in a cluster and to keep virtual machines paired or separated.		
25.	Virtualisation software should provide proactive High availability capability that utilizes server health information and migrates VMs from degraded hosts before problem occurs		

S.No	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
26.	Virtualisation software should provide abilities to offload specific storage operations to compliant storage hardware thereby performing these operations faster and consuming less CPU, memory, and storage fabric bandwidth		
27.	Virtualisation software should provide VM-level encryption protects unauthorized data access both at-rest and in-motion		
28.	The solution should have single reboot to dramatically reduce the upgrade times by skipping a host reset and also help to reduce patching and upgrade times by rebooting the hypervisor without rebooting the physical host, skipping time-consuming hardware initialization		
29.	Hypervisor should have inbuilt Distributed Switch to centralize network provisioning, administration and monitoring using data center-wide network aggregation, should provide Network QoS to define priority access to network resources.		
30.	The solution should provide in-built enhanced host-level packet capture tool which will provide functionalities like SPAN, RSPAN, ERSPAN and will capture traffic at uplink, virtual switch port and virtual NIC level. It should also be able to capture dropped packets and trace the path of a packet with time stamp details		
31.	The solution should provide a “Latency Sensitivity” setting in a VM that can be tuned to help reduce virtual machine latency. When the Latency sensitivity is set to high the hypervisor will try to reduce latency in the virtual machine by reserving memory, dedicating CPU cores and disabling network features that are prone to high latency.		
32.	The solution should provide link aggregation feature in the virtual switch which will provide choice in hashing algorithms on which link aggregation in decided and this should also provide multiple link aggregation groups to be provided in a single host (64 groups per physical host)		

S.No	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
33.	Virtualisation software shall also natively have feature to enable live migration of virtual machines between servers in a cluster, across clusters as well as as long distances from one site to another (up to 100 milliseconds round trip time) with no disruption to users or loss of services, eliminating the need to schedule application downtime or business downtime.		
34.	Virtualisation software should provide abilities to offload specific storage operations to compliant storage hardware thereby performing these operations faster and consuming less CPU, memory, and storage fabric bandwidth		
35.	The solution should be able to create a cluster out of multiple storage datastores and automate load balancing by using storage characteristics to determine the best place for a virtual machine's data to reside, both when it is created and when it is used over time.		
36.	Virtualisation software should provide solution to automate and simplify the task of managing hypervisor installation, configuration and upgrade on multiple physical servers.		
37.	The solution should provide an option to easily deploy and manage big data solutions like Hadoop on the virtualization platform		
38.	OEM should provide direct support 24x7x365 with unlimited incident support (Telephonic/ Web/ Email) and 30 mins or less response time including the unlimited upgrades and updates.		

5.2.2.5 Storage

S.No	Parameter	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
1.	Product details-			
2.	Please mention Make Model			

S.No	Parameter	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
	No. or Part Code			
3.	Controllers and Architecture	• Storage Should be Fully Symmetric and fully distributed clustered Architecture written for Scale-Out Storage operations • Scale out storage should be configured with minimum 8 controllers of the same type • Over all storage cluster should be upgradable to min 2 x numbers of Storage controllers / Storage nodes, without any disruptions / downtime to production workflow for performance, capacity enhancement, software / firmware upgrades. • The storage cluster should support linear scalability of performance and capacity. • All storage nodes / controllers must be active for all Storage shares, contributing in performance and capacity of the system Storage Controllers should have Intel processors.		
4.	Onboard Memory	The scale out storage must be configured with minimum 256GB globally coherent, DRAM based cache/memory.		
5.	Operating System Network Ports	Scale-Out Storage operating system should have Fully journaled, fully distributed, specialized Operating System by OEM or Software Defined Storage solution dedicated for serving data efficiently and customised for True Scale-Out Storage. Entire data should automatically balance across proposed controllers/nodes within		

S.No	Parameter	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
		each tier without any administrative intervention		
6.		The scale out storage should be offered with minimum 16 x 10Gbps SFP+ ports, and should be scalable to 2x the number of offered ports		
7.	Disk support	Storage cluster should have capability to support different kinds of disks tiers likes SSD, SAS, SATA/NL-SAS drives within single filesystem.		
8.	Redundancy with No Single Point of Failure (SPOF)	• The Scale-Out Storage System should be able to protect the data against simultaneous three disks failure without any data loss and data unavailability • The Scale-Out Storage should have self-optimizing architecture so the system does not require defragmentation, nor consistency check like “fsck” in the event of an ungraceful shutdown of the cluster to ensure higher uptime. • All data should be striped across all storage controllers in the proposed storage system, so that performance of all controllers can be utilized for all read and write operations. • The backend internal connectivity between storage controllers / storage nodes should be using high performance Infiniband or 10 /40 GigE network with no single point of failure. • The backend internal connectivity configured between Storage controllers / Storage nodes themselves and between storage controllers / nodes and disk		

S.No	Parameter	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
		controllers, if configured, should be redundant and there should be "No Single Point of Failure". • Redundant and Hot replaceable modules: Controllers, Hard Disk Drive and power supplies (230V AC, 50 Hz.) • The Complete multi-controller Storage System Solution should be fully redundant, configured in High Availability mode and should NOT have any Single Point of Failure (SPOF).		
9.	Total Storage Capacity	• Scale out storage should be configured with 3 PB usable capacity with triple disk failure protection, using equal to or less than 12TB NL-SAS/ SATA HDD • The storage should be scalable upto 5x the capacity as a single filesystem and a single global namespace.		
10.	Capacity Performanc e Expansion	• There should not be any downtime or migration activity required in the event it is needed to add additional capacity or additional performance to the storage system. • Storage solution should enable linear scalability of performance and capacity (ie X TB increase in capacity should lead to Y GBps increase in performance) • In the event of addition of storage controller/storage node to storage solution, existing data should be rebalanced across all nodes of storage controllers / storage nodes automatically. This autobalance should be done with low priority		

S.No	Parameter	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
		avoiding any impact to client performance. • Addition of storage controller/ storage nodes should not require any complicated configuration of new controller/node. It should be done easily, seamlessly and without having any impact to user access. • The storage file system shall not require metadata performance tuning. • The system must be able to support policy based tiering to different storage tiers with Storage sub-system.		
11.	Protection Levels	• Storage solution should support required protection level which can protect data against simultaneous 3 disks failures • Should have capability to change the protection level on-the-fly. • Should be able to assign protection level on cluster, directory or file level.		
12.	Protocol Support	• Network protocol Support: Must provide access for a variety of operating systems using native OS protocols. Licenses if any, required for such protocol access to be provided. • Should support user security mechanisms like AD, LDAP and NIS. • Storage solution must support multiple protocols at the same time on the same piece of hardware (No separate, individually managed servers shall be required).		

S.No	Parameter	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
		• License should be provided for all the protocol and it should be perpetual.		
13.	Client Load Balancing	Storage System should have capability to load balance client connectivity across these multiple controllers so that all clients gets distributed across all existing controllers/nodes to avoid any performance hotspot.		
14.	Heterogeneous support for end user systems	Operating system support RedHat Linux, Suse Linux, Windows Servers 2003/2008 or later , Windows XP/7 or later. Unix Based operating systems like SUN solaris, HP Unix, IBM AIX		
15.	Management Interface software	Support the management, administration and configuration of the whole storage platform through a single management interface along with CLI		
16.	Security	• The system must support encrypting data at rest. • The system must be able to support Write Once Read Many (WORM) compliant to SEC17a-4. • The system must support Role Base Access Control with Integration with Active Directory and LDAP • The system must be able to support System Auditing for system as well as supported protocols. • The system must support multiple DNS. • The system must be able to support Anti-Virus Scanning through Internet Content		

S.No	Parameter	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
		Adaptation (ICAP) protocol or equivalent capability to provide virus scanning functionality. • The system should have file system integrity and data integrity checks built in to prevent data loss due to bit rot and other soft errors		

5.2.2.6 Server/Networking Rack Specifications

S.No	Parameter	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
1.	Product details-			
2.	Please mention Make Model No. or Part Code			
3.	Type	• 19” 42U racks mounted on the floor • Floor Standing Server Rack - 42U with Heavy Duty Extruded Aluminium Frame for rigidity. Top cover with FHU provision. Top & Bottom cover with cable entry gland plates. Heavy Duty Top and Bottom frame of MS. Two pairs of 19" mounting angles with 'U' marking. Depth support channels - 3 pairs with an overall weight carrying Capacity of 500Kgs. • All racks should have mounting hardware 2 Packs, Blanking Panel. • Stationery Shelf (2 sets per Rack)		

S.No	Parameter	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
		• All racks must be lockable on all sides with unique key for each rack • Racks should have Rear Cable Management channels, Roof and base cable access		
4.	Wire managers	Two vertical and four horizontal		
5.	Power Distribution Units	• 2 per rack • Power Distribution Unit - Vertically Mounted, 32AMPs with 25 Power Outputs. (20 Power outs of IEC 320 C13 Sockets & 5 Power outs of 5/15 Amp Sockets), Electronically controlled circuits for Surge & Spike protection, LED readout for the total current being drawn from the channel, 32AMPS MCB, 5 KV AC isolated input to Ground & Output to Ground		
6.	Doors	• The racks must have steel (solid / grill / mesh) front / rear doors and side panels. Racks should NOT have glass doors / panels. • Front and Back doors should be perforated with at least 63% or higher perforations. • Both the front and rear doors should be designed with quick release hinges allowing for quick and easy detachment without the use of tools.		
7.	Fans and Fan Tray	• Fan 90CFM 230V AC, 4" dia (4 Nos. per Rack) • Fan Housing Unit 4 Fan Position (Top Mounted) (1 no. per Rack) - Monitored - Thermostat based -		

S.No	Parameter	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
		The Fans should switch on based on the Temperature within the rack. The temperature setting should be factory settable. This unit should also include - humidity & temperature sensor		
8.	Metal	Aluminium extruded profile		
9.	Side Panel	Detachable side panels (set of 2 per Rack)		

5.2.2.7 Core Router

S.No	Item	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
1.	Product details-			
2.	Please mention Make Model No. or Part Code			
3.	Multi-Services	Should deliver multiple IP services over a flexible combination of interfaces		
4.	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.		
5.	Speed	As per requirement, to cater to entire bandwidth requirement of the project.		
6.	Interface modules	Must support up to 10G interfaces. Must have capability to interface with variety interfaces.		

S.No	Item	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
7.	Protocol Support	• Must have support for TCP/IP, PPP, Frame relay or any equivalent protocols • Must support VPN • Must have support for integration of data and voice services • Routing protocols of RIP, OSPF, and BGP. • Support IPV4 & IPV6 • Should support Multicast-only fast reroute (MoFRR) or other equivalent ways to minimize packet loss in PIM and multipoint LDP domains with dual paths available.		
8.	Manageability	Must be SNMP manageable		
9.	Scalable	• The router should be scalable. For each slot multiple modules should be available. • The chassis offered must have free slots to meet the scalability requirement of expansion of the project in the future. • Should support minimum 4 million ipv4 and 4 million ipv6 routes • should support at least 4000 VRF/ MPLS VPN		
10.	Traffic control	Traffic Control and Filtering features for flexible user control policies		
11.	Bandwidth	Bandwidth on demand for cost effective connection performance enhancement		

S.No	Item	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
12.	Remote Access	Remote access features		
13.	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		
14.	Security features	• MD5 encryption for routing protocol • NAT • RADIUS Authentication • Management Access policy • IPSec / Encryption • L2TP		
15.	QOS Features	• RSVP • Priority Queuing • Policy based routing • Traffic shaping • Time-based QoS Policy • Bandwidth Reservation / Committed Information Rate		

5.2.2.8 Internet Router

S.No	Item	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
1.	Product details-			
2.	Please mention Make Model No. or Part Code			

S.No	Item	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
3.	Multi-Services	Should deliver multiple IP services over a flexible combination of interfaces		
4.	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.		
5.	Interface modules	Must support up to 10G interfaces as per the design. Must have capability to connect with variety of interfaces.		
6.	Protocol Support	• Must have support for TCP/IP, PPP, Frame relay or any equivalent protocols • Must support VPN • Must have support for integration of data and voice services • Routing protocols of RIP, OSPF, and BGP. • Support IPV4, IPV6 • Support load balancing		
7.	Manageability	Must be SNMP manageable		
8.	Traffic control	• Traffic Control and Filtering features for flexible user control policies • Should support minimum 1 million IPv4 and 1 million IPv6 routes		
9.	Bandwidth	Bandwidth on demand for cost effective connection performance enhancement		
10.	Remote Access	Remote access features		
11.	Redundancy	• Redundancy in terms of Power supply(s). Power supply should be able to support fully loaded chassis		

S.No	Item	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
		• All interface modules, power supplies should be hot-swappable		
12.	Security features	• MD5 encryption for routing protocol • NAT • RADIUS/AAA Authentication • Management Access policy • IPSec / Encryption • L2TP		
13.	QOS Features	• RSVP • Priority Queuing • Policy based routing • Traffic shaping • Time-based QoS Policy • Bandwidth Reservation / Committed Information Rate		

5.2.2.9 Firewall

S.No	Item	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
1.	Product details-			
2.	Please mention Make Model No. or Part Code			
3.	Physical attributes	• Should be mountable on 19" Rack • Modular Chassis • Internal redundant power supply		
4.	Interfaces	• Minimum 6 x 10 Gbps interfaces • Console Port 1 number		

S.No	Item	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
5.	Performance and Availability	• Next Generation Firewall Throughput: minimum 20 Gbps for internet and 20 Gbps for intranet firewall" • Concurrent connections: up to 100,000 • Simultaneous VPN tunnels: 2000		
6.	Routing Protocols	• Static Routes • RIPv1, RIPv2 • OSPF		
7.	Protocols	• TCP/IP, PPTP • RTP, L2TP • IPSec, GRE, DES/3DES/AES • PPPoE, EAP-TLS, RTP • FTP, HTTP, HTTPS • SNMP, SMTP • DHCP, DNS • Support for Ipv6		
8.	Other support	1Q, NAT, PAT, IP Multicast support, Remote Access VPN, Time based Access control lists, URL Filtering, support VLAN, Radius/ TACACS		
9.	QoS	QoS features like traffic prioritization, differentiated services/Preservation, and committed access rate. Should support for QoS features for defining the QoS policies."		
10.	Management	• Console, Telnet, SSHv2, Browser based configuration • SNMPv1, SNMPv2 • Should Support SDK for IOT		

5.2.2.10 Intrusion Prevention System

S.No	Item	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
1.	Product details-			

S.No	Item	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
2.	Please mention Make Model No. or Part Code			
3.	Performance	Should have an aggregate throughput of no less than 20Gbps Total Simultaneous Sessions – 20 Million		
4.	Features	• IPS should have Dual Power Supply • IPS system should be transparent to network, not default gateway to Network • IPS system should have Separate interface for secure management • IPS system should be able to protect Multi Segment in the network, should be able to protect 4 segments.		
5.	Real Time Protection	• Web Protection • Mail Server Protection • Cross Site Scripting • SNMP Vulnerability • Worms and Viruses • Brute Force Protection • SQL Injection • Backdoor and Trojans		
6.	Stateful Operation	• TCP Reassembly • IP Defragmentation • Bi-directional Inspection • Forensic Data Collection • Access Lists		
7.	Signature Detection	Should have provision for Real Time Updates of Signatures, IPS Should support Automatic signature synchronization from		

S.No	Item	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
		database server on web Device should have capability to define User Defined Signatures		
8.	Block attacks in real time	• Drop Attack Packets • Reset Connections • Packet Logging • Action per Attack		
9.	Alerts	• Alerting SNMP • Log File • Syslog • E-mail		
10.	Management	• SNMP V1, 2C, 3 • HTTP, HTTPS • SSH/ Telnet, Console		
11.	Security Maintenance	• IPS Should support 24/7 Security Update Service • IPS Should support Real Time signature update • IPS Should support Provision to add static own attack signatures • System should show real-time and History reports of Bandwidth usage per policy • IPS should have provision for external bypass Switch		

5.2.2.11 SIEM

S.No	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
1.	Product details-		
2.	Please mention Make Model No. or Part Code		
3.	Next generation platform should encompass log, packet and end point data with added context and threat Intelligence. Should provide complete network		

S.No	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
	visibility through deep packet inspection high speed packet capture and analysis.		
4.	The solution should be a physical appliance form factor with following components:		
5.	a. Management & Reporting b. Normalization and Indexing c. Correlation Engine d. Data Management		
6.	There should be no limitation on number of devices to be supported. Any addition in no. of devices should have no cost impact on department.		
7.	SIEM & Log Monitoring solution should be from a different OEM than the Prevention Security solutions like F/W, IPS, HIPS, AV, DLP, and Encryption.		
8.	The solution should provide an integrated SOC dashboard and Incident analysis system that could provide a single view into all the analysis performed across all the different data sources including but not limited to logs and packets. The Tool should have role based access control mechanism and handle the entire security incident lifecycle.		
9.	Real time contextual information should be used at collection/normalization layer and also be available at correlation layer where any events are matched during correlation rule processing. In addition solution must provide contextual Hub at investigation layer for all relevant contextual awareness data regarding alerts/incidents available for any information asset like IP /Device etc		
10.	All logs that are collected should be studied for completeness of information required, reporting, analysis and requisite data enhancement, normalization should be performed to meet the reporting and analysis needs.		
11.	A single log appliance should support minimum 30,000 EPS and packet appliance should support up		

S.No	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
	to 1GBPS line rate with multiple ingress interfaces for capturing from multiple network interfaces.		
12.	Correlation Engine appliance should be consolidated in a purpose build appliance and should handle 100,000 EPS.		
13.	The solution should be storing both raw logs as well as normalized logs. The same should be made available for analysis and reporting. Solution should be sized to provide online storage for 1 year at central site.		
14.	The solution should incorporate and correlate information that enables the Information Security Team to quickly prioritize it's response to help ensure effective incident handling.		
15.	The monitoring should be cross device and cross vendor and be both out of the box and scalable to cover additional devices and applications as required		
16.	Appliance should have minimum 128 GB RAM to provide optimal performance and should provide at least 4 network interfaces onboard.		
17.	Should be managed and monitored from SIEM unified console for Correlation, Alerting and Administration		
18.	Should store RAW packet DATA for 7 days and normalized packet data for 30 days for forensics.		
19.	Should be able to provide complete packet-by-packet details pertaining to one or more session of interest including Session replay, page reconstruction, image views, artefact & raw packet and object extractions.		
20.	Should be able to filter the captured packets based on layer-2 to layer-7 header information.		
21.	Should provide comprehensive deep packet inspection (DPI) to classify protocols & application.		

S.No	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
22.	The proposed solution must be able to provide the complete platform to perform Network forensics solution		
23.	The solution must be able to detect malicious payload in network traffic · Detect and reconstruct files back to its original type · Detect hidden or embedded files · Detect and flag out renamed files		
24.	The solution must have the ability to capture network traffic and import PCAP files using the same infrastructure.		

5.2.2.12 Data Centre Switch

#	Parameter	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
1.	Product details-			
2.	Please mention Make Model No. or Part Code			
3.	Hardware features	32x 100GbE QSFP28 Ports expandable to Support 10G/25G/40G/50G/100G Ports, Enterprise class advance Layer-3 image, standard rack mountable switch.		
4.		Proposed network device must be 19'' rack mountable		
5.		Network Infrastructure equipment must use 240V AC power.		
6.		The switch should support Dual Power supply and Fan supporting variable speeds to control the switch temperature.		
7.		The switch should support minimum 64GB SSD Flash		
8.		The switch should support minimum 16GB RAM/Processing memory		

#	Parameter	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
9.		The switch should support minimum 32MB Buffer memory		
10.		The Switch should be populated with required no of ports		
11.		The switch should support minimum 6.4 Tbps of Switching Performance with 2400 Mpps of Forwarding rate and less than 900 nanosecond latency.		
12.		Switch must support SDN Technologies like VXLAN, BGP-EVPN Natively without any change of Hardware & Software.		
13.	Layer 2 and Layer 3 Features	All Optic and modules offered should be hot swappable.		
14.		Must support port channeling or equivalent across multiple switches using the IEEE standard LAG features.		
15.		Physical standards for Network Device Should support Ethernet (IEEE 802.3, 10BASE-T), Fast Ethernet (IEEE 802.3u, 100BASE-TX), Gigabit Ethernet (IEEE 802.3z, 802.3ab), Ten Gigabit Ethernet (IEEE 802.3ae)		
16.		Software based standards for Network Device Must support IEEE 802.1d - Spanning-Tree Protocol, IEEE 802.1w - Rapid Spanning Tree, IEEE 802.1s - Multiple Spanning Tree Protocol, IEEE 802.1q - VLAN encapsulation, IEEE 802.3ad - Link Aggregation Control Protocol (LACP), IEEE 802.1ab - Link Layer Discovery Protocol (LLDP), IEEE 802.3x Flow Control		
17.		Must support auto-sensing and auto-negotiation (Link Speed/Duplex)		
18.		Routing protocol support; Static IP routing, OSPF, BGPv4, BGP Route ,		

#	Parameter	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
		appropriate L2/L3 advance Licenses to be included from day one		
19.		The switch should support IPv4 and IPv6 features and function in hardware with minimum Layer-3 routing capacity of 32K table for IPv4 and 8K table for IPv6 in hardware. Any license or hardware required to enable all feature to be incorporated in the offer.		
20.		The network infrastructure must allow for multiple equal metric/cost routes to be utilized at the same time		
21.		The switch should support minimum 160K MAC address and 4K Vlan ID and 802.1Q vlans		
22.		Switch must have the ability to offer complete hitless software upgrades with zero interruption to services or data forwarding. Functionality offering the same to be offered to address Switch firmware upgrades major/minor OS releases and patch upgrades.		
23.		Should support 802.1, Q-in-Q Vlan, Layer-2 Vlans, Layer-3 Vlans, Private Vlan, GARP VLAN Registration Protocol, Native Vlan, Voice Vlan etc.		
24.		IEEE 802.3ad Link Aggregation or equivalent capabilities		
25.		The switch hardware shall be designed to run both IPv4 & IPv6 simultaneously (Dual Stack).		
26.		IP Version 6 (IPv6) must be supported in hardware		
27.		Must support Static IPv6 routing, OSPFv3,		

#	Parameter	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
28.		Should support ECMP for all routing protocols		
29.		Should support both IPv4 and IPv6 routing concurrently. There should be the ability to tunnel IPv6 within IPv4.		
30.		Supported IPv6 features should include: DHCPv6, ICMPv6, IPv6 Multicast support, IPv6 PIMv2 Sparse Mode,		
31.		Device must support multicast in hardware supporting feature PIM-SM, MSDP, SSM, MLD, IGMP V1/V2/V3.		
32.	Security features	Must support multiple privilege levels for remote access (e.g. console or telnet access)		
33.		Must support Remote Authentication Dial-In User Service (RADIUS) and/or Terminal Access Controller Access Control System Plus (TACACS+)		
34.		Switch should support ACL Standard, Extended ACL and Time based ACL.		
35.		The ACL should be configurable using combination of IP protocol number, Source and Destination address, Source and destination TCP/UDP port number,		
36.		ACL should be able to configure and Manage Access control, Define Filters and re-sequence data flow and patterns, Traffic management, Route Distribution, Qos, Cos, Policy Maps, Policy based routing, Logging and flow based monitoring for IPv4 and IPv6 packets.		
37.	QoS features	Must support IEEE 802.1p class-of-service (CoS) prioritization, with 8 queues per port.		

#	Parameter	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
38.		Must support rate limiting (to configurable levels) based on source/destination IP/MAC, L4 TCP/UDP		
39.		Must have the ability to complete traffic shaping to configurable levels based on source/destination IP/MAC and Layer 4 (TCP/UDP) protocols		
40.		There should not be any impact to performance or data forwarding when QoS features		
41.		Must support a "Priority" queuing mechanism to guarantee delivery of highest-priority (broadcast critical/delay-sensitive traffic) packets ahead of all other traffic		
42.		Should support Network monitoring features like NetFlow, sFlow, SPAN, RSPAN or similar technologies		
43.	High Availability Features	The switch should support STP/RSTP/MSTP/PVST+, VRRP/HSRP, Clustering multiple switches using OEM or standard based technology.		
44.		The switch should support Ring based technologies for faster recovery / convergence of network setup.		
45.	Management features	Must support SNMP V1,V2, V3		
46.		Must support SNMP traps (alarms / alerts) for a minimum of four destinations		
47.		Network switch should support Remote Monitoring on every port covering the following four groups (Statistics, Alarm, Event, History).		
48.		Should support flow based traffic analysis features and the ability to export of network IP flow information.		

#	Parameter	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
49.		Must support Network Timing Protocol and support SDN using Openflow or similar technologies.		
50.		The switch should support dedicated Out of band management port - 10/100/1000baseT, USB port to support additional flash drive expansion, copy/backup/restore switch firmware and configuration, and serial console port via an RJ45 and or USB-B port or serial interface.		

5.2.2.13 Server Load balancer and Web Application Firewall

- Server Load Balancing Mechanism
  - Cyclic, Hash, Least numbers of users
  - Weighted Cyclic, Least Amount of Traffic
  - NT Algorithm / Private Algorithm / Customizable Algorithm / Response Time
- Redundancy Features
  - Supports Active-Active and Active-Standby Redundancy
  - Segmentation / Virtualization support
- Routing Features
  - Routing protocols RIPv1/RIPv2/OSPF
  - Static Routing policy support
- Server Load Balancing Features
  - Server and Client process coexist
  - UDP Stateless
  - Service Failover
  - Backup/Overflow
  - Direct Server Return
  - Client NAT
  - Port Multiplexing-Virtual Ports to Real Ports Mapping
  - DNS Load Balancing
- Load Balancing Applications
  - Application/ Web Server, MMS, Streaming Media
  - DNS, FTP- ACTIVE & PASSIVE, REXEC, RSH,
  - LDAP, RADIUS
- Content Intelligent SLB
- HTTP Header Super Farm
- URL-Based SLB
- Browser Type Farm

- Support for Global Server Load Balancing
- Global Server Load Balancing Algorithms
- HTTP Redirection,
- HTTP
- DNS Redirection/ RTSP Redirection
- DNS Fallback Redirection, HTTP Layer 7 Redirection

- SLB should support below Management options
  - Secure Web Based Management
  - SSH
  - SNMP 2, 3 Based GUI
  - Command Line

S.No	Features	Compliance (Yes / No)	Deviations (if any)
1	**Platform**		
1.0	Solution can be proposed with single / multiple appliances		
1.1	Must be an appliance with hardened OS		
1.2	Platform should be a full proxy architecture and must perform reverse proxy for inside applications		
1.3	Should have administration partitioning and segmentation / virtualization, whereby the physical device can span across multiple network segments without any inter device routing. The segmentation / virtualization feature should support the use of the same internal IP across the multiple network segments.		
1.4	Should have a dedicated out-of-band Ethernet management port		
1.5	Should have full support IPv6. It should support all IPv6 scenarios: a. IPv4 on the inside and IPv6 on the outside b. IPv6 on the inside and IPv4 on the outside c. IPv6 on the inside and outside		
1.6	Should support VLAN, LACP & Trunking		
1.7	Should have a chassis height of 1U / 2U (1 / 2 Rack Unit)		
1.8	Application should support throughput of minimum 60 Gbps for Server Load balancing		
1.9	The appliance must provide appliances with minimum 8 X 10 Gbps Short Range Fiber Ports Interfaces		

S.No	Features	Compliance (Yes / No)	Deviations (if any)
1.10	The solution must support to Server Load Balancing along with WAF together from same appliance		
1.11	Should have a SSD with minimal capacity of 128 GB or above		
1.12	"OS should be certified by ICSA"		
1.13	Should have SSL acceleration and Compression		
1.14	Should have dual power supply		
2	**Performance**		
2.1	Platform should have "L7" throughput of minimum 20 Gbps		
2.2	Should have capability to support up to 20 Million Concurrent Connection		
2.4	Should have 20000 TPS, where TPS = Only one HTTP Transaction over each new SSL handshakes per second, without session reuse and using a 2048 bit key SSL Certificate.		
2.5	Should have SSL Throughput of minimum 40 Gbps		
2.6	Should have compression throughput of minimum 10 Gbps		
2.8	Should support configurable TCP Optimization features for Server- side		
3	**Server Load Balancing**		
3.1	Should have application delivery features such as layer 7 load balancing, layer 7 content switch, caching, hardware based SSL offload and hardware based server side compression		
3.2	Should have capability to monitor the applications using intelligent application level monitors which can be system defined, internal or external executable scripts		
3.3	Should be able to tune monitoring frequency and time automatically when server is available for long time, this is to avoid monitoring load on server		
3.4	Should have 2048 and 4096 bit key for SSL certificate support		
3.5	Should have capability to support Elliptic Curve Cryptography, Rivest-Shamir-Adleman and Elliptic		

S.No	Features	Compliance (Yes / No)	Deviations (if any)
	Curve Cryptography+Rivest-Shamir-Adleman (Hybrid) Certificates for SSL offload		
3.6	Should provide static and dynamic load balancing algorithms such as round robin, weighted round robin, fastest, predictive and observed		
3.7	Should be application aware and provide Full Proxy for protocols such as HTTP, HTTPS, FTP, SIP, DNS, Diameter, RADIUS etc.		
3.8	Should support inspection of SSL traffic for reverse proxy and forward proxy deployment. Should also support ICAP interface for integration with external security systems.		
3.9	Should support IoT Device authentication over SSL and MQTT Message parsing and MQTT load balancing.		
3.10	Should have HTTP 2.0 gateway in environment where the client to load balancer traffic is HTTP 2.0 and from load balancer to server is normal HTTP 1.1		
4	**Web Application Firewall**		
4.1	Should be an ICSA WAF 2.1 certified		
4.2	WAF should have positive and negative security model		
4.3	The proposed WAF should be equipped with a set of pre-built application specific security policies that provide out-of-the-box protection for common applications		
4.4	The proposed WAF should have a mechanism to deploy preconfigured policy that can immediately secures the web application. These validated policies should require zero configuration time and serve as a starting point for more advanced policy creation, based on heuristic learning and specific application security needs for the application.		
4.5	The proposed WAF should have a dynamic policy builder engine, which is responsible for automatic self-learning and creation of security policies. It should automatically build and manage security policies around newly discovered vulnerabilities without manual intervention.		

S.No	Features	Compliance (Yes / No)	Deviations (if any)
4.6	The proposed WAF should at the minimum query the signature service on a daily basis and automatically downloads and apply new signatures, and all signatures must be visible to administrator for review.		
4.7	The proposed WAF should defend against the OWASP Top 10 Vulnerabilities		
4.8	WAF should have capability to automatically analyze attacks like Brute Force and avail CAPTCHA on the fly to users to identify bot / scripted attacks		
4.9	WAF should have Proactive BOT defense and must have BOT signatures		
4.10	WAF should have different policies for different web applications		
4.11	Should be a scalable platform and support minimum 4 Gbps of WAF throughput capacity with all Signatures enabled and scanning HTTP Request and Response together		
4.12	a. Should protects against various application attacks, including: a. Layer 7 DoS and DDoS b. Brute force c. Cross-site scripting (XSS) d. Cross Site Request Forgery e. SQL injection f. Form Field and Parameter Tampering and HPP tampering g. Sensitive information leakage h. Session high jacking i. Buffer overflows j. Cookie manipulation/poisoning k. Various encoding attacks l. Broken access control m. Forceful browsing n. Hidden fields manipulation o. Request smuggling p. XML bombs/DoS		
4.13	Should have HTTP 1.0, HTTP 1.1, HTTPS protection as part of WAF		

S.No	Features	Compliance (Yes / No)	Deviations (if any)
4.14	Should have automatic detection of heavy URLS and protect against BOT attacks to those URLS		
4.15	Should have HTTP based DDOS detection and should start automatic capturing traffic in batch mode for forensic purpose		
4.16	Should support signature staging after update – so that newly added signature to a policy in block mode does not break the application. If needed this can be disabled.		
5	**Device Administration**		
5.1	Should provide HTTPS interface management for administering the device		
5.2	Should provide SSH interface management for administering the device		
5.3	Should provide troubleshooting and traffic analysis tool like TCP dump		
5.4	Should support role based admin access with roles like no access, Guest, Operator, Application editor, Resource Administrator and Administrator		
5.5	a. Should have a live dashboard with graphical reporting a. CPU Usage b. Memory Usage c. Connections Statistics d. Throughput Statistics e. Virtual Server Status f. Pool Status g. Node Status		
5.6	Should provide historical graphical reporting for the last 30 days on appliance itself		
5.7	Should have a built-in tool to take a snapshot of the unit for troubleshooting and analysis purpose		
5.8	Vendor should provide a service to upload this snapshot and get feedback on the health of the unit & missing Hotfixes and best practices		
6	**High Availability**		
6.1	Should have active-active and active-backup high availability with TCP/IP connection mirroring as well		

S.No	Features	Compliance (Yes / No)	Deviations (if any)
	as SSL ID mirroring. Hence old connection should not fail or forced for SSL renegotiation.		
6.2	Should have transparent failover between 2 devices, the failover should be transparent to other networking devices		
6.3	Should support network based failover for session mirroring, connection mirroring and heartbeat check		
6.4	Should support config autosync, manual sync to and from active and backup unit		
6.5	Should support the feature to force the active device to standby and back to active state; or force a device to offline mode		
6.6	Should support MAC masquerading		
6.7	Should support N+1 High Availability Clustering for future scalability with the ability to add heterogeneous devices from the same OEM into the cluster		
7	**Reporting Features**		
7.1	Should have a Reporting Engine built-in		
7.2	Should support High Speed Logging to a syslog server		
7.3	Support for customized logging through scripts to log any parameter from L3 to L7, like Geolocation, IP addresses, client browser, client OS, etc.		
7.4	Should support integration with SIEM tools like Arcsight and Splunk		
7.5	Should have a log publisher to publish logs to multiple log destinations for the same application (or virtual server)		
7.6	Should have a filtering capability before publishing to a log destination		
8	**Others**		
8.2	Vendor should provide regular updates to geolocation database from their public downloads website		

5.2.2.14 Link Load Balancer and DDoS (Single Appliance or Separate Appliances)

S.No	Technical Specifications	Compliance (Yes / No)	Deviations (if any)
	General Requirements		

S.No	Technical Specifications	Compliance (Yes / No)	Deviations (if any)
1.	Anti-DDos solution should be a dedicated appliance based solution for DDos Detection and Mitigation.		
2.	The solution must support stateful and stateless based protection.		
3.	The Appliance should support throughput of 20Gbps for Link Load Balancing		
4.	The appliance must provide appliances with minimum 8 X 10 Gbps Short Range Fiber Ports Interfaces		
5.	The appliance should have out of band management port of 1 Gigabit Ethernet Interface.		
6.	The solution must support to Link Load Balancing along with DDoS mitigation together from same appliance		
7.	The Solution must support the ability to enhance overall protection by integrating local protection with automated cloud-based DDoS services as and when required.		
8.	The system should support the capability to perform SSL Version 3.0 /TLS (Version 1.2 & above) inspection on different module/ hardware it should not impact the core performance of DDOS device.		
9.	The appliances must have dual power supplies for redundancy.		
10.	The appliance must have a capacity to maintain logs of 30 days		
11.	The Appliance should support 20 Million PPS DDoS mitigation anytime.		
12.	The solution should support a minimum of 20 Gbps (hardware assisted) SSL decryption capacity "		
	Functional Requirement		
1.	DDos Protection based on IP reputation feed.		
2.	The solution should have GeoIP Tracking		
3.	The solution must be able to protect following UDP, TCP, SIP, DNS, HTTP, SSL, MQTT and other network attack targets while delivering uninterrupted service for legitimate connections:		

S.No	Technical Specifications	Compliance (Yes / No)	Deviations (if any)
4.	The solution must be able to detect sources that send excessive amounts of traffic according to configurable thresholds, and then must provide the flexibility to place those sources on the temporary blocked hosts list (rate-base blocking)		
5.	The solution should support auto tuning of threshold for all DDoS vectors based on system throughput, capacity and traffic load		
6.	The system must support the ability to blacklist a host, country, domain, URL		
7.	Solution should be capable of monitoring of Internet bandwidth and signaling to cloud based on defined thresholds		
	Layer 3 - 4 DDoS Functionality		
1	The solution must be able to protect following IP based - IP Fragment, Tear Drop		
2	The solution must be able to protect following TCP based - SYN, SYN-ACK, ACK and PUSH-ACK Flood, RST or FIN Flood, Fragmented ACK, Redirect Traffic Attack and Invalid TCP flags		
3	The solution must be able to protect following UDP based - UDP Flood, and UDP Fragmentation, Short UDP packet		
4	The solution must be able to, but not limited to, protect from following kinds of flood		
4.1	ARP Flood		
	ICMP v4 Flood		
	ICMP v6 Flood		
	IGMP Flood		
	IGMP Fragment Flood		
	TCP RST Flood		
	TCP SYN ACK Flood		
	TCP SYN Oversize		
	UDP Flood		
5	The solution must at least, but not limited to detect following bad headers in IPv4 packet		
5.1	Bad IP TTL Value		

S.No	Technical Specifications	Compliance (Yes / No)	Deviations (if any)
	Bad IP Version		
	Header Length > L2 Length		
	IP Error checksum		
	IP Length > L2 Length		
	IP Option Frames		
	IP Option illegal length		
	Unknown Option Type		
6	The solution must at least, but not limited to detect following bad headers in IPv6 packet		
6.1	IPv6 extended headers wrong order		
	Bad IPv6 Hop Count		
	Bad IPv6 Version		
	IPv6 duplicate extension headers		
	Bad IPv6 Address		
	IPv6 Extended Header Frames		
	Payload Length < L2 Length		
	Too Many Extension Headers		
7	The solution must be able to protect following Bad Header - DNS, ICMP, IGMP IPv4, IPv6, L2, TCP and UDP		
8	The solution must support rate- limit protections for UDP flood detection, fragment flood detection, private address blocking and multicast blocking		
	Layer 7 DDoS Functionality		
1.	The solution must be able to protect following HTTP based - HTTP Fragmentation, L7 DoS (Slowloris, Slow HTTP POST) and Excessive GET/POST		
2.	The solution must be able to protect following other Application based attacks - SIP flood or SMTP based attacks or NTP amplification/reflection or XML DoS etc.		
3.	The solution should have DDos Protection from active botnets		
4.	The solution should identify web crawlers and white list crawlers like search engine		

S.No	Technical Specifications	Compliance (Yes / No)	Deviations (if any)
5.	The system must support the blocking of malformed DNS requests on port 53 that do not conform to RFC standards		
6.	The system must be able to limit the number DNS Queries per second for following type of queries		
6.1	A Query		
	AAAA Query		
	NS Query		
	MX Query		
	PTR Query		
	SOA Query		
	SRV Query		
	TXT Query		
	CNAME Query		
	AXFR Query		
7.	The system must be able to limit SIP Traffic based on following categories		
7.1	SIP ACK Method		
	SIP BYE Method		
	SIP Cancel Method		
	SIP INVITE Method		
	SIP MESSAGE Method		
	SIP NOTIFY Method		
	SIP OPTIONS Method		
	SIP PRACK Method		
	SIP PUBLISH Method		
	SIP REGISTER Method		
8.	The system must be able to detect and drop malformed HTTP packets that does not conform to RFC standards for request headers, and then facility to blacklist the source hosts		
9.	The system must be able to block hosts exceeding a configurable threshold for total number of HTTP operations per second, per destination server		

S.No	Technical Specifications	Compliance (Yes / No)	Deviations (if any)
10.	The system must provide the ability to block bot-originated traffic according to system- supplied signatures		
11.	The system must be able to regularly activate new defense techniques from regularly updated attack signatures that are maintained by the vendor's research team via 24x7 monitoring of the Internet to identify the most significant and recent botnets and attack strategies		
12.	The system must enforce correct protocol usage and block malformed SSL/TLS requests.		
13.	The system must detect unreasonably extended TLS/SSL headers		
14.	The system must detect rate based and connection exhausting attacks against SSL/TLS		
15.	The solution must be able to mitigate DoS vectors focusing on protocol weaknesses of HTTP Slowloris		
16.	The solution must be able to mitigate DoS vectors focusing on protocol weaknesses of HTTP Slow Post		
17.	The solution must be able to mitigate DoS vectors focusing on protocol weaknesses of HTTP such as Hash DoS or HTTP Cache Abuse DDoS		
18.	The solution must be able to mitigate DoS vectors focusing on protocol weaknesses of HTTP Get Flood		
19.	The system must allow protection parameters to be changed while a protection is running		
20.	The solution must be able to protect following LAND, Fake Session, Recursive GET (web scraping)		
	Solution Management & Reporting Requirements		
1.	The solution Graphical User Interface (GUI) must allow for multiple levels of access including administrator and operator levels. The GUI access must be via HTTPS		
2.	The solution GUI must include a change log that reports all relevant events that might affect its administration including user logins, configuration changes, CLI commands and solution updates		

S.No	Technical Specifications	Compliance (Yes / No)	Deviations (if any)
3.	The solution must provide the ability to create and export diagnostics packages that contain configuration and status information to be used for troubleshooting purposes.		
4.	The solution must provide the ability to manage its files through the GUI, including upload, download and deletion.		
5.	The solution must provide a CLI interface that provides solution monitoring functions and CLI access must be provided using SSH		
6.	The solution must provide a alert/notification provision like Syslog, SNMP or SMTP to alert administrators on important events.		
7.	The solution must allow for configuration of multiple local user accounts		
8.	The solution must provide user- level privilege access controls that may be assigned to users or groups of users to enforce privilege separation		
9.	The solution must support multiple authentication mechanisms via local, RADIUS, TACACS		
10.	The solution must have provision to define IP Access Control lists for all remote services that are accessible		
11.	The solution must provide the ability to backup and restore the solution configuration.		
12.	The solution must provide the ability to configure scheduled automatic backups, download/upload backup files, view backups that have been created, and manually backup data		
	Reporting		
1.	The solution must provide an appliance status dashboard that includes information about active alerts, all protections applied to traffic, total passed and blocked traffic, blocked hosts, traffic through the interfaces and solution CPU/Memory status		
2.	The solution must provide summary reporting of user defined Top IP Sources and Destinations		
3.	The solution must display summary reporting by Country classification		

S.No	Technical Specifications	Compliance (Yes / No)	Deviations (if any)
4.	The solution must display statistics on the amount of dropped and passed traffic		
5.	The solution must provide detailed statistics and graphs for specific prefixes, showing their impact on traffic over a custom specified interval		
6.	The solution must display real- time protection statistics on dropped and passed traffic in bytes and packets, with rate statistics in bps and pps		
7.	The detailed statistics and graphs for each protection group for Servers like Web, DNS, File Servers, Custom Servers must include information on total traffic, total passed/blocked traffic, number of blocked hosts, statistics on each prevention type, traffic by URL, traffic by Domain, IP Location information, Protocol distribution, Services distribution, Web Crawlers, and statistics on top blocked hosts		
8.	The solution must support the generation of pdf reports containing the detailed statistics and graphs for any user defined entity from the solution		
9.	The solution must support the generation of e-mail reports with the detailed statistics and graphs for any user defined entity from the solution		
10.	The solution shall be able to perform time synchronization (NTP, etc.)		
11.	The solution shall support monitoring using SNMP version 3		
12.	The solution must provide built in logging to 3rd party security event tracking systems (SIEM)		
	Additional feature support		
1.	The solution shall support an open API that has SOAP/XML message exchanges that allow 3rd party to fully administer the solution.		
2.	Should have market ready API for SDN environment integration for attack mitigation		

5.2.2.15 Platform

S.No	Features	Compliance (Yes / No)	Deviations (if any)
1	**Platform**		
1.0	Solution can be proposed with single / multiple appliances		
1.1	Must be an appliance with hardened OS		
1.2	Platform should be a full proxy architecture and must perform reverse proxy for inside applications		
1.3	Should have administration partitioning and segmentation / virtualization, whereby the physical device can span across multiple network segments without any inter device routing. The segmentation / virtualization feature should support the use of the same internal IP across the multiple network segments.		
1.4	Should have a dedicated out-of-band Ethernet management port		
1.5	Should have full support IPv6. It should support all IPv6 scenarios: a. IPv4 on the inside and IPv6 on the outside b. IPv6 on the inside and IPv4 on the outside c. IPv6 on the inside and outside		
1.6	Should support VLAN, LACP & Trunking		
1.7	Should have a chassis height of 1U/2U Rack Units		
1.8	Application should support throughput of minimum 60 Gbps for Server Load balancing		
1.9	The appliance must provide appliances with minimum 8 X 10 Gbps Short Range Fiber Ports Interfaces		
1.10	The solution must support to Server Load Balancing along with WAF together from same appliance		
1.11	Should have a SSD with minimal capacity of 128 GB or above"		
1.12	Should have a SSD with minimal capacity of 300 GB		
1.13	"OS should be certified by ICSA"		
1.14	Should have SSL acceleration and Compression		
1.15	Should have dual power supply		
2	**Performance**		

S.No	Features	Compliance (Yes / No)	Deviations (if any)
2.1	Platform should have "L7" throughput of minimum 20 Gbps		
2.2	Should have capability to support up to 20 Million Concurrent Connection		
2.4	Should have 20000 TPS, where TPS = Only one HTTP Transaction over each new SSL handshakes per second, without session reuse and using a 2048 bit key SSL Certificate.		
2.5	Should have SSL Throughput of minimum 40 Gbps		
2.6	Should have compression throughput of minimum 10 Gbps		
2.8	Should support configurable TCP Optimization features for Server- side		
3	**Server Load Balancing**		
3.1	Should have application delivery features such as layer 7 load balancing, layer 7 content switch, caching, hardware based SSL offload and hardware based server side compression		
3.2	Should have capability to monitor the applications using intelligent application level monitors which can be system defined, internal or external executable scripts		
3.3	Should be able to tune monitoring frequency and time automatically when server is available for long time, this is to avoid monitoring load on server		
3.4	Should have 2048 and 4096 bit key for SSL certificate support		
3.5	Should have capability to support ECC, RSA and ECC+RSA (Hybrid) Certificates for SSL offload		
3.6	Should provide static and dynamic load balancing algorithms such as round robin, weighted round robin, fastest, predictive and observed		
3.7	Should be application aware and provide Full Proxy for protocols such as HTTP, HTTPS, FTP, SIP, DNS, Diameter, RADIUS etc.		
3.8	Should support inspection of SSL traffic for reverse proxy and forward proxy deployment. Should also		

S.No	Features	Compliance (Yes / No)	Deviations (if any)
	support ICAP interface for integration with external security systems.		
	Should support IoT Device authentication over SSL and MQTT Message parsing and MQTT load balancing.		
3.9	Should have HTTP 2.0 gateway in environment where the client to load balancer traffic is HTTP 2.0 and from load balancer to server is normal HTTP 1.1		
4	**Web Application Firewall**		
4.1	Should be an ICSA WAF 2.1 certified		
4.2	WAF should have positive and negative security model		
4.3	The proposed WAF should be equipped with a set of pre-built application specific security policies that provide out-of-the-box protection for common applications		
4.4	The proposed WAF should have a mechanism to deploy preconfigured policy that can immediately secures the web application. These validated policies should require zero configuration time and serve as a starting point for more advanced policy creation, based on heuristic learning and specific application security needs for the application.		
4.5	The proposed WAF should have a dynamic policy builder engine, which is responsible for automatic self-learning and creation of security policies. It should automatically build and manage security policies around newly discovered vulnerabilities without manual intervention.		
4.6	The proposed WAF should at the minimum query the signature service on a daily basis and automatically downloads and apply new signatures, and all signatures must be visible to administrator for review.		
4.7	The proposed WAF should defend against the OWASP Top 10 Vulnerabilities		
4.8	WAF should have capability to automatically analyze attacks like Brute Force and avail CAPTCHA on the fly to users to identify bot / scripted attacks		

S.No	Features	Compliance (Yes / No)	Deviations (if any)
4.9	WAF should have Proactive BOT defense and must have BOT signatures		
4.10	WAF should have different policies for different web applications		
4.11	Should be a scalable platform and support minimum 4 Gbps of WAF throughput capacity with all Signatures enabled and scanning HTTP Request and Response together		
4.12	b. Should protects against various application attacks, including: a. Layer 7 DoS and DDoS b. Brute force c. Cross-site scripting (XSS) d. Cross Site Request Forgery e. SQL injection f. Form Field and Parameter Tampering and HPP tampering g. Sensitive information leakage h. Session high jacking i. Buffer overflows j. Cookie manipulation/poisoning k. Various encoding attacks l. Broken access control m. Forceful browsing n. Hidden fields manipulation o. Request smuggling p. XML bombs/DoS		
4.13	Should have FTP & SMTP protection as part of WAF		
4.14	Should have automatic detection of heavy URLS and protect against BOT attacks to those URLS		
4.15	Should have HTTP based DDOS detection and should start automatic capturing traffic in batch mode for forensic purpose		
4.16	Should support signature staging after update – so that newly added signature to a policy in block mode does not break the application. If needed this can be disabled.		
5	**Device Administration**		

S.No	Features	Compliance (Yes / No)	Deviations (if any)
5.1	Should provide HTTPS interface management for administering the device		
5.2	Should provide SSH interface management for administering the device		
5.3	Should provide troubleshooting and traffic analysis tool like TCP dump		
5.4	Should support role based admin access with roles like no access, Guest, Operator, Application editor, Resource Administrator and Administrator		
5.5	b. Should have a live dashboard with graphical reporting a. CPU Usage b. Memory Usage c. Connections Statistics d. Throughput Statistics e. Virtual Server Status f. Pool Status g. Node Status		
5.6	Should provide historical graphical reporting for the last 30 days on appliance itself		
5.7	Should have a built-in tool to take a snapshot of the unit for troubleshooting and analysis purpose		
5.8	Vendor should provide a service to upload this snapshot and get feedback on the health of the unit & missing Hotfixes and best practices		
6	**High Availability**		
6.1	Should have active-active and active-backup high availability with TCP/IP connection mirroring as well as SSL ID mirroring. Hence old connection should not fail or forced for SSL renegotiation.		
6.2	Should have transparent failover between 2 devices, the failover should be transparent to other networking devices		
6.3	Should support network based failover for session mirroring, connection mirroring and heartbeat check		
6.4	Should support config autosync, manual sync to and from active and backup unit		

S.No	Features	Compliance (Yes / No)	Deviations (if any)
6.5	Should support the feature to force the active device to standby and back to active state; or force a device to offline mode		
6.6	Should support MAC masquerading		
6.7	Should support N+1 High Availability Clustering for future scalability with the ability to add heterogeneous devices from the same OEM into the cluster		
7	**Reporting Features**		
7.1	Should have a Reporting Engine built-in		
7.2	Should support High Speed Logging to a syslog server		
7.3	Support for customized logging through scripts to log any parameter from L3 to L7, like Geolocation, IP addresses, client browser, client OS, etc..		
7.4	Should support integration with SIEM tools like Arcsight and Splunk		
7.5	Should have a log publisher to publish logs to multiple log destinations for the same application (or virtual server)		
7.6	Should have a filtering capability before publishing to a log destination		
8	**Others**		
8.2	Vendor should provide regular updates to geolocation database from their public downloads website		

5.2.2.16 ICCC Application Software for Workflow & SOP Management

S.No	Features	Compliance (Yes / No)	Deviations (if any)
1	**ICCC Application Software**		
1.1	This shall be a highly scalable enterprise level software solution. It shall offer a complete video surveillance solution that will be distributed net- work architecture, user-friendly interface, scalable to required numbers of cameras that can be added on a unit-by-unit basis.		
1.2	The network video management software shall be licensed and shall operate on open architecture and shall require no proprietary IT hardware.		

S.No	Features	Compliance (Yes / No)	Deviations (if any)
1.3	The network video management software shall allow for video to be streamed on workstation in Matrix or on a video wall.		
1.4	The user with administrative rights shall create clients (users) and give access to the software client application based on predefined user access rights.		
1.5	The system shall allow the recording, live monitoring, playback of archived video and data simultaneously.		
1.6	The software shall provide the following: - • Several simultaneous live picture connections of camera in network. • Configuration of monitoring situation (site maps). • Programming of alarm-triggered automatic events in various alarms configuration. • System set up with limited operation options for clearly defined surveillance tasks. • Programming of automatic recording events on a network recorder.		
1.7	The software shall display dual H.264, H.265/H.265+ video streams in real time simultaneously at frame rates ranging from 1 fps to 25 fps and resolution ranging Full HD to other HD/SD resolution.		
1.8	Each camera's bit rate, frame rate and resolution shall be set independently from other cameras in the system, and altering these settings shall not affect the recording and display settings of other cameras.		
1.9	The software shall provide automatic search and discovery of component of video surveillance system on the network, which can be network cameras and mNVRs.		
1.10	The software shall provide drag & drop functions on the system and for set up of connection between cameras and monitors connected to one workstation.		
1.11	The software shall allow: • Live display of cameras. • Live display of camera sequences. • Control of cameras. • Playback of archived video.		

S.No	Features	Compliance (Yes / No)	Deviations (if any)
	• Retrieval of archived video. • Instant Replay of live video. • Use of site maps. • Configuration of system settings. • Configuration and programming of cameras, features like auto tours, presents, etc.		
1.12	The software shall be able to do video recording on any of the following options - inbuilt hard disks on the server, direct attached storage boxes attached to servers, network attached storage, storage area network.		
1.13	The software shall be capable of handling camera and alarm icons on area maps.		
1.14	The software shall support SNMP trap and LDAP.		
1.15	The software shall support Third Party Device Integration: Integration with devices other than cameras via SDK and software triggers provided by connected hardware controllers. Device can be Access Control, Motion Sensors and Door Switches, Fire alarms etc. VMS SDK should also be available for any such kind of integration.		
1.16	The area map shall be configurable to pop up upon the receipt of an alarm received from a camera on the map. This can be on the same or other monitors on the PC.		
1.17	The software shall be able to select the required recording based on the time recording was activated, the duration of recording, operator activated recording, event activated recording, scheduled recording.		
1.18	The software shall provide a reporting utility for tracking for the following minimum options. Video clips and image snapshots shall be stored with reports for documenting events. • Alarms • Incidents • Operator Logs		
1.19	The software shall have the facility to export the desired portion of clipping of video from a desired date/time to another desired date/time on DVD/ on any		

S.No	Features	Compliance (Yes / No)	Deviations (if any)
	client/ network storage device. Viewing of this recording shall be possible on authorized player, which shall be provided by soft- ware manufacturer or in media player on computer utilizing a Window environment.		
1.20	The Servers shall not limit the number of network video recording servers which can be networked together to form video management and recording system.		
1.21	The Servers shall maintain a catalogue of settings for all the clients, servers, and IP cameras & IP enabled cameras in the system. If a single server cannot manage the Video Management servers & recording, in such cases, additional server shall be provided.		
1.22	The software shall enable the client to dynamically create connections between cameras and clients and view live or recorded video on Monitors.		
1.23	The software shall provide the client seamless operation of all cameras and clients available in the system regardless of the actual connection to different Network Video Recording servers.		
1.24	The software shall detect signal loss and have the capability to alert the systems administrator.		
1.25	The software shall receive all incoming events (motion detection and triggered digital input and relay output) in the system and take appropriate actions based on user-defined event/action relationships.		
1.26	The software shall create an audit trail of all events and user activities.		
1.27	The Software shall support the following: - • The Software shall provide a full matrix operation of IP video to display monitors. • The Software shall have the capability of creating camera sequences with the following functionalities: ✓ Each Sequence shall have capability up to hundreds of cameras. ✓ Each camera in the sequence shall have its own individual dwell time, from 1 to 60 seconds.		

S.No	Features	Compliance (Yes / No)	Deviations (if any)
	✓ Multiple users shall be able to view the same camera sequence simultaneously, not necessarily synchronized one with the other. ✓ Web and Mobile surveillance shall be available. ✓ Event based playback shall be available. ✓ Shall support Video Time Lapse or Video Synopsis feature to summarize the video of hours to seconds.		
1.28	The software shall provide alarm management module. • The alarm management shall be able to set any monitor or groups of monitors to display cameras automatically in response to alarm inputs. • The alarm management shall be able to reset automatically or manually alarmed video.		
1.29	It shall be possible to search for recordings in the software by camera, date and time. If a date and time is specified, playback shall commence from that date and time. It shall be possible to playback more than one camera simultaneously.		
1.30	The software shall support at least 64 video streams concurrently. It shall support at least four monitors in one server/ workstation for displaying live video. It shall allow minimum five levels of user and alarm prioritization. It shall allow minimum 16 cameras to be re-played simultaneously.		
1.31	The Software shall be seamlessly integrated with Face recognition Software and have capability to receive the alerts.		
1.32	Software shall provide comprehensive health check of all the cameras, mNVR and NVR periodically and shall generate a log for the same.		
2	**Graphic User Interface Client Software Features**		
2.1	GUI Software shall perform the following applications simultaneously without interfering with any of the storage server operations (recording, alarms, etc.): - • Live display of cameras.		

S.No	Features	Compliance (Yes / No)	Deviations (if any)
	• Live display of camera sequences. • Control of cameras. • Playback of archived video. • Retrieval of archived video. • Instant replay of live video. • Use of graphical controls (maps) and alarm management. • Configuration of system settings.		
2.2	GUI Software shall support any form of IP network connectivity including LAN, WAN and wireless LAN technologies.		
2.3	GUI Software shall support multicast and unicast video streaming.		
2.4	GUI Software shall provide an authentication mechanism, which verifies the validity of the user.		
2.5	GUI Software shall allow for live monitoring of video.		
2.6	It shall enable view of 1 to minimum 16 video tiles simultaneously on a single digital monitor at 25 fps per camera.		
2.7	Software shall provide on each of the digital monitors independently the following tile views: • Full screen • Quad view • 4x4 (16-view) • Any other window division based on the site requirement.		
2.8	GUI Software shall allow operators to view an instant replay of any Camera. • The operator shall be able to define the amount of time he/she wishes to go back from a timeline bar or through a custom setup period. • The operator shall be able to control the playback with play, pause, forward, and speed buttons.		
2.9	The operator shall be able to choose and trigger following minimum action from a macro/site map: • View Camera in a video tile. • View map or procedure in a video tile. • Starting/stopping PTZ pattern (Future).		

S.No	Features	Compliance (Yes / No)	Deviations (if any)
	• Go to PTZ pre-set (Future).		
2.10	GUI Software shall provide management and control over the system using a standard PC mouse, keyboard and Digital keyboard.		
2.11	GUI Software shall display all cameras attached to the system regardless of their physical location on the network.		
2.12	GUI Software shall display all camera sequences created in the system.		
2.13	GUI Software shall allow operators to control (pause/play, skip forwards, skip backwards) camera sequences.		
2.14	GUI Software shall display all cameras, sequences and users in a logical tree.		
2.15	GUI Software operator shall be able to drag and drop a camera from a tree of available cameras into any video tile for live viewing.		
2.16	GUI Software operator shall be able to view the camera from a tree of available cameras into any video tile for live viewing.		
2.17	GUI Software shall support graphical site representation (map) functionality, where digital maps are used to represent the physical location of cameras and other devices throughout facility.		
2.18	GUI Software with inbuilt GIS map display shall have the ability to contain hyperlinks to create a hierarchy of interlinked maps.		
2.19	GUI Software operator shall be able to view the camera from a map into a video tile for live viewing in the same browser without opening a new browser.		
2.20	The operator shall be able to click on an icon in a map to initiate PTZ camera pre-sets, run PTZ pattern, view camera on a monitor (on demand as well as automated pop up of camera stream from bus in alarm state) or send an I/O stream.		
2.21	The GUI software shall support digital zoom on a fixed camera's live video streams.		

S.No	Features	Compliance (Yes / No)	Deviations (if any)
2.22	The GUI software shall support digital zoom on a PTZ camera's live video streams.		
2.23	The operator shall be able to control Pan, Tilt and Zoom patterns of PTZ Camera.		
2.24	The software shall be able to display video of cameras on 40-inch Large Format Display Monitors and Workstation Monitors.		
2.25	The software shall allow the control of display from the client PC.		
2.26	The operator from the GUI software shall be able to decide the screen layout and also the cameras that shall be displayed on the monitors.		
2.27	The software shall support multicasting.		
2.28	It shall be possible to switch the screen layout in response to an alarm.		
2.29	The GUI Software shall support text superimposing the title and date & time on the video.		
3	**Video Recording Software**		
3.1	Software shall support recording of H.264, H.265/ H.265+ video streams. It shall support recording of video and audio for all the channels.		
3.2	Software shall support triplex applications, recording, re-play and backup simultaneously. It shall be compatible with windows Server OS or Linux for highest performance and reliability.		
3.3	Software shall operate on open architecture and shall not require any proprietary hardware.		
3.4	Software shall be able to record minimum 64 different video streams or more simultaneously. It shall be accessible from any client PC connected to the network.		
3.5	Software shall provide network time server function to ensure the synchronization of the video servers and the recordings.		
3.6	The servers shall be connected to the network so that these can be placed at any location which has network access.		

S.No	Features	Compliance (Yes / No)	Deviations (if any)
3.7	The software shall be able to receive alarms of different types from equipment to start a recording. These alarms can be motion detection, video loss, and unified picture and trigger input.		
3.8	The software alarm recording shall support pre-and post-alarm periods. Both can be configured in duration.		
3.9	The software shall provide a status of the available recording capacity.		
3.10	Fault Tolerant Recording: • If Software & Server(s) operation are interrupted, like power disconnection and once the server(s) are restarted, these shall automatically resume recording of any cameras these were recording prior to the interruption. • Software shall support network fault-tolerant recording such that if the network connection between a video management server and video recording server becomes unavailable, for example through cable break- age, network congestion or WLAN inter		
3.11	Search & Export: • It shall be possible to search for recordings in the software by camera, date and time. If a data and time is specified, playback shall commence from that date and time. It shall be possible to playback more than one camera simultaneously. • Software shall be able to export sections of recordings to a separate Windows folder, which can then be written to CD-ROM, DVD-ROM or USB Flash Drives etc. to be played back at a location not connected to the network video management & recording		
3.12	Software should provide the option to access the number of cameras in the bus, based on the user requirement.		
4	**Vehicle Tracking Software**		

S.No	Features	Compliance (Yes / No)	Deviations (if any)
4.1	The system should be capable to track 5000 vehicles simultaneously. However, the present requirement is 1800 nos. of vehicles only.		
4.2	The offered Vehicle Tracking System shall be able to view the progress of the vehicle on the entire route on real time basis. The data displayed shall include but not limited to position, direction and speed vehicle registration number, distance, halt report etc. as per requirement of MTC.		
4.3	The system should be capable of providing seamless information of the status of vehicles under monitoring/ tracking by the system. In case of non-availability of communication link or system at base, the vehicle-mounting unit should be equipped with minimum 1 day of store and for- ward mechanism to ensure no loss of any data/ information.		
4.4	The system should be able to integrate with any third-party Passenger Information System, ITMS, ITS to be commissioned by the Purchaser in future.		
4.5	The system should have automatic log/ historical data (track record of all vehicles) capturing feature.		
4.6	The system should also be compatible with any other mobile network service provider.		
4.7	All the necessary statutory licenses and authorization, if any, from the respective authorities will be under the scope of work of the bidder at no extra cost to the Purchaser.		
4.8	The system should be based with access through login ID and password.		
4.9	The GIS should be capable of editing features such as addition/ deletion of POIs (Point of interest) search feature etc.		
4.10	The system should have provision for flexibility in customization of output reports.		
4.11	Vehicle Management System will be hosted in proposed data centre of this project.		
4.12	Live tracking, tracking data, related reports etc. should be available on server which should be secure.		

S.No	Features	Compliance (Yes / No)	Deviations (if any)
4.13	GPS integration with GIS is required to locate all buses of MTC and (on which GPS units are fitted) on GIS Map. Vehicle tracking should happen even while any vehicle is parked/stationary/ignition-off		
4.14	The proposed map should have feature to select a bus from which the panic alert is received.		
4.15	It shall show the status of the bus with different colours for health and alarm monitoring.		
4.16	It shall show the status of the bus with different colours for health and alarm monitoring.		
4.17	The map should provide the feature to select a bus to provide following details on click of bus icon: • On demand live feed of in-vehicle camera • Health status of device • Alarm history • Health log • Bus license plate number • GPS coordinate (dynamic) of bus • Crew member's phone number of the bus		
4.18	SMS Gateway Features: • SI to provision SMS Gateway for Integration with the VMS and develop necessary applications to send and receive all SMS alerts as per the functional requirements. SMS gateway will also act as a fall back communication to receive details from the buses with GPS location, panic alert and health status information, which will be system generated from each mNVR. Any external/third party SMS gateway can be used, but this needs to be specified in the Technical Bid, and approved during Bid evaluation. • In addition to receipt of SMS as communication fall back as received from mNVR, Implementation Agency to provision SMS Gateway for Integration with VMS & VTS and develop necessary application to send all filtered (panic alerts at CCC) SMS to respective stakeholders (at least Four) as per the functional requirements. Information format		

S.No	Features	Compliance (Yes / No)	Deviations (if any)
	of the SMS will be defined at the time of the implementation. Bidder to consider the recurring charges for the contract period.		
4.19	Development and incorporation of Standard Operating Procedures (SOPs) in system so that it is visible to operators in control room and other relevant staff and can be referred as and when required. Operator should be able to access the standard operating procedure for the incidence management. There must be option to customise the SOPs as per the requirement of MTC. SOPs should include pro-visioning of sending the automatic/manual alerts to the various stake- holders, as per selection by the operator/system.		
4.20	SI to integrate CCC application with Dial 100 application. CCC operator will forward the filtered alert received from bus to Dial 100 application. SI has to integrate, customise and carry out all the required development for seamless integration of both of these systems as per requirements of the MTC.		
5	**Others**		
5.1	SI shall offer required number of Camera Recording Licenses along with Video Management License. Preferably, License shall not restrict the number of recording Servers used in the system. If Licensing restricts the number of recording Servers then adequate extra recording server Licenses shall be provided.		
5.2	Preferably, Licensing shall not restrict the Storage size used in the system. If it does then storage, Licensing shall be provided for required percentage of current storage size as per offered system design or offered solution requirement.		
5.3	Client Licensing shall not be restricted to specific physical client Work-stations (PC) and shall provide access from any Workstation within the network with required number of users simultaneous.		
5.5	SI System should have the ability to integrate with any third-party vehicle tracking system.		

S.No	Features	Compliance (Yes / No)	Deviations (if any)
5.6	SI should ensure Future integration of other applications like Automatic Fare Collection System, ITMS, ITS, etc. Application should be built in such a way that future integrations and enhancements can be done easily		

5.2.2.17 Fire proof enclosure

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

S.No	Parameter	Description	Compliance (Yes / No)	Deviations (if any)
1.	Product details-			
2.	Please mention Make Model No. or Part Code			
3.	Capacity	300 Liters		
4.	Temperature to Withstand	1000° C for at least 1 hour		
5.	Internal Temperature	30°C after exposure to high temperature For 1 hour		
6.	Locking	IO-lever high security cylindrical/ Electronic lock		

5.2.2.18 KVM Module (If required)

S.No	Item	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
1.	Product details-			
2.	Please mention Make Model No. or Part Code			
3.	KVM Requirement	Keyboard, Video Display Unit and Mouse Unit (KVM) for the IT Infrastructure		

S.No	Item	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
		Management at Data Centre		
4.	Form Factor	19” rack mountable		
5.	Ports	minimum 8 ports		
6.	Server Connections	USB or KVM over IP.		
7.	Auto-Scan	It should be capable to auto scan servers		
8.	Rack Access	It should support local user port for rack access		
9.	SNMP	The KVM switch should be SNMP enabled. It should be operable from remote locations		
10.	OS Support	It should support multiple operating system		
11.	Power Supply	It should have dual power with failover and built-in surge protection		
12.	Multi-User support	It should support multi-user access and collaboration		

5.2.2.19 Back-up Software

- The software shall be primarily used to back up the necessary and relevant video feeds from storage that are marked or flagged by MTC. The other data that would require backing up would include the various databases that shall be created for the surveillance system. Details of data that would be created are available in the table at section ‘Data Requirements’
- Scheduled unattended backup using policy-based management for all Server and OS platforms

- The software should support on-line backup and restore of various applications and Databases
- The backup software should be capable of having multiple back-up sessions simultaneously
- The backup software 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
- The backup software should support different types of user interface such as GUI, Web-based interface

S.No	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
1.	Product details-		
2.	Please mention Make Model No. or Part Code		
3.	The proposed appliance must be a converged, integrated appliance for long term data retention and disaster recovery		
4.	The solution must support data protection of physical systems as well as virtual environments		
5.	The Proposed backup solutions should support online backup of IBM DB2, IBM Lotus Domino, Microsoft Exchange, Microsoft Office Share Point Server, Microsoft SQL Server, MySQL, and Oracle Databases without any additional licenses requirement The proposed solution should reduce network bandwidth for backup by sending only changed data blocks over network.		
6.	Must Support Enterprise Applications and Database Backups without integration with Backup Software, for better visibility of Backups to Application and database Owners, thus ensuring faster and direct recovery on application/database level. This integration must be available for Oracle, SAP, SAP HANA, DB2, MS SQL, etc.		
7.	The proposed solution should support Instant Access and Restore of the protected virtual machine.		

S.No	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
8.	The proposed integrated appliance should support NVMe flash to help in superior performance		
9.	The proposed solution must have minimal foot print in the Data Centre. The bidder must provide details on the rack, power and cooling requirements.		
10.	The proposed appliance must support monitoring and simplified management via standard browser and intitutive user interface		
11.	The proposed solution must be able to de-duplicate backup data globally across sites, desktop, laptops and servers, applications and databases		
12.	The proposed solution must provide efficient data reduction by using variable block length deduplication at the source as well as target side.		
13.	Must support 256 bit AES encryption for data at rest and data-in-flight during replication. It must offer internal and external key management for encryption		
14.	The proposed solution should have the ability to synchronously as well as asynchronously replicate the virtual machine		
15.	Solution should have point in copy recovery whenever needed for Virtual environment		
16.	Fully integrated with VMware or equivalent Change Block Tracking for both backups and restore		
17.	It must support VMware or equivalent image level backup as well as provide granular file, folder as well as virtual machine level restore ability.		
18.	The integrated solution must provide a plug-in for vSphere GUI and vCenter GUI or equivalent for management, policies and restore. It must also integrate with VMware vRealize, vCloud Director, vRealize Operations Manager or equivalent to provide self service provisioning, automation and reporting.		

S.No	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
19.	It must support web based advance search from the backup catalog based on dates, time, full text and patterns etc. and also able to recover the data to original / alternate path from the same search console		
20.	Must have inbuilt feature for extensive alerting and reporting with pre-configured and customizable formats. The proposed solution must have capability to do trend analysis for capacity planning of backup environment not limiting to Integrated Backup Solution /Clients, Virtual Environment, Replication etc.		
21.	The proposed solution must have the ability to reduce network bandwidth and source side compute overheads by only transferring the changed blocks to the backup target.		
22.	The proposed solution should be capable of throttling Network Bandwidth to customize the need.		
23.	The solution should be capable of integration with active directory infrastructure for ease of user rights management along with role based access control to regulate the level of management		
24.	The proposed backup software should support restore a single VM or equivalent, single file from a VM or equivalent, a VMDK or equivalent restore from the same management console for ease of use. Proposed backup software should not need a physical proxy server for VMware or equivalent backups and should have a minimum of 16 concurrent sessions capability for the VMWARE VM machines or equivalent image based backups with single virtual proxy. It should support instant access of multiple VM machines or equivalent		
25.	The proposed backup solution must provide a on a single pane of glass for monitoring the complete backup infrastructure		

S.No	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
26.	The proposed backup solution must have advanced analytic & reporting capabilities built in at no additional cost.		
27.	The proposed solution must have the ability to move long term backup data to the public or private or hybrid cloud storage as well as provide DR capabilities to AWS.		
28.	Solution should also be able to be provided in a "Air-Gap" offering to help against ransomware		
29.	The proposed appliance must be configured with minimum 55 TB usable capacity and should provide the scalability upto 90 TB usable capacity within the same appliance.		
30.	De-Duplication Appliance must have minimum 10% share in the IDC's Target & Integrated Appliance.		

5.2.2.20 Database Licenses

Bidder needs to provide Licensed RDBMS, enterprise/full version as required for the proposed Surveillance System and following all standard industry norms for performance, data security, authentication and database shall be exportable in to XML.

5.2.2.21 Enterprise Management System (EMS)

The Enterprise Management System (EMS) is an important requirement of this Project. Various key components of the EMS are:

- SLA & Contract management System
- Network Monitoring System
- Server Monitoring System
- Helpdesk System

Proposed EMS Solution shall be based on industry standard best practice framework such as ITIL etc.

5.2.2.21.1 SLA & Contract management System

The SLA & Contract Management solution should enable the GCP to capture all the System based SLAs defined in this Tender and then calculate quarterly (or for any duration) penalty automatically. Measuring service performance requires incorporation of a wide variety of data sources of the Surveillance project. The SLA solution should support the collection data from

various sources in order to calculate Uptime / Performance / Security SLAs. Various features required in this component to EMS are -

- It must be a centralized monitoring solution for all IT assets (including servers, network equipment etc.)
- The solution must have integrated dashboard providing view of non performing components / issues with related to service on any active components
- The solution must follow governance, compliance and content validations to improve standardisation of service level contracts
- Application should be pre-configured so as to allow the users to generate timely reports on the SLAs on various parameters.
- The solution must support Service Level Agreements & Lifecycle Management including Version Control, Status Control, Effectively and audit Trail to ensure accountability for the project.
- The solution must have the ability to define and calculate key performance indicators from an End to End Business Service delivery perspective related to Surveillance Project under discussion.
- The solution should support requirements of the auditors requiring technical audit of the whole system
- The solution most have an integrated dashboard, view of Contract Parties & current SLA delivery levels and view of Services & current SLA performance
- The solution should support SLA Alerts escalation and approval process.
- Solution should support effective root cause analysis, support capabilities for investigating the root causes of failed service levels and must make it possible to find the underlying events that cause the service level contract to fail.
- Accept Data from a variety of formats; provide pre-configured connectors and adapters, Ability to define Adapters to data source in a visual manner without coding.
- Support for Defining and Calculating service Credit and Penalty based on clauses in SLAs.

5.2.2.21.2 ***Reporting***

- Ability to generate reports on penalty and credit due, to check on non-compliance of SLAs for the surveillance project
- Monetary penalties to be levied for non-compliance of SLA, thus the system must provide Service Level Performance Report over time, contract, service and more.
- The solution should provide historical and concurrent service level reports for the surveillance project in order to ensure accountability of the service provider's performance
- Automatic Report creation, execution and Scheduling, must support variety of export formats including Microsoft Word, Adobe PDF etc.
- The solution must support Templates for report generation, Report Filtering and Consolidation and Context sensitive Drill-down on specific report data to drive standardisation and governance of the surveillance project

- The solution must support security for drill-down capabilities in dashboard reports ensuring visibility for only relevant personnel of the surveillance project
- Support real-time reports as well as historical analysis reports (like Trend, TopN, Capacity planning reports etc.)
  - Resource utilisation exceeding or below customer-defined limits
  - Resource utilisation exceeding or below predefined threshold limits

An indicative List of SLAs that need to be measured centrally by SLA contract management system are given in the Tender Document. These SLAs must be represented using appropriate customisable reports to ensure overall service delivery.

5.2.2.21.3 *Network Management System*

Solution should provide Fault, Configuration & Performance management of the entire datacentre infrastructure and should monitor IP\SNMP enabled devices such as Routers, Switches, Cameras, Online UPS, etc. Proposed Network Management shall integrate with SLA & Contract Management system in order to supply KPI metrics like availability, utilisation in order to measure central SLA's and calculate penalties. Following are key functionalities that are required, which will help measuring SLA's as well as assist administrators to monitor network faults & performance degradations in order to reduce downtimes, increase availability and take proactive actions to remediate & restore network services.

- The proposed solution must automatically discover manageable elements connected to the infrastructure and map the connectivity between them. Solution should provide centralized monitoring console displaying network topology map from central location to Zonal / Police Station Level.
- Proposed solution should provide customizable reporting interface to create custom reports for collected data.
- The system must use advanced root-cause analysis techniques and policy-based condition correlation technology for comprehensive analysis of infrastructure faults.
- The system should be able to clearly identify configuration changes as root cause of network problems and administrators should receive an alert in case of any change made on routers spread across surveillance project.
- Network Performance management system should provide predictive performance monitoring and should be able to auto-calculate resource utilisation baselines for the entire managed systems and networks and allow user to set corresponding upper and lower threshold limits based on baseline data instead of setting up manual thresholds for monitored devices.
- The system must support the ability to create reports that allow the surveillance administrators to search all IP traffic over a specified historical period, for a variety of conditions for critical router interfaces.
- The proposed system must be capable of providing the following detailed analysis across surveillance domain:
  - Top utilised links (inbound and outbound) based on utilisation of link

- Top protocols by volume based on utilisation of link
- Top host by volume based on utilisation of link

5.2.2.21.4 *Server Performance Monitoring System*

- The proposed tool should integrate with network performance management system and support operating system monitoring for various platforms supplied as part of the Surveillance Project.
- The proposed tool must provide information about availability and performance for target server nodes.
- The proposed tool should be able to monitor various operating system parameters such as processors, memory, files, processes, file systems, etc. where applicable.
- The solution should provide a unified web based console, which consolidates all aspects of role based access under a single console.
- Proposed Network Management shall integrate with SLA & Contract Management system in order to supply KPI metrics like availability, utilisation, and performance in order to measure central SLA's and calculate penalties.

5.2.2.21.5 *Centralized Helpdesk System*

- The proposed helpdesk solution must provide flexibility of logging, viewing, updating and closing incident manually via web interface for issues related to surveillance project.
- Helpdesk system should provide incident management, problem management templates along with helpdesk SLA system for tracking SLA's pertaining to incident resolution time for priority / non-priority incidents.
- The proposed helpdesk solution must have a built-in workflow engine to define escalations or tasks to be carried out after issues or change order are logged pertaining to surveillance project.
- Centralized Helpdesk System should have integration with Network/Server Monitoring Systems so that the Helpdesk Operators can to associate alarms with Service Desk tickets to help surveillance operators that for what particular alarms corresponding helpdesk tickets got logged.
- Surveillance Network admin should be able to manually create tickets through Fault Management GUI.
- System should also automatically create tickets based on alarm type
- System should provide a link to directly launch a Service Desk view of a particular ticket created by alarm from within the Network Operation console.

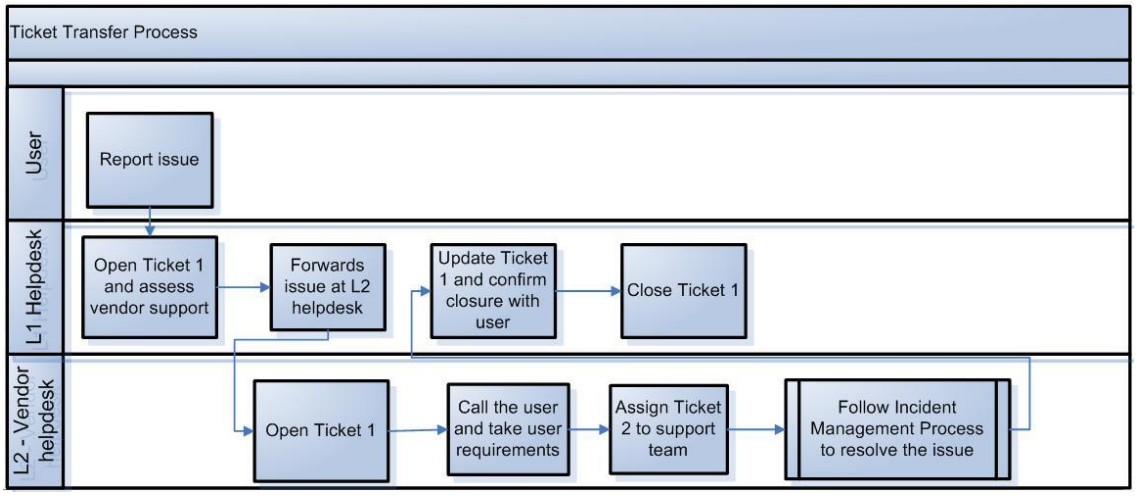
5.2.2.21.6 *Helpdesk Management*

It is envisaged that the centralized helpdesk, functioning as proposed below, would be managed by the Systems Integrator and shall serve following objectives:

- Act as the Point of Contact for the users of Surveillance System
- Own an Incident throughout its Lifecycle

- Communicate effectively with Dept. Officers and IT support teams.
- Maintain high user satisfaction levels
- Maintain the SLA statistics & submit quarterly report to Department

A general process flow for the helpdesk management is depicted in the flow-chart given as follows. Systems Integrator shall prepare a detailed Helpdesk Policy in consultation with MTC & its Consultant prior to the Go Live date.



System Integrator shall deploy a State-of-Art Enterprise Management System to handle the complexity of Operations & SLA Management

5.2.2.22 Centralized Anti-virus Solution

- Shall be able to scan through several types of compression formats.
- Must update itself over internet for virus definitions, program updates etc. (periodically as well as in push-updates in case of outbreaks)
- Able to perform different scan Actions based on the virus type (Trojan/ Worm, Joke, Hoax, Virus, other)
- Shall be able to scan only those file types which are potential virus carriers (based on true file type)
- Shall be able to scan for HTML, VBScript Viruses, malicious applets and ActiveX controls
- Shall provide Real-time product Performance Monitor and Built-in Debug and Diagnostic tools, and context- sensitive help.
- The solution must support multiple remote installations
- Shall provide for virus notification options for Virus Outbreak Alert and other configurable Conditional Notification.
- Should be capable of providing multiple layers of defence
- Shall have facility to clean, delete and quarantine the virus affected files.
- Should support scanning for ZIP, RAR compressed files, and TAR archive files
- Should support online update, where by most product updates and patches can be performed without bringing messaging server off-line.

- Should use multiple scan engines during the scanning process
- Should support in-memory scanning so as to minimize Disk IO.
- Should support Multi-threaded scanning
- Should support scanning of nested compressed files
- Should support heuristic scanning to allow rule-based detection of unknown viruses
- Updates to the scan engines should be automated and should not require manual intervention
- All binaries from the vendor that are downloaded and distributed must be signed and the signature verified during runtime for enhanced security
- Updates should be capable of being rolled back in case required
- File filtering should be supported by the proposed solution; file filtering should be based on true file type.
- Should support various types of reporting formats such as CSV, HTML and text files
- Shall scan at least HTTP, FTP traffic (sending & receiving) in real time and protect against viruses, worms & Trojan horse attacks and other malicious code.

5.2.2.23 Directory services

- Should be compliant with LDAP v3
- Support for integrated LDAP compliant directory services to record information for users and system resources
- Should provide authentication mechanism across different client devices / PCs
- Should provide support for Group policies and software restriction policies
- Should support security features, such as Kerberos, Smart Cards, Public Key Infrastructure (PKI), etc.
- Should provide support for X.500 naming standards
- Should support that password reset capabilities for a given group or groups of users can be delegated to any nominated user
- Should support that user account creation/deletion rights within a group or groups can be delegated to any nominated user
- Should support directory services integrated DNS zones for ease of management and administration/replication.

5.2.2.24 VoIP Phone

S.No	Parameter	Minimum Specifications	Compliance (Yes/No)	Deviations (if any)
1.	Product details-			
2.	Please mention Make Model No. or Part Code			
3.	Display	2 line or more, Monochrome display for viewing features like messages, directory, operator name, etc.		

S.No	Parameter	Minimum Specifications	Compliance (Yes/No)	Deviations (if any)
4.	Integral switch	10/100 mbps for a direct connection to a 10/100BASE-T Ethernet network through an RJ-45 interface		
5.	Speaker Phone	Yes		
6.	Head set	Port for Head set (Headset also to be provided)		
7.	VoIP Protocol	SIP V2		
8.	PoE	IEEE 802.3af or better		
9.	Supported Protocols	SNMP, DHCP, DNS		
10.	Codecs	G.711, G.722 including handset and speakerphone		
11.	Speaker Phone	Full duplex speaker phone with echo cancellation Speaker on/ off button, microphone mute		
12.	Volume control	Easy decibel level adjustment for speaker phone, handset and ringer		
13.	Phonebook/Address book	Minimum 100 contacts		
14.	Call Logs	Access to missed, received, and placed calls. (Minimum 20 overall)		
15.	Clock	Time and Date on display		
16.	Ringer	Selectable Ringer tone		
17.	Directory Access	LDAP standard directory		

5.3 CCTV Monitoring Systems (VMS) for 6 MTC Officers

5.3.1 Minimum Technical Specifications

5.3.1.1 Workstations for MTC officers at HQ

S.No	Parameter	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
1.	Product details-			
2.	Please mention Make Model No. or Part Code			
3.	CPU	Quad core CPU with 8 threads or equivalent or better		
4.	Memory	8 GB DDR4 or better		
5.	Hard-Disk Drive	512 GB SSD or better		
6.	Display	55”-inch LCD / LED Display		
7.	Display ports	4 Display Port / mini Display Ports		
8.	GPU	Base clock: 1290 Mhz or better Number of cores: 768 or better VRAM: 4GB or better Display connectors: DP 1.4, HDMI 2.0b, dual link-DVI multi-monitor support Max resolution: 7680 x 4320 @ 60 Hz or better		
9.	Keyboard	Wired keyboard with 104 keys		
10.	Mouse	Wired Optical with USB interface		
11.	Ports	USB Ports including 2 USB 3.0 Ports and audio ports for microphone and headphone		
12.	Cabinet	Mini Tower.		
13.	Operating system	Windows 10 64-bit operating system		
14.	Antivirus	To be provided		
15.	Power Supply (SMPS)	700 W or better		

5.3.1.2 8 Port PoE Switches

S.No	Parameter	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
1.	Product details-			
2.	Please mention Make Model No. or Part Code			
3.	Type of Switch	Managed		
4.	Technology	PoE		
5.	Number of 1G Copper Ports	8		
6.	No. of 1 G SFP Port (Uplink)	1		
7.	Switching Capacity -Non Blocking (Gbps)	20		
8.	Throughput (MPPS)	14.9		
9.	Security Feature	SSH v1/v2 SSL v2/v3/TLSv1 Port Security Broadcast/Multicast/ Unicast Storm Control 802.1		
10.	Management Protocol	Web-based GUI and CLI management SNMP v1/v2c/v3, compatible with public MIBs		
11.	QoS	Support 802.1p CoS/DSCP priority Support 8 priority queues Queue scheduling: SP, WRR		
12.	Operating Temperature Range (Degree C)	0°C to 55°C		
13.	Operating Humidity (RH)(%)	90		
14.	IPv6 Ready from day one and dully certified	Yes		

5.4 CTV Monitoring Systems (VMS) – TAB with Mobile Application for 50 MTC Staffs

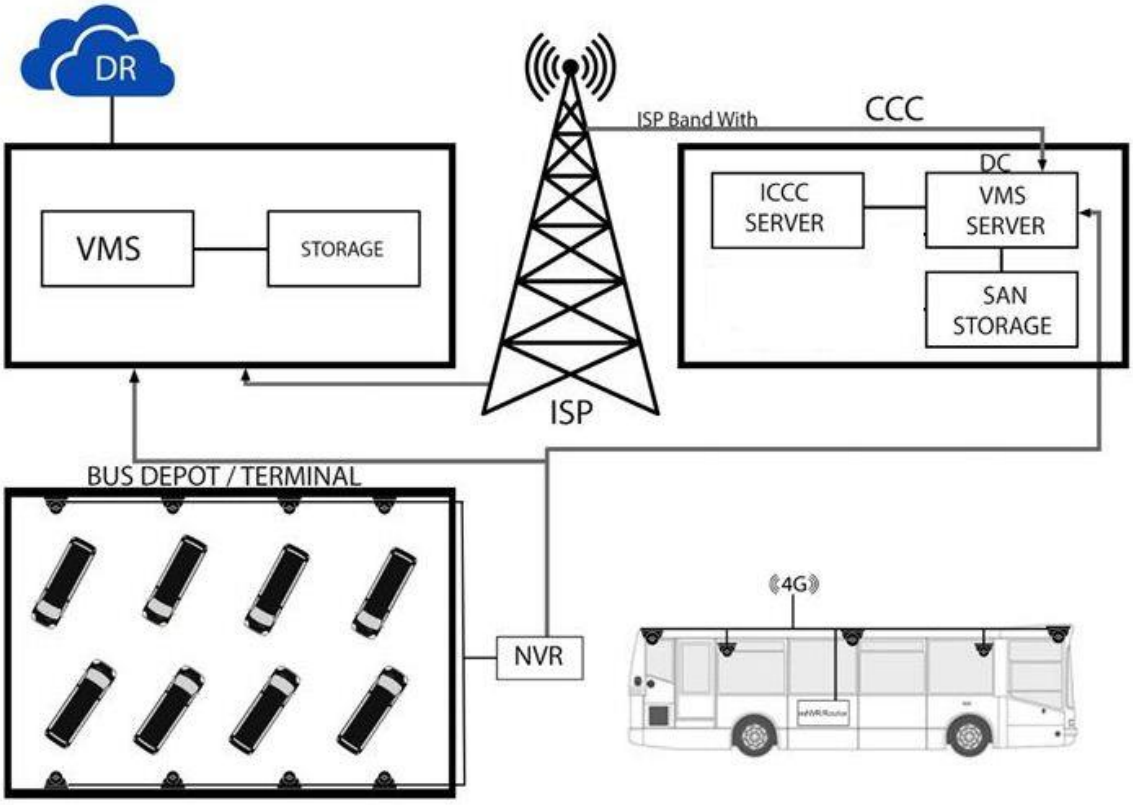
5.4.1 Minimum Technical Specification

5.4.1.1 TAB with Mobile Application

S.No	Parameter	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
1.	Product details-			
2.	Please mention Make Model No. or Part Code			
3.	Screen	12” Touch Screen		
4.	Resolution	800*480		
5.	Speaker	Built-In		
6.	Network	4G		
7.	Communication functions	Bluetooth, GPS, Wifi		
8.	Processor	Quad Core		
9.	Memory capacity	64 GB		
10.	RAM	4 GB		
11.	Operating System	Android		
12.	Operating Voltage	12V		
13.	Operating Temperature	0°C to 55°C		
14.	Relative Humidity	10%~90%		

5.5 CCTV Surveillance System for Women Safety in MTC Depots & Terminals (66)

A High level system overview of the proposed CCTV Surveillance System for MTC is given in the diagram below:



5.5.1 Information security policy, including policies on backup

System Integrator shall be asked to prepare the Information Security Policy for the overall project, which would be reviewed & finalized by the MTC & its Consultant. It is proposed that Security policy would be submitted by the Systems Integrator within 1st quarter of the successful Final Acceptance Tests. The Systems Integrator shall obtain ISO 27001 certification for the Control Centre within 2 quarters of final acceptance test.

5.5.2 Surveillance Equipment – Functional Requirements

The core of system design for the Safe City Surveillance system for MTC Depots & Terminals shall be the feeds from surveillance cameras (Eight numbers) installed at the Depots & Terminals and their analysis. The cameras and related components shall be placed after a thorough assessment at the identified locations. SI should ensure that proper protection is taken against power surges and ensure power stabilization to the surveillance equipment. The System Integrator would need to follow required earthing standards (e.g. IS-3043).

The video surveillance data from various cameras deployed will be stored at the data centre and monitored at the Command & Control Centre. Storage of Video feeds should be for minimum 30 Days at the Data Centre and in NVRs with 1080p Resolution. Cameras would be connected to the Depot & Terminal NVR or VMS recording unit which in turn will be given minimum 20Mbps connectivity to Data Centre over MPLS network. The video feed transmitted should be received at the DC/DR/CCC with zero packet loss.

Once a camera view is positioned, there shall be a mechanical locking arrangement that prevents the camera from drooping / shaking / change of view. Provision (such as spikes) shall also be made to prevent the birds / animals from sitting on the cameras.

The cameras shall also embed the time stamp (in IST) on the captured video and shall sync regularly using a time server.

The camera shall report back to the VMS on the following statuses at regular intervals:

- Camera availability and alerts on disconnection / failure
- Storage availability and alerts on failure
- Time server synchronization status

Viewing of feeds shall primarily be on the following:

a. Remote PC viewing
b. Mobile viewing
c. Video wall

5.5.3 Minimum Technical Specifications

5.5.3.1 IP Bullet Camera

S.No	Parameter	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
1.	Product details-			
2.	Please mention Make Model No. or Part Code			
3.	Image sensor	1/2.8", progressive scan, 2.0megapixel, CMOS		
4.	Lens	2.8~12 mm, AF automatic focusing and motorized zoom lens		
5.	Shutter speed	Auto/Manual, 1~1/100000		
6.	Illumination	Colour: 0.002 Lux (F1.2, AGC ON) 0 Lux with IR on		

S.No	Parameter	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
7.	DNR	2D/3D DNR		
8.	IR Range	Up to 30m (98 ft) IR range		
9.	Defog	Digital Defog		
10.	WDR	120dB		
11.	Resolution	1920 X 1080		
12.	Video Compression	H.265, H.264		
13.	Frame rate	Resolutions and frame rates: 25/30 fps at 1920x1080 (1080p)		
14.	Image enhancing	HLC,BLC, OSD, Privacy masking, ROI, motion detection		
15.	Analytics (in case of Edge)	Intrusion, cross line, motion detection, Scene Change,		
16.	Protocols	IPv4, IGMP, ICMP, ARP, TCP, UDP, DHCP, PPPoE, RTP, RTSP, RTCP, DNS, DDNS, NTP, FTP, UPnP, HTTP, HTTPS, SMTP, 802.1x, SNMP		
17.	Onvif	ONVIF(S/G), API		
18.	Interface	1 RJ45 10M/100M Base-TX Ethernet		
19.	Power supply	12 V DC±25%, PoE (IEEE802.3 af)		
20.	Working temperature	0°C ~ +55°C, Humidity:10%~95% RH(non-condensing)		
21.	Ingress Protection	IP67, IK10		
22.	General Function	Watermark, IP Address Filtering, Tampering Alarm, Alarm input, Alarm output, Access Policy, ARP Protection, RTSP Authentication, User Authentication		
23.	Local Storage	Micro SD, up to 128 GB		
24.	Certification	CE / FCC / UL / BIS certification		

5.5.3.2 8 Channel NVR with minimum 30 Days Storage

S.No	Parameter	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
1.	Product details-			
2.	Please mention Make Model No. or Part Code			
3.	IP Camera Input	8 channel		
4.	Resolution	6MP, 5MP, 4MP, 3MP, 1080p, UXGA, 960p, 720p, XGA, SVGA, D1, CIF, QCIF		
5.	Compression	H.265 / H.264		
6.	Incoming Bandwidth	45Mbps		
7.	Local Display	1 x HDMI, 1 x VGA, simultaneously output different content		
8.	Multi-Screen Display Local monitor (Main / Secondary):	1/1, 4/4, 1+5/1+5, 1+7/1+7, 9/9		
9.	Multi-Screen Display	up to 4 screen simultaneously:		
10.	Client	1 ~ 64 Multiple Layouts		
11.	E-Map	Live Viewing in E-Map (V Station)		
12.	Function	E-PTZ / Scheme (V Station) / Virtual channel		
13.	Search Mode	Date and time (Calendar) / Event		
14.	Playback (Local Monitor)	4 x 1080p@30fps / 8 x 720p@30fps		
15.	Playback (Client)	up to 8x 1080p@30fps		
16.	Synchronize Playback (Local Monitor)	4 x 1080p@30fps		
17.	Synchronize Playback (Client)	up to 8 x 1080p@30fps		
18.	SATA Ports	2 x 3.5'' HDD		
19.	Bit rate	32kbps ~ 64kbps		

S.No	Parameter	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
20.	Audio Function	Bi-directional audio / Dumb / Mute / Broadcasting		
21.	Network Protocols	TCP/IP, UDP, HTTP, DHCP, DNS/DDNS, RTP/RTCP, RTSP, PPPoE, FTP, SNTP, VSIP, UPNP, SMTP, IPv4		
22.	Max. User Access	16 Users		
23.	Output Bandwidth	64Mbps		
24.	Ethernet	1 x 10/100M, RJ45 interface		
25.	Video Out	1 x HDMI (up to 3840 x 2160@60Hz) 1 x VGA (up to 1920 x 1080@60Hz)		
26.	Audio In / Out	1 x RCA Line in / 1 x RCA Line out		
27.	Alarm In / Out	4 x Inputs / 2 x Outputs		
28.	Control	1 x RS485		
29.	USB	2 x USB 2.0		
30.	Operating Temperature	0ºC to 55ºC.		
31.	Operating Humidity	10% ~ 90%		
32.	Power	12V DC ± 10%		
33.	Power Consumption	Max. 15W (HDD not included)		
34.	Certification	CE / FCC / UL / BIS certification		

5.5.3.3 16 Port PoE Switch

S.No	Parameter	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
1.	Product details-			
2.	Please mention Make Model No. or Part Code			
3.	Technology	PoE		

S.No	Parameter	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
4.	Number of 1G Copper Ports	16		
5.	No. of 1 G SFP Port (Uplink)	1		
6.	Switching Capacity -Non Blocking (Gbps)	20		
7.	Throughput (MPPS)	14.9		
8.	Security Feature	SSH v1/v2 SSL v2/v3/TLSv1 Port Security Broadcast/Multicast/ Unicast Storm Control 802.1		
9.	Management Protocol	Web-based GUI and CLI management SNMP v1/v2c/v3, compatible with public MIBs		
10.	QoS	Support 802.1p CoS/DSCP priority Support 8 priority queues Queue scheduling: SP, WRR		
11.	Operating Temperature	0ºC to 55ºC.		
12.	Operating Humidity (RH)(%)	90		
13.	IPv6 Ready from day one and dully certified	Yes		

5.5.3.4 UPS

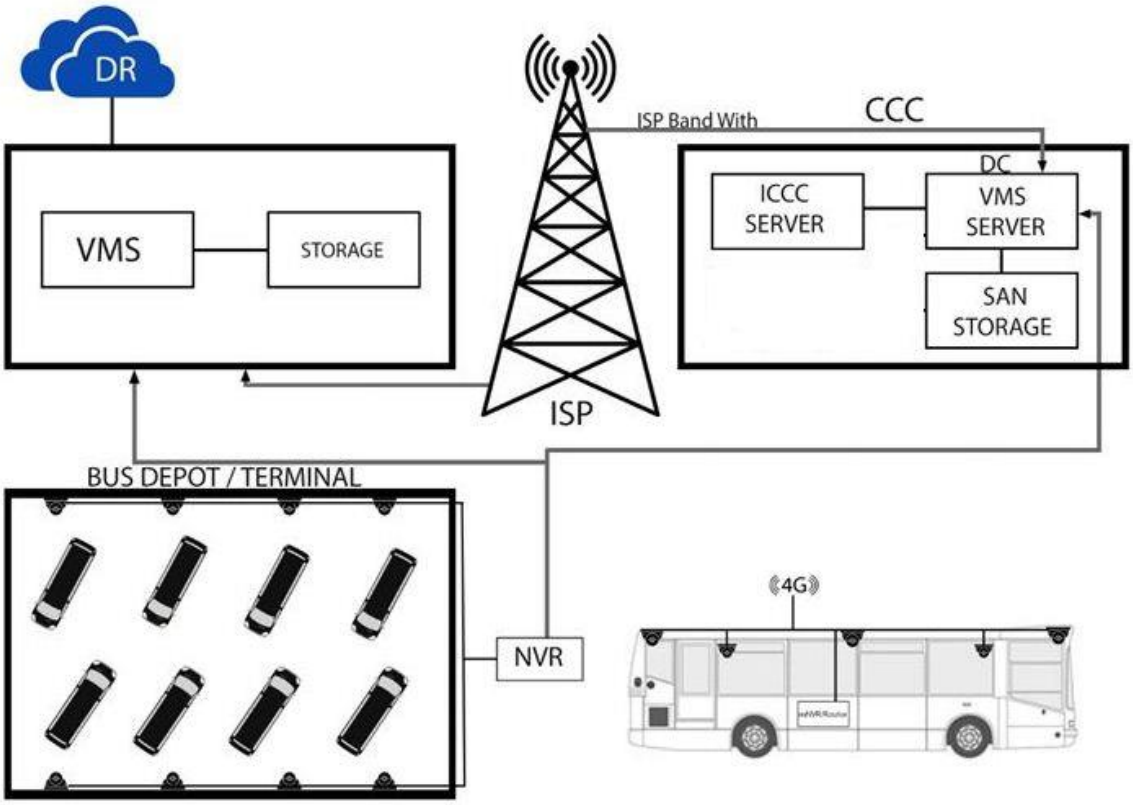
#	Parameter	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
1.	Product details-			
2.	Please mention Make Model No. or Part Code			
3.	Capacity	1 KVA (Minimum). SI to calculate Power Loading and propose more if required		

#	Parameter	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
4.	Input Range	Voltage Range 155-280 V on Full Load Voltage Range 110-280 V on Less than 70% Load Frequency 50 HZ ±3 Hz		
5.	Output Voltage & Waveform	220V AC/ 230V AC/ 240V AC (Selectable)		
6.	I/P & O/P Power Factor	0.9 or higher power factor		
7.	Mains & Battery	Sealed Lead Maintenance Free VRLA type (Lead Calcium SMF batteries NOT acceptable), Mains & Battery with necessary indicators, alarms and protection with proper battery storage stand		
8.	Frequency	50 Hz +/- 0.5% (free running), Pure Sine wave		
9.	Crest Factor	min. 3:1		
10.	Third Harmonic Distribution	3% on Linear Load 5% on Non Linear Load		
11.	Input Harmonic Level	< 10%		
12.	Overall Efficiency	Min. 90% on Full Load;		
13.	Noise Level	< 55 dB @ 1 Meter		
14.	Backup	at least 2 hours		
15.	Warranty	3 years with UPS & battery		
16.	Certification	ISO 9001:2008 & ISO 14001 certified		
17.	Protection	To be provided for overload/ short circuit; overheating; input over/under voltage; output over/ under voltage.		
18.	Alarms & Indications	All necessary alarms & indications essential for performance monitoring of UPS like mains fail, low battery & fault detection		
19.	Interface	SNMP interface support (for remote monitoring)		

#	Parameter	Minimum Specifications	Compliance (Yes / No)	Deviations (if any)
20.	Galvanic Isolation	To be provided through Inbuilt transformer		
21.	Compatibility	UPS to be compatible with DG Set supply and mains supply		
22.	Bypass	Automatic Bypass Switch		
23.	Technology	True ON-LINE (Double Conversion) with IGBT based inverter and PWM Technology		
24.	Support	The system should not be an end of life / end of service product		
25.	Operating Temperature	0°C to 55°C		

5.6 CCTV Surveillance System for Women Safety in 2800 MTC Buses

A High level system overview of the proposed CCTV Surveillance System for MTC is given in the diagram below:



5.6.1 Information security policy, including policies on backup

System Integrator shall be asked to prepare the Information Security Policy for the overall project, which would be reviewed & finalized by the MTC & its Consultant. It is proposed that Security policy would be submitted by the Systems Integrator within 1st quarter of the successful Final Acceptance Tests. The Systems Integrator shall obtain ISO 27001 certification for the Control Centre within 2 quarters of final acceptance test.

5.6.2 Surveillance Equipment – Functional Requirements

The core of system design for the Safe City Surveillance system for MTC Bus shall be the feeds from surveillance cameras (Three numbers) and Panic Button (Four Numbers) at least during the Bus operational hours. The cameras and panic buttons shall be placed as per MTC requirements. SI should ensure that proper protection is taken against power surges and ensure power stabilization to the surveillance equipment.

The video surveillance data from various cameras deployed will be stored at the Bus mNVR for minimum 30 Days with minimum 720p Resolution. Connectivity to Data Centre will be via 4G with MPLS backhaul. System should be capable of viewing the Surveillance Feed from the

Bus at the CCC as and when required. System to transmit all the Surveillance Feed inside the Bus at least 30 Seconds before the Panic Button is pressed and minimum 30 Seconds footage after Panic Button is pressed. Si can select Cameras capable with regional recording to reduce bandwidth requirement. The video feed transmitted should be received at the DC/DR/CCC with zero packet loss.

In case of a need to download large volumes of video data, a mechanism should be provided to be able to connect using an authenticated device using Wi-Fi. Device authentication should be based on time-limited / multi-factor authentication (MFA). All downloads should be allowed only after necessary authorizations. SOP shall be defined by SI. Download of videos by plugging directly in to the mNVR should not be possible. All videos stored in the mNVR should be encrypted.

The cameras shall also embed the time stamp (in IST) on the captured video and shall sync regularly using a time server.

The camera shall report back to the VMS on the following statuses at regular intervals:

- Camera availability and alerts on disconnection / failure
- Storage availability and alerts on failure
- Time server synchronization status

Viewing of feeds shall primarily be on the following:

a. Remote PC viewing
b. Mobile viewing
c. Video wall

5.6.3 Minimum Technical Specifications

5.6.3.1 IP Camera

S.No	Parameter	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
1.	Product details-			
2.	Please mention Make Model No. or Part Code			
3.	Image sensor and Effective Pixels (Resolution)	1/3″ Progressive Scan CMOS		
4.	Lens	2.8mm / 3.6mm / 4mm (as per SI survey for appropriate coverage)		
5.	Min. Illumination	0.5Lux@F1.2		
6.	WDR	up to 100 db		

S.No	Parameter	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
7.	Electronic Shutter	1/5~1/45500s		
8.	Day/Night	ICR Filter Auto Switch		
9.	Max. Image Resolution	1920x1080		
10.	Frame Rate	30fps(1920x1080), 30fps(1280x960), 30fps(1280x720), 30fps(704x576)		
11.	Video Compression	H.265 / H.264		
12.	Ethernet	1*RJ45 10M/100M Ethernet Port		
13.	Protocol	IPv4, TCP, UDP, RTP, RTSP, RTCP, HTTP, HTTPS, DNS, DDNS, DHCP, FTP, NTP, SMTP, SNMP		
14.	Alarm I/O	1/1		
15.	SD Card Support	minimum 128 GB		
16.	Event Action	FTP Upload/ SMTP Upload/ SD Card Record/ External Output		
17.	Working Temperature	0ºC to 55ºC.		
18.	Power Supply	Automotive Grade Power Supply		
19.	Weather Proof	IP67, IK10		
20.	Certification	CE / FCC / UL / BIS certification		

5.6.3.2 GPS Device with Panic Buttons (4Nos) AS140 Complaint

S.No	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
1.	Product details-		
2.	Please mention Make Model No. or Part Code		
3.	GPS / GNSS		
4.	GPS & GSM Internal Antenna		
5.	Features: • Up to 45000 Location Records • FOTA • Programmable Update Frequency		

S.No	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
	• Main Power and Ignition Status • GPS and Pulse Odometer • TCP/HTTP/HTTPS/UDP • Password Protection • SMS/GPRS/SERIAL Configuration • SIM Lock, DNS, Angle Tracking, Distance Tracking		
6.	Input / outputs: 2xDigital Input, 2xDigital Output, 1xAnalog Input, 2xSerial Ports, 15 Pin Connector		
7.	IP Rating: IP65;		
8.	Working Temperature: 0°C to 55°C		
9.	Power Supply • Operational: 12V, 24V • Maximum: 40V • Range: 7V~40V		
10.	Alert Types: • Panic Alerts • Main Power Removal Alerts • Tamper Alerts • SIM Change Alerts • Over Speed Alerts • Ignition Alerts • SMS Alerts • Tilt Alert		
11.	Panic Buttons (4 Nos) • Plastic transparent cover with LED Push-Button in Red Color • Stainless Steel Face Plate with GI Junction box • AS140 Compliance • Contact Resistance : 100m Ohms • IK10 and IP66 rated		

5.6.3.3 4 Channel mobile NVR with minimum 30 Days Storage

S.No	Parameter	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
1.	Product details-			

S.No	Parameter	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
2.	Please mention Make Model No. or Part Code			
3.	Camera Input	4 channel		
4.	Resolution	8MP(4K),1080p, UXGA,960p,720p, XGA,SVGA,D1,CIF,QCIF		
5.	Compression	H.264/H.265		
6.	Bitrate	64kbps~16384kbps		
7.	Recording Bandwidth	Max 64 Mbps		
8.	Local Display	1xHDMI,1xVGA,2xCVBS, Simultaneously output same content		
9.	Layout	1,4,9,16		
10.	Function	E-PTZ/Scheme/Polling		
11.	Resolution	1080p,UXGA,960p,720p, XGA,SVGA,D1,CIF,QCIF		
12.	Recording frame rate	Full HD (1920 x1080) @30 fps		
13.	Recording Mode	Manual/Continuous/Schedule/Event(Pre/Post)		
14.	Event Trigger	Supported		
15.	Tag	Supported		
16.	Search Mode	Date and time (Calendar)/ Event		
17.	Playback Resolution	1080p,UXGA,960p,720p, XGA,SVGA,D1,CIF,QCIF		
18.	Playback (Local Monitor & Client)	4 x 1080p@30fps		
19.	Synchronize Playback	4 x 1080p@30fps		

S.No	Parameter	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
	(Local Monitor & Client)			
20.	Function	Slow forward/ Fast forward/ Loop/ Single frame/E-PTZ		
21.	SATA Ports	2x2.5''HDD		
22.	Audio Compression	G.711a/G.711u/ADPCM/ G.722/G.722.1c/ AAC-LC/G.726		
23.	Bitrate	32kbps~64kbps		
24.	Audio Function	Bi-directional audio/ Dumb/Mute/Broadcasting		
25.	Service Alarm Triggers	Alarm input/Video lost/Motion detection/Tampering/ Guard line/Defocus/ Scene change/ Enter guard area/ Exit guard area/ Object left/Object removal/ Gathering/Audio surge		
26.	System Alarm Triggers	Device disconnected/ No disk/ Disk error/ IP Address conflict/ Network fault/ Insufficient recording space/ MAC address conflict/ Insufficient snapshot space/ Unauthorized access		
27.	Alarm Events	Snap shot/ Recording/ PTZ preset/ Buzzer/ Email/Link to Client/ Alarm caption/ Live view in first window/Link to TV Wall/ Full screen viewing		
28.	Operating System	Embedded Linux		
29.	User Management	Admin/ User		
30.	Log Management	User login/ User operation/Alarm/ Backup/Update		
31.	Network Protocols	TCP/IP, UDP,HTTP,DHCP,DNS/ DDNS,RTP/ RTCP, RTSP, PPPoE, FTP,SNTP,VSIP,UPNP,SMTP,IPv 4,IPv6		

S.No	Parameter	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
32.	Viewer Software	Web		
33.	Max. User Access	16 Users		
34.	Function	NAT/ Socks5/Multiple network access/Packet loss recovery		
35.	Network Test	Supported		
36.	Wireless	Wi-Fi, 3G/ 4G		
37.	Number of SIM card Slots	Default 1,upto 2		
38.	3G/4GFrequency Band	FDD-LTE: B1/B2/B3/ B5/B7/B8 /B20 TDD-LTE:B38/B39/B40/B41 HSPA/UMTS:850/900/1800/1900/2100MHzGS M/GPRS/EDGE:850/900/1800/1900MHzTD- SCDMA: B34/B39 EVDO/CDMA: BC0/BC1		
39.	Wi-Fi	802.11b/g/n/a/ac 2.4G/5G,Wi-FiAP		
40.	Location Technology	GPS		
41.	Application Programming	ONVIF (Profile S, Profile G),API,CGI		
42.	Ethernet	1x10/100M, RJ45 interface		
43.	AudioIn/Out	1x Linein/1 x Mic in/1x Lineout		
44.	Aviation Plug	4x10pin:4x PoE input 1x4 pin:2x CVBSoutput 1x4pin:Power supply for PTZ camera 1x9 pin: Power input9~ 36VDC		
45.	Video Out	1xHDMI / 1xVGA		

S.No	Parameter	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
46.	PoE Camera Input	4 channel with M12/M23 connector		
47.	Alarm In/Out	4x Input / 4 x Output		
48.	Network Detection	Automatic		
49.	Antenna	Wi-Fi Antenna interface, GNSS Antenna interface,4G Antenna interface		
50.	Control / IO	1xRS485 / 1xRS232 (serial Interface), 2xDigital Input, 2xDigital Output		
51.	USB	2 Ports		
52.	Operating Temperature	0ºC to 55ºC.		
53.	Operating Humidity	10%~90% Non-Condensing		
54.	Electrical Power	DC9~36V		
55.	Power Consumption	Max.96W		
56.	Certificates	CE / FCC / UL / BIS certification		

5.6.3.4 4 Port PoE Switch (in case of External Switch)

S.No	Parameter	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
1.	Product details-			
2.	Please mention Make Model No. or Part Code			
3.	Technology	PoE		
4.	Number of 1G Copper Ports	4		
5.	Switching Capacity -Non Blocking (Gbps)	20		
6.	Throughput (MPPS)	14.9		

S.No	Parameter	Minimum Specification	Compliance (Yes / No)	Deviations (if any)
7.	Security Feature	SSH v1/v2 SSL v2/v3/TLSv1 Port Security Broadcast/Multicast/ Unicast Storm Control 802.1		
8.	Management Protocol	Web-based GUI and CLI management SNMP v1/v2c/v3, compatible with public MIBs		
9.	QoS	Support 802.1p CoS/DSCP priority Support 8 priority queues Queue scheduling: SP, WRR		
10.	Operating Temperature Range	0ºC to 60ºC.		
11.	Operating Humidity (RH)(%)	90		
12.	IPv6 Ready from day one and dully certified	Yes		

5.7 Network

Network Connectivity is one of the most important components of the project and needs detailed 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.

The entire network connecting field locations to Command and Control Centre (CCC) and CCC to DC/DR shall be provided by the SI. All the above mentioned Offices will be connected to Data Centre for Live viewing and retrieval of stored video footage as and when require for evidence.

- It is envisaged that the network connectivity shall be provided via 4G / 5G / RF based network though which status updates will be continually transmitted
- The System Integrator will have to procure the required mobile connectivity (in case of 4G / 5G) from a Telecom Service Provider with required bandwidth as per the proposed solution
- The video feeds from the Bus will be securely transported to the CCC @ minimum 5 FPS in optimised resolution in addition to on premises storage @ minimum 20 FPS in mNVR for bus and the alarm data will be transmitted at minimum 20 FPS.
- The video feeds from the Depots and Terminals will be securely transported to the CCC @ minimum 20 FPS in optimised resolution in addition to on premises storage in NVR.
- All Alarm data to be stored at CCC for 365 Days
- CCC will be connected to DC/DR cloud and shall store back up for disaster recovery as well on cloud

5.7.1.1 Information to be analyzed at the CCC / Viewing Stations

The proposed Video Management System shall provide a complete end-to-end solution for security surveillance application. The Bidder has to provide VMS client software at the Control centre to monitor and manage all the surveillance cameras which is part of the Safe city initiative.

The control centre shall allow an operator to view live / recorded video from any camera on the IP Network. The combination of control centre and the IP Network would create a virtual matrix, which would allow switching of video streams around the system.

Not all the cameras would be simultaneously viewed at the CCC. The CCC shall from time to time take decisions on utilization of Alerts / Exceptions / Triggers generated by alerts engine, and specify the client machines where these would get populated automatically.

MTC shall have following access to the video feeds of the cameras of their jurisdiction:

- Viewing rights to all the live Camera Feeds at the Control Room / Respective field offices
- Viewing rights to the stored feeds at the Control Room / Respective field offices
- Access to view Alerts / Exceptions / Triggers raised
- Trail Report on specific person / object / vehicle for a specific period / location

- Personalized Dashboard (depending upon grade of police officer)
- Accessibility to advanced analytics on recorded footages
- Provide search of recorded video. Advanced search should be possible based on various filters like alarm / event, area, camera, etc.

5.7.1.2 Control Centre Requirements

- Alarm Monitor

Alarm Monitors must show the name of alarms when generated. The layout must not be restrictive

- Customizable and programmable Event Response Mechanism

All the Event Response Mechanisms must be customizable based upon functional parameters like criticality, region, access, automatic/manual etc. (not limited to these four). SOPs for the daily incident management to be designed and approved by MTC and same must be implementable in the system.

System must allow generation of reports for all Incidents based upon filters like Criticality, Current Status, Date / Time (not limited to these). System to support excel/pdf for export.

Dashboards generated by the system (functional / technical) must be customizable based upon the user's requirements. The system must remember the edits done by the user to his/her own dashboard when he logins next time in the system.

System should allow generation of Audit Reports for the perusal of concerned MTC personnel.

5.7.1.3 Other General Requirements

5.7.1.3.1 Management / Integration functionality

- The Surveillance System shall offer centralized management of all devices, servers and users.
- The Surveillance System should not have any limit on the number of cameras to be connected for Surveillance, Monitoring and recording. Any increase in the no. of cameras should be possible.
- The Surveillance System shall support distributed viewing of any camera in the system using Video walls or big screen displays.
- The Surveillance System shall support alerts management. The alerts management shall allow for the continuous monitoring of the operational status and event-triggered alerts from system servers, cameras and other external devices.
- It should be possible to integrate the Surveillance System with 3rd-party software, to enable the users to develop customized applications for enhancing the use of video surveillance solution. For e.g., integrating alert management to initiate SMS, E-Mail, VoIP call etc.

- The Management system shall store the overall network elements configuration in central database, either on the management server computer or on a separate DB Server on the network.
- System should be able to be integrated with Event Management / Incident Management System.

5.7.1.3.2 *System Administration functionality*

- The System Administration Server shall provide a feature-rich administration client for system configuration and day-to-day administration of the system.
- The System Administration Server shall support different logs related to the Management Server.
  - The System Log
  - The Audit Log
  - The Alert Log
  - The Event Log
- Rules

  The system shall support the use of rules to determine when specific actions occur. Rules shall define what actions shall be carried out under specific conditions. The system shall support rule initiated actions such as:
  - Start and stop recording
  - Set non-default live frame rate
  - Set non-default recording rate
  - Start and stop PTZ patrolling
  - Send notifications via email
  - Pop-up video on designated Client Monitor recipients

5.7.1.4 Client system

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

- Viewing live video from cameras on the surveillance system
- Browsing recordings from storage systems
- Creating and switching between multiple of views.
- Viewing video from selected cameras in greater magnification and/or higher quality in a designated hotspot.
- Controlling PTZ cameras.
- Using digital zoom on live as well as recorded video.
- Using sound notifications for attracting attention to detected motion or events.
- Getting quick overview of sequences with detected motion.
- Getting quick overviews of detected alerts or events.
- Search using a indexed database of commonly available objects (vehicles, buildings, trees etc) & people (gender, type and colour of clothes, age, etc) in order to assist in easy retrieval of video footage based of these parameters.

5.7.1.5 Web/Mobile Client

1. The client shall offer live view, including PTZ control (if applicable) and event / output activation. The Playback function shall give the user concurrent playback of multiple recorded videos with date, alert sequence, time searching, smart search, etc.
2. The client shall provide the ability to search / select cameras from a GIS layer. It should also provide the ability to search for nearby cameras based on the users' current location
3. It should have support for push notifications based on alerts generated from the VMS
4. It should provide the users the ability to take a picture and run a image search across feeds from (nearby) cameras
5. User Authentication – The Remote Client shall support logon using the user name and password credentials
6. The client shall access the H.264/H.265/VP9/MJPEG/MPEG4 live stream from the cameras directly or through the data centre

5.7.1.6 Matrix Monitor

- Matrix Monitor – The Matrix Monitor feature shall allow distributed viewing of multiple cameras on the system on any monitor
- The Matrix Monitor feature shall access the H.264/H.265/VP9/MJPEG/MPEG4 live stream from the cameras directly or through the data centre

5.7.1.7 Alert Management Module

- The alert management module shall allow for continuous monitoring of the operational status and event-triggered alerts from various system servers, cameras and other devices. The alert management module shall provide a real-time overview of alert status or technical problems while allowing for immediate visual verification and troubleshooting.
- The alert management module shall provide interface and navigational tools to the client including;
  - Graphical overview of the operational status and alerts from servers, network cameras and external devices including motion detectors and access control systems.
  - Intuitive navigation using a map-based, hierarchical structure with hyperlinks to other maps, servers and devices or through a tree-view format.
- The module shall include flexible access rights and allow each user to be assigned several roles where each shall define access rights to cameras.
- VMS should be capable to accept third party generated events / triggers
- In case of memory / storage failure for cameras, the camera shall generate an alert which in turn can generate helpdesk tickets automatically for restoration of the functionality. The VMS shall be capable of handling such alerts

5.7.1.8 Other Miscellaneous Requirements

- System should have a facility to create CDs or other storage media for submission to Judiciary, which can be treated evidence for legal matters. Such storage media creation should be tamper proof and SI to provide appropriate technology so that integrity and quality of evidence is maintained as per requirements of the judiciary. Bidder is required to specify any additional hardware / software required for this purpose. SI will also prepare the guideline document to be followed by the Police Personnel for the retrieval of Video / images from the CCTV System so as to maintain integrity of the evidence. Such a guideline document should include methods of retrieval of data, check-list to be followed and flowchart of the entire process to be followed.
- All the systems proposed and operationalization of Video Management System should comply with requirements of IT Acts.
- Bidder shall be required to provide a standardized Mobile Application to integrate smart phones and tablets for 2-way communication with the Video Management System in a secure manner. MTC personnel may be allowed to use their existing tablets / smart phones. It will be the responsibility of SI to configure such tablets / Smartphones with the Surveillance System and ensure that all the necessary access is given to these mobile users so that uploading of video / pictures to the surveillance system is possible.
- Surveillance camera feeds from national highway Toll plaza, private residence, hospital places of large public gathering, Etc. needs to integrated to CC solution
- There shall be a provision for the third party audits once in 6 months.

5.7.1.9 Video Management System

Video management system shall constitute of a platform which will be designed for viewing, recording and replaying acquired video as part of overall project solution. This platform will be based on the Internet Protocol (IP) open platform concept. Major functionalities are described here:

5.7.1.9.1 VMS Overview

1. VMS shall be used for centralized management of all field camera devices, NVRs, video servers and client users
2. VMS server shall be deployed in a clustered server environment/Support in built for high availability and failover for directory & recording servers
3. VMS shall support a flexible rule-based system driven by schedules and events.
4. VMS shall be supported for fully distributed solution for monitoring and control function, designed for limitless multi-site and multiple server installations requiring 24/7 surveillance with support for devices from different vendors.
5. VMS shall support internet protocol (IP) cameras from major vendors.
6. The Contractor shall clearly list in their proposal the make and models that can be integrated with the VMS, additionally all the offered VMS and cameras must have Open Network Video Interface Forum (ONVIF) compliance.

7. VMS shall be enabled for any standard storage technologies and video wall system integration.
8. VMS shall be capable of being deployed in a virtualized server environment without loss of any functionality.
9. All CCTV cameras locations shall be overlaid in graphical map in the VMS Graphical User Interface (GUI). The cameras selection for viewing shall be possible via clicking on the camera location on the graphical map. The graphical map shall be of high resolution enabling operator to zoom-in for specific location while selecting a camera for viewing.
10. VMS shall have an administrator interface to set system parameters, manage codecs, manage permissions and manage storage.
11. The day to day control of cameras and monitoring on client workstations shall be controlled through the administrator interface.
12. Whilst live control and monitoring is the primary activity of the monitoring workstations, video replay shall also be accommodated on the GUI for general review and also for pre- and post-alarm recording display.
13. The solution design for the VMS shall provide flexible video signal compression, display, storage and retrieval.
14. All CCTV camera video signal inputs to the system shall be provided to control centre, various viewing centres etc., and the transmission medium used shall best suit the relative camera deployments and access to the CCTV Network.
15. VMS shall be capable of transferring recorded images to recordable media (such as CD/DVD and/or tapes) in tamper evident and auditable form. All standard formats shall be supported including, but not limited to:
    a) AVI files
    b) MP4 Export or latest
16. For Video Exports with VMS's Native Format along with Watermark and Encrypted with SSL / TSL technology, one can protect the video tampering and prove that the video is not tampered
17. All streams to the above locations shall be available in real-time and at full resolution. Resolution and other related parameters shall be configurable by the administrator in order to provide for network constraints.
18. The VMS shall support various settings. Each channel configured in the VMS shall have an individual setup for the following settings, the specific settings shall be determined according to the encoding device:
    a) Brightness
    b) Contrast
    c) Color
    d) Sharpness
    e) Saturation
    f) Hue
    g) White balance
19. The VMS shall support the following operations:
    a) Adding an IP device

b) Updating an IP device
c) Updating basic device parameters
d) Adding/removing channels
e) Adding/removing output signals
f) Updating an IP channel
g) Removing an IP device
h) Enabling/disabling an IP channel
i) Refreshing an IP device (in case of firmware upgrade)

20. The VMS shall support retrieving data from edge storage. Thus when a lost or broken connection is restored, it shall be possible to retrieve the video from edge storage and store it on central storage.
21. In case of memory / storage failure, the camera shall generate and alert which in turn can generate helpdesk tickets automatically for restoration of the functionality. The VMS shall be capable of handling such alerts
22. The VMS shall support bookmarking of videos. Thus, allowing the users to mark incidents on live and/or playback video streams.
23. VMS shall support automatic failover for recording. Some Critical cameras shall also be supported for Redundant (Mirrored Recording simultaneously)
24. VMS shall support manual failover for maintenance purpose.
25. VMS shall support access and view of cameras and views on a smartphone or a tablet (a mobile device).
26. VMS shall support integration with the ANPR application
27. VMS shall support integration with other online and offline video analytic applications.
28. VMS shall be able to accept alerts from other third party systems, sensors etc.
29. VMS shall support manual failover of Directory for maintenance purpose
30. System should support recording management to view the recordings available on a camera's local storage device (such as an HDD, SD card, etc.), and copy them to the server.
31. The VMS shall support replacement of the edge device with another device, while maintaining past recordings according to the defined retention period and device logical entities association (triggers association, pages, etc.)
32. The VMS shall support LoS (Level of Service) mechanism, choosing between several video streams according to its performance parameters and networking capabilities of the workstation and/or decoder.
33. The VMS recorders' performance shall support 100% of recording channels, 30% of the channels with live monitoring and 20% of the channels with playbacks all at the same time.

5.7.1.9.2 Client system

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

1. Viewing live video from cameras on the surveillance system
2. Browsing recordings from storage systems

3. Creating and switching between multiple of views.
4. Viewing video from selected cameras in greater magnification and/or higher quality in a designated hotspot.
5. Using digital zoom on live as well as recorded video.
6. Using sound notifications for attracting attention to detected motion or events.
7. Getting quick overview of sequences with detected motion.
8. Getting quick overviews of detected alerts or events.
9. Search using a indexed database of commonly available objects (vehicles, buildings, trees etc) & people (gender, type and colour of clothes, age, etc) in order to assist in easy retrieval of video footage based of these parameters. – smart search
10. The VMS shall use its own streaming server to efficiently steam the videos.
11. When the VMS client is set to view the live videos in say 4x4, 5x5 and 8x8 grids, the VMS should display lower resolution, high frame rate video to avoid high bandwidth and CPU usage on the VMS client
12. When the user selects a particular camera, and wants to view it in full screen, the VMS should automatically show the highest quality and high frame rate video.

5.7.1.9.3 Web / Mobile Client

1. The client shall offer live view, including PTZ control (if applicable) and event / output activation. The Playback function shall give the user concurrent playback of multiple recorded videos with date, alert sequence, time searching, smart search, etc.
2. The client shall provide the ability to search / select cameras from a GIS layer. It should also provide the ability to search for nearby cameras based on the users' current location
3. It should have support for push notifications based on alerts generated from the VMS
4. It should provide the users the ability to take a picture and run a image search across feeds from (nearby) cameras
5. User Authentication – The Remote Client shall support logon using the user name and password credentials
6. The client shall access the H.264/H.265/VP9/MJPEG/MPEG4 live stream from the cameras directly or through the data centre

5.7.1.9.4 Alert Monitoring

1. The VMS shall allow for continuous monitoring of the operational status and event-triggered alerts from various system servers, cameras, and other devices. It shall provide a real-time overview of alert status or technical problems while allowing for immediate visual verification and troubleshooting.
2. It shall provide interface and navigational tools through the client including but not limited to:
   - Graphical overview of the operational status and alerts from servers, network cameras and external devices including motion detectors and access control systems.

- Intuitive navigation using a map-based, hierarchical structure with hyperlinks to other maps, servers and devices or through a tree-view format.
- It shall include flexible access rights and allow each user to be assigned several roles where each shall define access rights to cameras.
- Basic VMS should be capable to accept third party generated events / triggers

5.7.1.9.5 Other functionality

1. The Surveillance System shall offer centralized management of all devices, servers and users.
2. The Surveillance System should not have any limit on the number of cameras to be connected for Surveillance, Monitoring and recording. Any increase in the no. of cameras should be possible by augmentation of Hardware components.
3. The Surveillance System shall support distributed viewing of any camera in the system using Video walls or big screen displays.
4. It should be possible to integrate the Surveillance System with 3rd-party software, to enable the users to develop customized applications for enhancing the use of video surveillance solution. For e.g., integrating alarm management to initiate SMS, E-Mail, VoIP call etc.
5. System should be able to be integrated with PSIM / Incident Management System.
6. The System Administration Server shall provide a feature-rich administration client for system configuration and day-to-day administration of the system.
7. The System Administration Server shall support different logs related to the Management Server.
    a) The System Log
    b) The Audit Log
    c) The Alert Log
    d) The Event Log
8. Rules: The system shall support the use of rules to determine when specific actions occur. Rules shall define what actions shall be carried out under specific conditions. The system shall support rule initiated actions such as:
    a) Start and stop recording
    b) Set non-default live frame rate
    c) Send notifications via email
    d) Pop-up video on designated Client Monitor recipients

- Security Platform shall have strong security mechanism such as the use of advance encryption, digital certificates and claims-based authentication to ensure that only authorized personnel have access to critical information, prevent man-in-the-middle attacks, and that the data is kept private.
- System should support Report and View Open Incident Cases. This also support associating the video footages pertaining to the incident either received from City CCTV Cameras or shared by public to the police agency. This also allows viewing and downloading and delete Incident clips that are stored on the server by the administrator.

5.7.1.9.6 Failover & Redundancy

1. Synchronized Failover directory feature should be provided with the offered system to avoid the single point of failure. Also the system should sustain all its current operations i.e. recording, playback and live video even in the event of primary as well as failover directory failure. This functionality can either be loaded on any of the recording server or on a dedicated server. If offered software need dedicated server for this, then the same will be in contractor's scope. Specifications of failover administration server should be same as that of recording server except storage size.
2. Automated Failover recording should be provided to maintain the reliability of the system. In case of failure of one or more of primary recording servers simultaneously. Additional servers/storage required to meet this requirement should be in Contractors scope.
3. Redundant recording/Dual recording feature of the VMS should be supported by VMS. System administrator should get the privilege to configure this feature on any cameras simultaneously depend on the criticality of the cameras.
4. The VMS shall allow for 2-way audio communication using amplifier/call station connected the IP cameras in the field without any need of audio cabling from camera to control room – applicable for locations with PA systems

6 Common guidelines / comments regarding the compliance of IT / Non-IT Equipment / Systems to be procured

- The specifications mentioned for various IT / Non-IT components are indicative requirements and should be treated for benchmarking purpose only. Bidders are required to undertake their own requirement analysis and may propose higher specifications that are better suited to the requirements.
- Any manufacturer and product name mentioned in the RFP should not be treated as a recommendation of the manufacturer / product.
- None of the IT / Non-IT equipment proposed by the bidder should be End of Life product. It is essential that the technical proposal is accompanied by the OEM certificate in the format given in this RFP, where-in the OEM will certify that the product is not end of life product & shall support for at least 84 months from the date of Bid Submission.
- Technical Proposal should be accompanied by OEM's product brochure / datasheet. Bidders should ensure complete warranty and support for all equipment from OEMs. All the back-to-back service agreements should be submitted along with the Technical Bid.
- All equipment, parts should be Original and New.
- The User Interface of the system should be a User Friendly Graphical User Interface (GUI).
- Critical / Core components of the system should not have any requirements to have proprietary Platforms and should conform to open standards.

- For the custom made modules, Industry standards and norms should be adhered to for coding during application development to make debugging and maintenance easier. Object oriented programming methodology must be followed to facilitate sharing, componentizing and multiple-use of standard code. The application shall be subjected to Application security audit to ensure that the application is free from any vulnerability.
- The Successful Bidder should also propose the suitable specifications of any additional servers / other hardware, if required for the system.
- The Servers provided should meet industry standard performance parameters (such as CPU Utilization of 60% or less, disk utilization of 75% or less).
- SI is required to ensure that there is no choking point / bottleneck anywhere in the system (end-to-end) to affect the performance / SLAs.
- All the hardware and software supplied should be from the reputed Original Equipment Manufacturers (OEMs). MTC reserves the right to ask replacement of any hardware / software if it is not from a reputed brand and conforms to all requirements specified in tender documents.
- All necessary hardware, software, licenses etc. will be in the name of MTC. In case of Custom-built bespoke application, the IPRs shall also be transferred to MTC.
- Successful bidder shall make the details of new technologies, new hardware available in the market to MTC. Both, MTC and SI, in agreement, will take decision of new technology/ hardware implementation in case any new/ advanced technology comes up during the contract period.

7 Payment Terms & Payment Schedule

7.1 Payment Terms

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 submitted pursuant to general conditions of the contract and upon fulfilment of all the obligations stipulated in the Contract.

Due payments shall be made by the Authority, after submission of an invoice or request for payment by System Integrator (Lead Bidder)

The currency or currencies in which payments shall be made to the System Integrator (Lead Bidder) under this Contract shall be Indian Rupees (INR) only.

Remittance charges, if any, shall be borne by the System Integrator (Lead Bidder).

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, as applicable, shall be deducted / paid, as per the prevalent rules and regulations

7.2 Payment Schedule

Payments to SI, after successful completion of the target milestones (including specified project deliverables), shall be made as under:

- T is the date of signing of contract
- G is the date of Go Live of the CCC solution & also marks the commencement of O&M Phase (the exact date of commencement of O&M shall be decided by MTC)

#	Milestone	% Payment
1.	Solution Design Sign-off	10% of CAPEX
2.	Supply of all ICT & Non-ICT infrastructure for the Surveillance Solution **Note:** Minimum cumulative Bill Value against product supply shall not be less than INR 2 Crores.	35% of CAPEX
3.	Installation of all ICT & Non-ICT infrastructure for the Surveillance Solution	35% of CAPEX
4.	Unit Testing by System Integrator	5% of CAPEX
5.	Final Acceptance Testing	5% of CAPEX
6.	Solution stabilization & Go-Live	5% of CAPEX
7.	Quarterly Payments - Operations & Maintenance Phase for a period of 3 years	OPEX equally amortized across 12 quarters
8.	36th month – Project Closures Exit Management	Remaining 5% of CAPEX

8 Annexures

8.1 Annexure 1 – Matrix for Scope of Work

#	Key Activities	Deliverables	CCC	Surveillance
	Project Inception Phase			
1.	Project Kick Off	1. Project Development Plan 2. Risk Management and Mitigation Plan	Yes	Yes
2.	Deployment of manpower		Yes	Yes
	Requirement Phase			
3.	Assess the requirement of IT Infrastructure and Non IT Infrastructure	1. Functional Requirement Specification Document 2. System Requirement Specification document 3. Requirements Traceability Matrix 4. Site Survey Report	Yes	Yes
4.	Assessment of Business processes		Yes	Yes
5.	Assessment of Software requirements		Yes	Yes
6.	Assess the Integration requirements		Yes	Yes
7.	Assess the connectivity requirement all locations (including Building)		Yes	Yes
8.	Assessment the Network laying requirement		Yes	Yes
9.	Assessment of training requirement		Yes	Yes
	Design Phase			
10.	Formulation of Solution Architecture	1. Final Bill of Quantity 2. HLD documents 3. LLD documents 4. Application architecture documents. 5. Technical Architecture documents. 6. Network Architecture documents. 7. ER diagrams and other data modeling documents.	Yes	Yes
11.	Creation of Detail Drawing		Yes	Yes
12.	Detailed Design of Safe City Solution		Yes	Yes
13.	Development of test cases (Unit, System Integration and User Acceptance)		Yes	Yes
14.	Preparation of final bill of quantity and material		Yes	Yes

#	Key Activities	Deliverables	CCC	Surveillance
15.	SoP preparation	8. Logical and physical database design. 9. Data dictionary and data definitions. 10. GUI design (screen design, navigation, etc.). 11. Test Plans 12. SoPs 13. Change management Plan	Yes	
	Development Phase			
16.	CCC setup	1. IT and Non IT Infrastructure Installation Report 2. Completion of UAT and closure of observations report 3. Training Completion report 4. Application deployment and configuration report	Yes	
17.	Physical Infrastructure setup		Yes	Yes
18.	Procurement of Equipment , edge devices, Commercial Of The Shelf (COTS) software (if any), Licenses		Yes	Yes
19.	IT and Non IT Infrastructure Installation		Yes	Yes
20.	Development, Testing and Production environment setup		Yes	Yes
21.	Software Application customization (if any)		Yes	Yes
22.	Development of Bespoke Solution (if any)		Yes	Yes
23.	Integration with Third party services/application (if any)		Yes	
24.	Unit and User Acceptance Testing		Yes	Yes
25.	Implementation of Solutions		Yes	Yes
26.	Preparation of User Manuals , training curriculum and training materials		Yes	Yes
27.	Role based training(s) on the Safe City Solutions		Yes	Yes
	Integration Phase			
28.	SoP implementation	1. Integration Testing Report	Yes	Yes

#	Key Activities	Deliverables	CCC	Surveillance
29.	Integration with GIS		Yes	Yes
30.	Integration of solutions with Control Centre			Yes
	Go -Live			
31.	Go Live	1. Go-Live Report	Yes	Yes
	Operation and Maintenance			
32.	Operation and Maintenance of IT, Non IT infrastructure and Applications	1. Detailed plan for monitoring of SLAs and performance of the overall system 2. Fortnightly Progress Report 3. Monthly SLA Monitoring Report and Exception Report 4. Quarterly security Report 5. Issues logging and resolution report	Yes	Yes
33.	SLA and Performance Monitoring		Yes	Yes
34.	Logging, tracking and resolution of issues.		Yes	Yes
35.	Application enhancement		Yes	Yes
36.	Patch & Version Updates		Yes	Yes
37.	Helpdesk services		Yes	Yes

8.2 Annexure 2 –: Indicative list of locations

The below list of locations is only indicative. MTC reserves the right to change the quantity or the location during the implementation phase.

S.No.	Place	Depot Area in acres	Terminus Area in acres	Latitude/Longitude
1	Adambakkam	1.52	0.50	**12.994890, 80.206690**
2	Adyar	5.635		**12.998189, 80.256461**
3	Alandur	3.37		**12.997006, 80.191718**
4	Ambattur Industrial Estate	3.56	0.66	**13.099555, 80.169956**
5	Anna Nagar West	5.80	1.36	**13.093802, 80.198147**
6	Avadi	3.79	1.89	**13.121380, 80.102082**
7	Ayanavaram	6.92	0.82	**13.098746, 80.241035**
8	Ayyapanthangal	2.78	1.52	**13.037233, 80.134635**
9	Basin Bridge	1.005		**13.102701, 80.273682**
10	Besant Nagar	0.55	0.40	**13.000343, 80.265937**
11	Central Depot	7.396		**13.075840, 80.275799**
12	Chemmencheri.		0.93	**12.874693, 80.209872**
13	Chrompet I	20.00		**12.947442, 80.140920**
14	Chrompet II	7.13		**12.947509, 80.144356**
15	Ennore	1.74	0.96	**13.215657, 80.320770**
16	K.K Nagar	3.86	2.10	**13.034841, 80.205415**
17	Kundrathur	2.78		**12.980404, 80.102187**
18	M.K.B Nagar	0.92	0.45	**13.123110, 80.265690**
19	Madhavaram	4.60		**13.131771, 80.236474**
20	Mandaveli	0.74	0.70	**13.026362, 80.266311**
21	Padiyanallur	3.28	0.77	**13.203698, 80.174104**
22	Perambur	7.98		**13.102234, 80.249026**
23	Poonamallee	5.40		**13.052055, 80.090679**
24	Saidapet	2.06		**13.014439, 80.225685**
25	Tambaram	4.91		**12.932504, 80.121025**
26	Theyagaraya Nagar	0.80	1.17	**13.034499, 80.230046**
27	Thiruvanmiyur	1.39	1.56	**12.986873, 80.259291**
28	Thiruvottiyur	1.79	0.71	**13.172324, 80.304347**
29	Tondairpet I	5.83		**13.131906, 80.292436**
30	Tondairpet II with Workshop	6.67		**13.135094, 80.290183**
31	Vadapalani	5.73	0.94	**13.050470, 80.206876**
32	Vyasarpadi	5.73		**13.120182, 80.259245**
33	Kannagi Nagar	1.77	0.63	**12.925528, 80.238407**
34	Perumbakkam	3.40	1.60	**12.886605, 80.210028**
35	Adyar Gandhi Nagar		1.15	**13.006810, 80.253009**

36	Dr.J.J.Nagar East		0.86	**13.080365, 80.180740**
37	Dr.J.J.Nagar West		1.00	**13.082514, 80.170347**
38	Foreshore Estate		1.40	**13.022420, 80.276322**
39	High Court		0.57	**13.086088, 80.285050**
40	Kannadhasan Nagar		1.20	**13.136230, 80.257002**
41	MMDA Arumbakkam		0.69	**13.062470, 80.215189**
42	Perambur		1.12	**13.108660, 80.248143**
43	Periyar Nagar		1.05	**13.116408, 80.224046**
44	Thiruverkadu		1.10	**13.069345, 80.123988**
45	Thiru-vi-ka Nagar		0.432	**13.119913, 80.232445**
46	Tolgate		0.489	**13.143555, 80.296726**
47	Vallallar Nagar		0.92	**13.104337, 80.276214**
48	Villivakkam		0.99	**13.105420, 80.208042**