With a view to address the above issues it is now proposed to implement the following modules under Intelligent Traffic Management System

1. Entry Exit Point Management
2. Corridor Management
3. Red Light Violation Detection
4. Speed Violation Detection
5. Adaptive Traffic Controller System
6. Automatic E Challan System

Following are ICT solutions.

1. Entry Exit Point Management with video based automatic traffic count & classification along with ANPR for all major Entry Exit points to have precise information about vehicle entering, exiting, monitoring and control of traffic in primary city corridor for Traffic Information, management & Control.
2. ATCS system with edge based processing using Local processing units(LPU)
3. Variable Messaging Display integrated with video based speed detection to display the speed information for awareness of drivers
4. Traffic Enforcement System:

   The ITMS shall provide various traffic violation detection use cases using Artificial Intelligence and Deep Learning based technology. It shall provide insights for the traffic planners using innovative dashboards for various parameters such as violations, traffic count, vehicle classification, present and historical trends, comparison of roads or junctions. The ITMS shall serve as a decision support system and provide actionable intelligence to help make the city roads safer and less congested for both motorists and pedestrians.

   The ITMS shall have the components such as Junction Servers (available at a traffic junction or available centrally), Event Aggregation Servers, Management Server and a Database. Each component shall provide failover redundancy. There shall be no dependency on the specific operating system, database software, virtualization platform, storage technology and compute infrastructure.

   The ITMS platform architecture shall allow flexible and modular deployment of software components in a distributed computing architecture. At the same time, it shall allow fully centralized deployment of the software application. The distributed architecture shall support a Junction Server installation in any COTS hardware server suitable for operation as per the respective temperature and environmental conditions at the traffic junction for local processing of the connected video surveillance cameras. The Junction Server should send the traffic events and the metadata to the Events Aggregation servers. The Events Aggregation Server shall manage and aggregate the alerts generated from the Junction Servers spread across various locations. Under the centralized deployment the video feeds shall be processed on the servers at the data center. The platform shall be robust to support on-premise or on-cloud infrastructure.

   It shall be possible to connect the Junction Servers using wireless connectivity such as 3G / 4G or 5G if required, without any dependency on the static public IP addresses. The Junction Servers shall store the violation records and the junction camera video streams locally for the configurable duration.

   The ITMS shall offer business continuity in case of disasters. DC-DR architecture shall support granular control on the data safe-keeping and business continuity with automated two-way synchronization of events, violation records, images, and video clips. It shall be

possible to configure business continuity, data safe -keeping , store archived information on DR .

The ITMS shall have support for Block and Object Storage on cloud platforms. The system shall support pushing the recorded video file on a definable schedule to the Object Storage.

The ITMS shall be built considering the information security risks. It shall have multiple levels of authentication and access control mechanisms such as

A. Role based Authentication

B. Session control using encrypted tokens

C. Restricted user to a particular hardware workstation

D. Multi Factor Authentication with provision to receive the OTP via text message on the registered mobile of the user and through the registered email address and

F. Single sign-on based on LDAP and Active Directory. It shall allow restricting an operator to a single or multiple traffic junction/s and associated cameras.

ITMS must provide necessary software required to meet the security requirements stated above.

All the communication among the servers and clients shall be secured and the ITMS shall support the SSL and TLS communication. It shall have option of encryption with AES 128/ 256 and RSA 1024/2048 encryption standards. It shall support secure communication between the camera and the server using SRTP and RTSP protocols. The ITMS shall have been tested for vulnerabilities and shall have been penetration tested as per the OWASP guidelines. Certificates from the CERT-In empaneled auditor from the respective country of origin clearly indicating the encryption and Vulnerability Assessment and Penetration Testing (VAPT) test shall be available.

To facilitate communication and information collaboration among the operators from various traffic zones, the ITMS shall provide the built-in chat function to exchange the text, image, video clips or any other file from the workstation to other fellow operators or supervisors, thus creating an ad-hoc collaborative environment for incident investigation.

The ITMS shall provide all the use cases and functionalities mentioned in the specifications in a unified platform. The ITMS shall provide the multicasting functionality for monitoring live and archived videos from the unified client. It shall provide an integrated management functionality for camera, recording, traffic violation and incident use cases management and user management for ease of operation.

The ITMS shall be a futuristic solution and shall offer flexibility in distributing the compute at various stages within the architecture to optimize the compute requirements.

System Management Functions

ITMS should have robust system management functions. The ITMS shall provide centralized management of the Junction Servers, aggregation, and processing servers through a unified client interface. The ITMS shall be based on the latest Artificial Intelligence and Deep Learning technologies for continuous improvement of accuracy in generating data by means of analyzing video frames.

At minimum, ITMS shall have:

- User friendly, centralized software update mechanism on Junction Servers based on the schedule.
- Framework to deploy trained model files to all the Junction Servers at a single go.
- Provision to check the performance of various stages in Analytics application deployment pipeline

- Camera-wise status showing processed and dropped frames.
- Total number of events generated in the Junction Servers, total events, event clips and images transferred to the control room servers and events in the queue that are yet to be transferred.
- Dashboard to display storage availability and in the Junction Servers including camera and Junction Servers uptime or SLA reports
- Provision to prioritize the transfer of data from the Junction Server to the central servers. Event Metadata and event images shall be prioritized over the video clips and also prioritize the latest events over the old events.
- Health-dashboard to display CPU and memory utilization status of Junction Server and servers

The ITMS unified client shall show system health alerts for camera, junction server, database server and storage. The drill-down system health shall cover area, junction, to further details of system utilization, major and minor stream, real time bitrate and frames configured for analytics, camera details such as Camera Name, IP Address, Recording Server status showing status of the live recording of the cameras in the central server, list of junctions which are sending live feed etc.
The storage status shall show central storage and all the network drives and utilization of the storage and alert when the total available ITMS storage drops below the configured threshold limit.
The ITMS shall maintain log of various system generated alerts. The system shall also maintain full audit trail in the logs.

Video Handling and General Functions

The Junction Servers shall record the camera streams locally (continuous, event based, schedule based, trigger based) for the duration as per the requirement. The ITMS shall synchronize the recorded video streams from the Junction Servers to the Control Room storage devices. The system shall synchronize such videos in the background depending on the event transfer priority. For example, during the night when there are fewer events generated in the system, the Junction Server shall transfer the recorded video to the Control Room ITMS servers. It shall be possible for the operators to replay the recorded videos stored in Junction Servers on-demand.

The below functionalities should be achieved by ITMS or VMS or integration of both as required.

1. ITMS shall allow recording a matrix of cameras from the operator workstation in a single file to create investigative report as a single video file in case of an event or an accident. It shall be possible to share such a file to the fellow operators or supervisors using a built-in chat function. It shall be possible to search the archive video using date, time, type of event, etc. It shall be possible to view live/archive videos in multiple matrix layout for all the cameras in the system in real time. At least 1x1, 2x2, 3x3, 1+5, 1+7. It shall be possible to cycle multiple layouts with configurable time. A drag and drop functionality shall be supported for viewing cameras on the screen.

2. ITMS shall allow creation of customized, layered maps using standard picture files or GIS maps and it shall be possible to drag and drop the cameras on the map for easy navigation based on the location on the map. It shall be possible to select any camera or group of cameras on the map for live viewing or archive viewing.

3. ITMS shall allow creation of manual events by the operators. from any live camera view using a drop-down menu of various anomalies. Such an event, when stored, shall be searchable based on the camera, time, and event type. It shall be possible to write description about the events.

4. The system shall allow the users to download multiple segments of the video, which are encrypted with password from single or multiple cameras from the archive with an option to tag each downloaded segment with text messages. The Video segments shall be downloaded in a single folder along with excel spreadsheet where details of each of the video segments are listed as hyperlinks to the exported video files.

The system shall provide facility to search for the cases of violations occurred during any specific span of time and provide a statistical analysis of the number of such incidences occurring during various days of the month, various months of the year in graphical format. A report of all such incidences shall be automatically generated by the system in a spreadsheet (.xls, .csv format) and can be automatically emailed to the designated email addresses.

The system shall allow the operator to configure email account and SMS gateway for sharing various alerts through email and SMS.

Data Analytics and Decision Support Functions

The ITMS shall support to implement a data driven ITMS and not a mere transaction based system. ITMS shall be useful to all the stakeholders such as Crime investigation department, Traffic Police and City Planners. The ITMS shall provide various ways to collect and synthesize the data. At minimum it shall be possible to:

- Analyze the frequency of the events and generate notifications on the configurable deviation from the median.
- It shall assist in finding the anomaly than mere violation alerts.
- It shall help extract various attributes for the actors operational on the road for assisting in traffic planning and investigation.
- Show graphical representation of the data generated from the system such as traffic violations by A. type, B. vehicle classes, C. Junction D. Time frame E. Traffic District, F. Traffic Flow, G. Average Speed, H. Headway, I. Private, Commercial, Auto, Electric Vehicles, J. License Plate Quality and classification such as HSRP, Non-HSRP, Dilapidated, No License Plates, etc. It shall allow comparison for a group of junctions (up to three) on these parameters.
- Provide impact analysis of the traffic planning decisions taken such as making a road one-way, blocking turns in a junction, restricting certain classes of vehicles during certain times of the day, restricting lanes for certain classes of vehicles, etc. It shall be possible via a video analysis, synopsis and simulation tool to analyze the before and after effect of the traffic planning decisions. It shall allow entering

information for such decisions and monitor the same on the graph. It shall have ready to use filters – last 1 day, 7 days, 15, days, month, year, etc.

- Plot average count of vehicles or violations on the GIS map. The system shall show traffic violations hotspot on the GIS.
- Provide customized dashboards for various stakeholders with configurable information such as a developing congestion, dropping headway, dropping average speed, increasing violations, etc.
- The system shall make use of the data being generated through the ITMS system for the benefit of the authority as a decision support system. ITMS shall generate an alert on the following conditions:
- When the average speed of any junction drops by the configured threshold (e.g., 20%) as compared to the regular average of last one or two weeks.
- When an average volume of vehicles of any category increases suddenly by the configured threshold (e.g., 20%) as compared to the regular average of last one or two weeks.
- When an overall volume of vehicles increases suddenly by the configured threshold (e.g., 20%) as compared to the regular average of last one or two weeks.
- Detect commercial vehicles having age more than the configured age in years (e.g., 15 years).

Integration Functions

ITMS should have published APIs to interface with external systems such as Integrated Command and Control Application,

The ITMS should have a proven track record in automatically validating the traffic violations based on the ANPR conversion confidence level.

The system should have the capability to integrate with the VAHAN / SARATHI system to fetch vehicle related details as required and as made available by the VAHAN / SARATHI system. It should allow automated and on-demand modes for verification.

The system should provide a query service to the other districts / states to query a particular vehicle if it was seen in the city OR a provision to issue a lookout notice to police which can be fed in the database and any detection of the lookout vehicle should generate an alert.

The system should have integration with the WhatsApp messaging service to share information on the selected groups. The operator should be able to share alert/violation/footage related to an event or a vehicle.

The system should be able to integrate with external systems such as integrated command and control system, C4i systems, IP Speakers, etc.

6.4.12 Entry Exit Point Management:

The City of Puducherry has 4 entry exits and it is proposed to install the Entry & Exit point Management system in the following indicative locations to monitor the Public transportation schedules and Bus timing thru ANPR along with City Entry/Exit.

#	Name

1	ECR Entry
2	Near Accord Pondy
3	Indira Gandhi Junction
4	Cuddalur Exit

The functional/ Technical requirement of the proposed system for entry exit point shall be as follows:

6.4.12.1 ANPR for Entry Exit:

The system shall capture the license plates of the vehicles while capturing the vehicle categories such as cars, Heavy Commercial Vehicles, Three Wheelers, Two Wheelers and Buses and shall store this information along with the license plate information for each transaction in the database. The system shall provide 95% and better detection accuracy and 90% and better license plate conversion accuracy into a text string for Four wheelers and above vehicles for standard reflective license plates.

The system shall categorize the license plates into Good (readable), Bad/dilapidated (partial or fully non-readable), Broken, License Plates without numbers. System shall also provide the license plate conversion confidence percentage. Dashboard with various filters shall also be available with the application. The system shall have the dashboard to view captured vehicles with categories such as private, commercial, electric, and other special vehicles such as military (subject to the availability of training datasets for the special categories) at day time without connecting other systems, e.g vehicles registry database.

The ITMS shall provide the ability to capture vehicles with no number plate, hand-written / fancy number plates, number plates with regional languages.

The system shall have Vehicle Counting and Classification functions using the ANPR and overview cameras.

The system shall detect the colour of all the vehicles on best effort basis, in the camera view during daytime and label them as per the predefined list of configured system colours. The system shall store the colour information of each vehicle along with the license plate information for each transaction in the database.

The system shall store certain license plates of vehicles which are stolen or suspicious with a facility to edit the lists as required including bulk importing functionality. The system shall generate an automatic alert in the control room when it detects the vehicle from the hot list/s through the ANPR camera. It shall be possible to get a trajectory of such/any selected vehicle on a GIS map on demand.

The operator shall be able to edit the license plate number of the vehicle in case it is wrongly captured. The system shall show the captured vehicles with selectable, ANPR conversion confidence. The system shall keep full audit trail of the user actions.

The system shall have function of quickly searching the number plate based on criteria such as full or partial number of the license plate, colour of the vehicle, Speed of the vehicle, Classification of vehicle, Junction Name, etc.

The system shall allow the operator to set traffic rule such as "no heavy vehicles during certain time of the day" for selected traffic junctions/cameras and display in VMD. The system shall identify the heavy vehicles and generate an alert in case the vehicle is violating the rule within the configured time.

The system shall self-analyse the confidence level of the ANPR conversion. In case the confidence level is above user-configured threshold, the violation shall be pushed automatically for traffic ticket generation.

The system shall be flexible to capture the license plates and the traffic violations (subject to the required field of view) from front-side or back-side using a single camera for two lanes at least.

ITMS : Pre Qualification

6.4.12.2 Specification for ANPR Camera /Overview Camera/ Evidence Camera

Sl.No	Minimum Specification		Compliance (Yes / No)
	Make:		
	Model:		
1	Image Sensor	1/2.8" 2MP Progressive Scan CMOS or better	
2	Day/Night Operation	Yes with IR Cut Filter	
3	Minimum Illumination	Color: 0.03 lux or better ; B/W 0 Lux with IR	
4	Lens	5.5-62 mm (+/- 1mm) Motorized Varifocal Lens or better	
5	Electronic Shutter	1/5 to 1/50,000s or better	
6	Image Resolution	1920x1080 or better	
7	Compression	H.265 or better	
8	Frame Rate and Bit Rate	Up to 60 fps with Controllable bit rate, frame rate and Maximum Bit rate	
9	Video Streams	Minimum 4 Nos, individually configurable simultaneous streams in H.265 @ 1920x1080 & 60 Fps	
10	Angular Field of View	H: 54.58°(Wide)~5.30°(Tele) / V: 32.19°(Wide)~3.00°(Tele) / D: 61.4(Wide)~6.06(Tele)	

11	Motion Detection	Built in 8 point polygonal zones areas in the video stream.	
12	Lens/Barrel Distortion Correction & Corridor View	Built in feature required	
13	Wide Dynamic Range	150 dB or better	
14	IR	100 Meter (Built in or External) IR.	
15	Alarm	1 Input & 1 Output	
16	Audio In	Selectable (Mic in/Line in), Supply voltage: 2.5VDC(4mA), Input impedance: 2K Ohm	
17	Audio Out	Line out, Max. output level: 1Vrms	
18	Audio Compression	G.711 u-law /G.726 Selectable G.726(ADPCM) 8KHz, G.711 8KHz G.726 : 16Kbps, 24Kbps, 32Kbps, 40Kbps AAC-LC : 48Kbps at 16KH	
19	Analytics	Defocus detection, Directional detection, Fog detection, Face detection, Motion detection, Digital auto tracking, Appear/Disappear, Enter/Exit, Loitering, Tampering, Virtual line, Audio detection, Sound classification. Can be achieved via VMS and VA	
20	Event Triggers	Alarm input, Motion detection, Analytics, Network disconnect and others	
21	Event Actions	FTP, HTTP, Email notification, Edge Storage, Alarm Output	
22	Edge Storage	Micro SD/SDHC/SDXC 1 no. slot of 512GB capacity or better with min.512GB Memory card	
23	Protocols	IPv4, IPv6, TCP/IP, UDP/IP, RTP(UDP), RTP(TCP), RTCP,RTSP, NTP, HTTP, HTTPS, SSL/TLS, DHCP, FTP, SMTP, ICMP, IGMP, SNMPv1/v2c/v3(MIB-2), ARP, DNS, DDNS, QoS, PIM-SM, UPnP, Bonjour , LLDP, SRTP	
24	Security	HTTPS(SSL) Login Authentication, Digest Login Authentication, IP Address Filtering, User access Log 802.1X Authentication (EAP-TLS, EAP-LEAP)	
25	Firmware Upgrade	The firmware upgrade shall be done though web interface, The firmware shall be available free of cost	
26	Interface	RJ 45, 100 Base TX or better	

27	Memory	1024 MB RAM, 256 MB Flash or better	
28	Enclosure	IP67, IK10 & Nema4x or better	
29	Power requirements	Vendor to specify, POE Preferred	
30	Operating Temperature	0 °C to 55 °C or better	
31	Operating Humidity	Max 90% RH or better	
32	Certification	UL, CE, FCC, BIS, NDAA	
33	Application Programmers Interface	1. The interface shall be available for integration with 3rd party analytics and applications in public domain 2. ONVIF	
34	Embedded Applications	The camera shall provide a platform allowing the upload of third-party applications into the camera	
35	Mount	Wall Mount/ Pole Mount	
36	Warranty	Min. 5 Years	
37	Privacy Masks	Minimum 4	

6.4.13 Corridor Management**:**

- With a view to ensure that the traffic in the major trunk roads are monitored and proper details are being disseminated to the commuters. It is proposed to install corridor management systems in three corridors. These Corridors will also have Traffic enforcement systems like Instant Speed, Average Speed, Wrong direction, sudden lane changing. Prime corridor as mentioned above will have evidence cameras video-based analytics to provide traffic data and will also provide possibility to view video from these monitoring stations to verify any unusual incident from ICCC. The precise information from solution will provide volume, classification, average speed of traffic, any unusual incident on the corridor which can impact traffic flow conditions. The system should have Vehicle Counting and Classification functions using the ANPR and evidence cameras.

  The details of the said corridor are as follows:

Sl. No	Name	From	To
1	Main Corridor	ECR Entry	Cuddalur Exit
2	Corridor 1	Indira Gandhi Junction	Beach Start
3	Corridor 2	Adigal Salai Junction	PWD Office Junction

The functional/Technical requirement of the said system shall be as follows:

6.4.14 Variable Message Display

- The Variable Message Display(VMD) will be able to play Text Image and Full Color Video and approximately 3.8 meterX1.9 meter. Hardware should have minimum 5 year warranty
- The (VMD) should have : pixel density 2500Pixels/sq.m , RGB Resolution 16pixelsX 8 pixels , brightness >12300 cd/sq.m., color amount 16million., Contrast 3000:1,
- The (VMD) should have best view distance of 20 to 100 meter with optimum viewing Horizontal>30, Vertical>
- The (VMD) shall be of IP 67
- The cabinet material should be steel and should double side back door for traffic display
- The (VMD) system should be supplied with all required controllers and should have integrated base with traffic and other information portal from smart city control room

- ICCC and Central Control Software shall allow controlling multiple (VMD) from one console. Capable of programming to display all types of Message/ advertisement having alphanumeric character in English, - and combination of text with pictograms signs. The system should have feature to manage video / still content for VMS display.
- The system should have capability to divide VMS screen into multi-parts to display diverse form of information like video, text, still images, advertisements, weather info, city info etc. The system should also provide airtime management and billing system for paid content management. Capable of controlling and displaying messages on VMS boards as individual/ group.
- Capable of controlling and displaying multiple font types with flexible size and picture sizes suitable as per the size of the (VMD). Capable of controlling brightness & contrast through software.
- Capable to continuously monitor the operation of the Variable Message sign board, implemented control commands, and communicate information to the ICCC via communication network.
- Real time log facility – log file documenting the actual sequence of display to be available at central control system.
- Multilevel event log with time & date stamp.
- Access to system only after the authentication and acceptance of authentication based on hardware dongle or similar with its log.
- Location of each (VMD) will be plotted on GIS Map with their functioning status which can be automatically updated.
- Report generation facility for individual/group/all (VMD) with date and time which includes summary of messages, dynamic changes, fault/repair report and system accessed logs, link breakage logs, down time reports or any other customized report.
- Configurable scheduler on date/day of week basis for transmitting pre-programmed message to any (VMD) unit.
- Various users should access the system using single sign or similar and should be role based. Different roles which could be defined (to be finalized at the stage of SRS) could be Administrator, Supervisor, Officer, Operator, etc.
- Apart from role-based access, the system should also be able to define access based on location.
- Rights to different modules / Sub-Modules / Functionalities should be role based and proper log report should be maintained by the system for such access
- Mounting : Should be mounted with standard poles , erecting structures and road clearance.

6.4.15 Specification for Speed Violation Camera:

#	Parameter	Minimum Specifications or better	Compliance (Yes or No)
	Make:		
	Model:		
1	Image Sensor	1/2.8" 2MP Progressive Scan CMOS or better	
2	Day/ Night Operation	Yes with IR Cut Filter	
3	Minimum Illumination	Color: 0.03 lux or better ; B/W 0 Lux with IR	
4	Lens	5.5-62 mm (+/- 1mm) Motorized Varifocal Lens or better, F1.6	
5	Electronic Shutter	1/10 to 1/12,000s or better	
6	Image Resolution	1920x1080 or better	
7	Compression	H.265 or better	
8	Frame Rate and Bit Rate	Upto 60 fps with Controllable bit rate, frame rate and Maximum Bit rate	
9	Video Streams	Minimum 4 Nos, individually configurable simultaneous streams in H.265 @ 1920x1080 & 60 Fps	
10	Angular Field of View	H:54.58°(Wide)~5.30°(Tele)/V: 32.19°(Wide)~3.00°(Tele)/D: 61.4(Wide)~6.06(	
11	Motion Detection	Built in 8 point polygonal zones areas in the video stream.	
12	Lens/ Barrel Distortion Correction & Corridor View	Built in feature required	
13	Wide Dynamic Range	150 dB or better	
14	IR	70 Meter (Built in or External) IR	
15	Alarm	1 Input & 1 Ouput	
16	Audio In	Selectable(Mic in/Line in), Supply voltage: 2.5VDC(4mA), Input impedance: 2K Ohm	
17	Audio Out	Line out, Max. output level: 1Vrms	
18	Audio Compression	G.711 u-law /G.726 Selectable G.726(ADPCM) 8KHz, G.711 8KHz G.726 : 16Kbps, 24Kbps, 32Kbps, 40Kbps AAC-LC : 48Kbps at 16KH	
19	Analytics	Defocus detection, Directional detection, Fog detection, Face detection, Motion	

		detection, Digital auto tracking, Appear/Disappear, Enter/Exit, Loitering, Tampering, Virtual line, Audio detection, Sound classification and others. Can be achieved via VMS and VA	
20	Event Triggers	Alarm input, Motion detection, Analytics, Network disconnect and others	
21	Event Actions	FTP, HTTP, Email notification, Edge Storage, Alarm Output	
22	Edge Storage	Micro SD/SDHC/SDXC 2 no. slot of 512GB capacity each or better with min.512GB Memory card	
23	Protocols	IPv4, IPv6, TCP/IP, UDP/IP, RTP(UDP), RTP(TCP), RTCP,RTSP, NTP, HTTP, HTTPS, SSL/TLS, DHCP, FTP, SMTP, ICMP, IGMP, SNMPv1/v2c/v3(MIB-2), ARP, DNS, DDNS, QoS, PIM-SM, UPnP, Bonjour , LLDP, SRTP	
24	Security	HTTPS(SSL) Login Authentication, Digest Login Authentication, IP Address Filtering, User access Log 802.1X Authentication (EAP-TLS, EAP-LEAP)	
25	Firmware Upgrade	The firmware upgrade shall be done though web interface, The firmware shall be available free of cost	
26	Interface	RJ 45, 100 Base TX or better	
27	Memory	1024 MB RAM, 256 MB Flash or better	
28	Enclosure	IP67, IK10 & Nema4x or better	
29	Power requirements	Vendor to specify, POE Preferred	
30	Operating Temperature	0 °C to 55 °C or better	
31	Operating Humidity	Max 90% RH or better	
32	Certification	UL, CE, FCC, BIS, NDAA	
33	Application Programmers Interface	1. The interface shall be available for integration with 3rd party analytics and applications in public domain 2. Onvif	
34	Embedded Applications	The camera shall provide a platform allowing the upload of third party applications into the camera	
35	Mount	Wall Mount/ Pole Mount	
36	Warranty	Min. 5 Years	

37	Speed detection system to capture speed	Upto 200 Kmph +/- 5%	
38	Speed Enforcement Technology	Radar/Laser/Other better technologies	

6.4.16 Instant Speed Violation Detection:

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

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

- Install the Speed Violation Detection Systems across the city. This system shall capture the infractions of speed violations at these locations. The proposed Instant Speed system should have proper test certification in compliance with standards for speed enforcement systems.
- Design, supply, and install the speed violation detection system as per requirement. This includes supply all the necessary equipment for the camera and detection system, including but not limited to sensors, computers, ancillary camera equipment, camera housings, camera poles, warning signs and shall make the final connections to the camera.
- The solution proposed shall seamlessly integrate with the E-Challan system proposed under the scope of this project.
- Providing all the necessary IT infrastructure for analysis, storage & retrieval of the infraction information at ICCC or any other location as per the requirement.

The functional requirement of the said system shall be as follows:

Functional Specification for Instant Speed System:

S/N	Functional Requirement	Compliance (Yes / No)
	Make:	
	Model:	
1	The proposed solution should have video based speed violation detection feature with a facility to set different speed limits for different categories of	

	vehicles and schedule. The feature should have the functionality to prove the vehicle speed using a simple on-screen tool.	
2	The speed detection use case (along with license plate recognition) should be capable to read speeds in excess of 100- 250 km/hr. A certificate from an institute of repute, which can issue such a certificate in India should be provided to substantiate the claim.	
3	The speed detection software system shall be certified by any accredited laboratory for speeds from 40 KMPH to 235 KMPH with variation of less than 2% at various speed thresholds such as 40 KMPH, 70 KMPH, 100 KMPH, 130 KMPH, 170 KMPH, 200 KMPH and 235 KMPH speeds.	
4	Software should also provide Average Speed detection functionality for a control section / corridor within the city. All vehicles passing through the control section at a Speed greater than a determined speed limit shall be detected as violation. It should be possible to create multiple points within a long corridor for determining the average speed.	

6.4.17 Average Speed Violation Detection:

Software should also provide Average Speed detection functionality for a control section / corridor within the city. All vehicles passing through the control section at a Speed greater than a determined speed limit shall be detected as violation. It should be possible to create multiple points within a long corridor for determining the average speed.

6.4.18 Wrong Side Driving Violation

#	Minimum Requirements	Compliance (Yes / No)
A.	**General**	
1.	Wrong Side Detection of Vehicle Movement –The system should be installed at critical junctions or streets as identified by the department to capture the wrong direction vehicle movement.	
2.	The system should identify and capture multiple violating vehicles and the E-Challan standard procedure should be triggered.	

6.4.19 Adaptive Traffic Control System

It is proposed to implement Adaptive Traffic Controller at identified junctions. The proposed system shall have a fully adaptive traffic controller with the following functionalities:

Traffic Signal Controller

#	Description	Compliance (Yes / No)
	Make:	
	Model:	

1	The Traffic Signal Controller equipment is a 32 bit or 64-bit microcontroller with a solid-state traffic signal lamp switching module with the ability to program any combination of traffic signal stages, phases, and junction groups. The controller will ideally have a conflict monitoring facility to ensure that conflicting, dangerous are pre-flagged at the programming stage and these are disallowed even during the manual override phase. Should have 5 year warranty	
2	The Traffic Signal Controller can be controlled through the central traffic control center as an individual junction or as part of the group of traffic junctions along a corridor or a region. The signal controller design must be flexible for the junction could be easily configured to be part of any corridor or group definition and could be changed through a central command controller easily	
3	Site-specific configuration data shall be stored in a non-volatile memory device (FLASH memory) easily programmable at the site through a keypad or laptop. A minimum of 512KB flash memory and 128KB RAM shall be provided. Volatile memory shall not be used for storing the junction-specific plans or signal timings.	
4	All timings generated within a traffic signal controller shall be digitally derived from a crystal clock which shall be accurate to plus or minus 100 milliseconds.	
5	The controller shall provide a real-time clock (RTC) with battery backup that sets and update the time, date, and day of the week from the GPS. The RTC shall have a minimum of 10 years battery backup with maximum time tolerance of +/- 2 sec per day.	
6	The controller shall have the facility to update the RTC time from the ATCS server, GPS, and through manual entry.	
7	The traffic signal system including the controller shall have provision for audio output tones and should be disabled-friendly.	
8	The controller shall be capable of communicating with the ATCS server through Ethernet on a managed leased line network or any other appropriate stable communication network.	

Police Panel

#	Description	Compliance (Yes / No)
	Make:	
	Model:	
1	Four Hurry Call switches: The Hurry Call mode will provide the means to force the controller to a defined stage, without violating safety clearances. A pre-emption input may be used to demand the Hurry Call mode to give the right of way to emergency vehicles. It should be possible to configure the Hurry Call switches to any stage as per site requirements.	
2	One Forced Flash Switch: Activation of this switch should force the signal to Flashing Amber / Flashing Red.	

3	One Auto / Manual Switch: Activation of this switch should enable the manual operation of the controller. Deactivation of the manual switch shall continue from the current stage without interruption.	
4	One Manual Advance Pushbutton Switch: In manual operation mode, the stages appear in the sequence specified in the signal plan timetable. Activating the pushbutton switch shall terminate the currently running stage and start the next, without violating safety clearances.	
5	One Junction OFF Switch: Activating this switch should put OFF all signal lamps. On deactivation of the switch, the traffic signal controller shall resume its normal operation without violating any safety clearances.	

Modes of Operation

#	Description	Compliance (Yes / No)
1	Fixed Time: In fixed time (pre-timed) mode the traffic signal controller shall execute stage timings according to the site-specific timetable maintained in the traffic signal controller FLASH memory. Inputs from vehicle detectors shall be ignored in this mode and no pre-emption shall be made at any stage. Cycle time remains constant in every cycle execution for a given time period.	
2	Vehicle Actuation with All Stages Pre-emption: In the vehicle actuation with all stages pre-emption mode, the traffic signal controller shall execute stage timings as per demand from vehicle detectors within the constraints of Minimum Green, Maximum Green running period for the stage, and Cycle time stored in the traffic signal controller FLASH memory. Pre-emption shall be possible for all demand actuated stages. Cycle time may vary in every cycle execution.	
3	Semi-Actuation: In the semi-actuation mode, the traffic signal controller shall execute stage timings in the vehicle actuated stages as per demand from vehicle detectors within the constraints of Minimum Green, Maximum Green running period for the stage, and Cycle time stored in the traffic signal controller FLASH memory. All other stages shall execute the Maximum green time configured for the stage. Pre-emption shall be possible for all demand actuated stages. Cycle time may vary in every cycle execution.	
4	Stage Skipping: The traffic signal controller shall not execute the stage enabled for skipping when there is no vehicle demand registered for the stage till the clearance amber time of the previous stage.	

5	Transit Signal Priority (TSP) for buses: The traffic signal controller shall provide transit signal priority for buses in the dedicated lane to ensure minimum stop delay at the intersection, without violating safety clearances.	
6	Vehicle Actuation with Fixed Cycle length: In-vehicle actuation with fixed cycle length mode, the traffic signal controller shall execute stage timings as per demand from vehicle detectors within the constraints of Minimum Green, Maximum Green running period for the stage, and Cycle time shall be maintained constant during a given timeslot. Pre-emption for all demand actuated stages except for the Priority Stage shall be possible.	
	Full ATCS (FATCS): In FATCS mode, the traffic signal controller shall execute stage timings as per demand within the constraints of Minimum Green, Maximum Green running period for the stage, and Cycle time specified by the Central Computer during every cycle switching. Pre-emption for all demand actuated stages except Priority Stage shall be possible in this mode. The traffic signal controller shall identify a communication failure with the central computer within a specified period. In such an event the signal plan timings shall be executed from the local timetable stored in the traffic signal controller FLASH memory. The fallback mode of the traffic signal controller shall be vehicle actuated. On the restoration of the communication with the central computer, the traffic signal controller shall automatically resort to FATCS mode. The traffic signal controller shall accept commands for remote selection / de-selection of the following from the Central Computer at ICCC. · Hurry Call · Flashing Amber / Flashing Red · Junction Off If not reverted to the normal operation within the period listed below, the traffic signal controllers shall timeout the commands and operate normally · Hurry Call – 5 Minutes · Flashing Amber / Flashing Red – 30 Minutes · Junction Off – 30 Minutes The traffic signal controller shall report the following to the Central Computer through the communication network every cycle or on an event as appropriate. · Green time exercised for each approach (stage pre-emption timing) against the Green running period set for the approach by the Central Computer · Mode of Operation · Lamp failure, if any · Output short circuit, if any · Detector failure, if any	

Traffic Signal Controller Operating Parameters

#	Description	Compliance (Yes / No)
1	It shall be possible to operate the filtered green (turning right signal) along with a vehicular phase. The filter green signal shall flash for some time	

	equal to the clearance amber period at timeout when operated with a vehicular phase.	
2	The pedestrian phase signal shall be configured for flashing red or flashing green aspects during pedestrian clearance.	
3	It shall be possible to configure any phase to the given lamp numbers at the site.	
4	Stages – The controller shall have the facility to configure at least 32 Stages	
5	Cycle Plans – The controller shall have the facility to configure 24 Cycle Plans and the Amber Flashing / Red Flashing plan. It shall be possible to define different stage switching sequences in different cycle plans. The controller shall have the capability for a minimum of 32 cycle-switching per day in the fixed mode of operation.	
6	Day Plans – The controller shall have the facility to configure each day of the week with different day plans. It shall also be possible to set any of the day's plans to any day of the week. The controller shall have the capability to configure 20-day plans or as per requirement.	
7	Special Day Plans – The controller shall have the facility to configure a minimum of 20 days as special days in a calendar year or as per requirement.	
8	Starting Amber – During power up the controller shall initially execute the Flashing Amber / Flashing Red plan for some time of 3 Seconds to 10 Seconds. The default value of this Starting Amber is 5 Seconds. The facility shall be available to configure the period of Starting Amber within the given limits at the site.	
9	Inter-green – Normally the inter-green period formed by the clearance Amber and Red extension period will be common for all stages. However, the controller shall have a facility to program individual inter- green periods from 3 Seconds to 10 Seconds.	
10	Minimum Green – The controller shall allow programming the Minimum Green period from 5 Seconds to 10 Seconds without violating the safety clearances. It should not be possible to pre-empt the Minimum Green once the stage starts commencing execution.	
11	All Red – Immediately after the Starting Amber all the approaches should be given the red signal for a few seconds before allowing any right of way, as a safety measure. The controller shall have programmability of 3 Seconds to 10 Seconds for All Red signal.	
12	Signal lamps monitoring – The controller shall have inbuilt circuitry to monitor the lamp status	
13	Green – Green Conflict Monitoring – The controller shall have a facility to list all conflicting phases at an intersection. The controller should not allow programming of these conflicting phases in a Stage. A hardware failure leading to a conflict condition (due to faulty devices or a short circuit in the output) shall force the signal into Flashing Amber / Flashing Red.	

14	Cableless Synchronization – It shall be possible to synchronize the traffic signal controllers installed in a corridor in the following modes of operation, without physically linking them and without a communication network. GPS enabled RTC shall be the reference for the cable less synchronization.	
15	Fixed Time mode with fixed offsets	
16	Vehicle Actuated mode with fixed offsets	

Input and Output facilities

#	Description	Compliance (Yes / No)
1	Lamp Switching: The controller shall have a minimum of 48 (Scalable to 64) individual output for signal lamp switching. The signal lamps shall be operating on appropriate DC/AC voltage of applicable rating	
2	Detector Interface: A minimum of 16 vehicle detector inputs shall be available in the controller. All detector inputs shall be optically isolated and provided with LED indication for detection of the vehicle For future scalability to ATCS	
3	Communication Interface: The traffic signal controller shall support an Ethernet interface to communicate with the ATCS server	
4	Power Saving: The traffic signal controller shall have a facility to regulate the intensity of signal lamps during different ambient light conditions thereby saving energy.	
5	Real-time Clock (RTC): The GPS receiver for updating time, date, and day of the week information of the traffic signal controller should be an integral part of the traffic signal controller.	
6	The traffic signal controller shall update the date, time, any day of the week automatically from GPS during power ON and at scheduled intervals.	
7	Manual entry for the date, time, any day of the week shall be provisioned for setting the traffic signal controller RTC (Real Time Clock).	
8	It shall be possible to set the RTC from the Central Server when networked	
9	Keypad (optional): The traffic signal controller shall have a custom- made keypad or should have provision for plan upload and download using PC/laptop/Central Server	
10	Operator Display (optional): The traffic signal controller shall have a LED-backlit Liquid Crystal Display (LCD) as the operator interface.	

Countdown Timer

Countdown Timer shall be installed at each traffic junction under this Project

#	Description	Compliance (Yes / No)
	Make:	
	Model:	
1	Count Down Timer to be configured in Vehicular Mode. Hardware should have 5 year warranty	
2	The Vehicular countdown timer should be dual-color, · Red for Stop or STP · Green color for Go	
3	There should be alternate Red and Balance phase time for STOP or STP in Flashing	
4	Alternate Green and Balance Phase Time for Go in Flashing	

Communication Network

#	Description	Compliance (Yes / No)
1	Function of the Communication network is for remote monitoring of the intersection and its management. Real time data (like RTC time, stage timing, mode, events, etc.) from the traffic signal controller is required to be sent to the ICCC and also individual junctions can be controlled and actuated from central ICCC(Hurry Calls, Forced Flash , Junction Switch off, Plan download and upload etc.).	

ATCS Software Application :

The Adaptive Traffic Control Software application software shall do the following:

#	Description	Compliance (Yes / No)
1	Identify the critical junction(s) of a corridor or a region based on maximum traffic demand and saturation.	
2	The critical junction cycle time shall be used as the group cycle time i.e. cycle time common to all intersections in that corridor or region.	
3	Stage optimization to the best level of service shall be carried out based on the traffic demand.	
4	Cycle optimization shall be carried out by increasing or decreasing the common corridor cycle time based on the traffic demand within the constraints of Minimum and Maximum designed value of cycle time.	

5	Offset correction shall be carried out to minimize the number of stops and delays along the corridor for the priority route. Offset deviation measured using distance and speed between successive intersections shall be corrected within 5 cycles at a tolerance of +/- 5 seconds maximum.	
6	The system shall have provision to configure the priority for upstream signals as default. The ATCS software shall continuously check the traffic demand for upstream and downstream traffic and automatically assign the priority route to the higher demand direction.	
7	Develop appropriate stage timing plans for each approach of every intersection under the ATCS, based on real-time demand	
8	Propose timing plans to every intersection under the ATCS in every Cycle	
9	Verify the effectiveness of the proposed timing plans in every cycle	
10	Identify Priority routes	
11	Synchronize traffic in the Priority routes	
12	Manage and maintain communication with traffic signal controllers under ATCS	
13	Maintain database for time plan execution and system performance	
14	Maintain error logs and system logs	
15	Generate Reports on request	
16	Graphically present signal plan execution and traffic flow at the intersection on desktop	
17	Graphically present time-space diagram for selected corridors on desktop	
18	Graphically present network status on desktop	
19	Make available the network status and report viewing on Web	
20	The ATCS shall generate standard and custom reports for planning and analysis	
21	It shall be possible to interface the ATCS with a popular microscopic traffic flow simulation software for pre and post-implementation analysis and study of the proposed ATCS control strategy	
22	Shall have the ability to predict, forecast, and smartly manage the traffic pattern across the signals over the next few minutes, hours, or 3-5 days and just in the current real-time.	
23	Shall provide a decision support tool for assessing strategies to minimize congestion, delays, and emergency response time to events via simulation and planning tools like real-time traffic data fusion and control of traffic signaling infrastructure on the ground.	

24	Shall collect continuous information about current observed traffic conditions from a variety of data sources and of different kinds (traffic states, signal states, vehicle trajectories, incidents, road works etc)	
25	Shall infer a coherent and comprehensive observed traffic state (speeds, vehicular densities, and presence of queues) on all network elements, from the above-mentioned observations, including vehicle trajectories, through several map matching, data validation, harmonization, and fusion processes	
26	Shall extend the measurements made on only several elements both on the rest of the unmonitored network, and over time, thus obtaining an estimation of the traffic state of the complete network and the evolution of this traffic state in the future	
27	Shall forecast the traffic state concerning current incidents and traffic management strategies (e.g., traffic signal control or variable message signs), improving the decision-making capabilities of the operators even before problems occur	
28	Shall calculate customizable Key Performance Indicators (KPI) to quickly assess the results	
29	Shall provide calculated traffic flows estimation and forecast, queues and delays to Urban Control and Adaptive Signal Control Systems, allowing for proactive Traffic Management and Control	
30	Shall generate alerts to the operator that trigger on customizable conditions in the network (starting with simple drops inflow, up to total queue lengths along emission sensitive roads surpassing a definable threshold)	
31	Shall distribute both collected and calculated traffic information via a variety of communication protocols and channels, ensuring high interoperability degree and thus acting as a "traffic data and information hub"	
32	Shall create a traffic data warehouse for all historic traffic information gathered from the hardware installed on the road network.	
33	Shall operate in real-time that is continuously updating the estimates on the state of the network and the travel times based on data collected continuously over time.	
34	Shall operate the traffic lights with the adaptive traffic controls, based on the current and forecasted traffic demand and the current incidents, thus optimizing the green waves continuously throughout the network	
35	Enable a smart public transport priority respecting the delays for all road users at once with the adaptive signal controller	

Reports

Reports System shall generate corridor based and junction/Intersection based reports. The application software shall generate the following reports, but not limited to the below. All the reports shall be possible for selected dates.

#	Description	Compliance (Yes / No)
1	Junction/Intersection based reports	
2	Stage Timing report – The report shall give details of the time at which every stage change has taken place. The report shall show the stage sequence, stage timings, and stage saturation of all stages of all cycles for a day. The saturation is defined as the ratio between the available stage timings to the actual stage timing executed by the traffic signal controller for the stage (stage pre-emption time).	
3	Cycle Timing report – The report shall give details of the time at which every cycle has taken place. The report shall show the cycle sequence and cycle timings for all the cycles in a day.	
4	Stage switching report – The report shall give details of the time at which a stage switching has taken place. The report shall show the stage sequence, stage timings, and stage saturation for a day.	
5	Cycle Time switching report – The report shall give details of the time at which a cycle switching has taken place. The report shall show the cycle sequence and cycle timings for the cycle in a day.	
6	Mode switching report – The report shall give details of the mode switching that takes place on a day.	
7	Event Report - The report shall show events generated by the controller with the date and time of the event.	
8	Power on & down: The report shall show the time when the master is switched on, and the last working time of the master controller.	
9	Intensity Change – The report shall show the brightness of the signal lamp is changed according to the light intensity either manually through the keypad or automatically by LDR with a time stamp.	
10	Plan Change – The report shall show the time of change of plan either through the keypad or remotely through a PC or Server.	
11	RTC Failure – The report shall show the time when the RTC battery level goes below the threshold value.	
12	Time Update – The report shall show the time when the Master controller updated its time either manually through the keypad, automatically by GPS, or through the remote server.	
13	Mode Change – The report shall show the time when the Master controller's operating mode is changed either manually through the keypad or a remote server. The typical modes are FIXED, FULL VA SPLIT, FULL VA CYCLE, FLASH, LAMP OFF and HURRY CALL.	

14	Lamp Status Report – The report shall show lamp failure report with date and time of failure, the color of the lamp, and associated phase	
15	Loop Failure Report – The report shall show the date and time of detector failure with detector number and associated phase.	
16	Conflict – The report shall show the conflict between lamps (RED, AMBER, GREEN) in the same phase or conflict between lamps with another phase.	
17	Corridor Performance Report – The report shall show the saturation of all the intersections in a corridor for every cycle executed for the corridor and the average corridor saturation for a day	
18	Corridor Cycle Time Report – The report shall show the Corridor cycle time, Intersection cycle time, Mode of operation, and degree of saturation of all the intersections in a corridor for every cycle for a day	

Graphical User Interface

The application software shall have following Graphic User Interface (GUI) for user friendliness

#	Description	Compliance (Yes / No)
1	User login – Operator authentication shall be verified at this screen with login name and password	
2	Network Status Display – This online display shall indicate with appropriate color coding on the site map whether an intersection under the ATCS is online or off. On double-clicking the intersection, a link shall be activated for the traffic flow display for the intersection.	
3	Traffic Flow Display – This online display shall indicate the current traffic flow with animated arrows, mode of operation, stage number being executed, and elapsed stage time.	
4	Saturation Snapshot – This display shall show the current saturation levels of all intersections in a corridor.	
5	Reports Printing / Viewing – This link shall allow selection, viewing, and printing of different reports available under ATCS	
6	Time-Space Diagram – The time-space diagram shall display the current stages being executed at every intersection in a corridor with immediate previous history.	
7	Junctions shall be plotted proportionally to their distance on Y-axis and time elapsed for the stage in seconds on X-axis.	
8	Junction names shall be identified with each plot.	
9	The facility shall be available to plot the time-space diagram from history.	

10	Currently running stage and completed stages shall be identified with different colors.	
11	Stages identified for synchronization shall be shown in a different color.	
12	Speed lines shall be plotter for stages identified for synchronization to the nearest intersection in both directions.	
13	It should be possible to freeze and resume online plotting of the Time-Space diagram.	
14	The system shall have other graphical interfaces for configuring the ATCS, as appropriate.	

Other features of the components in ATCS:

The proposed traffic controller shall be disabled friendly and shall also provide audio tones output. The supplied ATCS controller would have all the functional capability as mentioned above and also the future scalability to work an any of adaptive traffic algorithms available

- The system shall be able to detect the presence of vehicles near stop-line and do advance detection for vehicles such as Traffic volume, count
- The system shall be capable of
  - Counting the vehicle with at least 80% accuracy
  - Classification of the vehicle with at least 3 classes

Red Light Violation Detection:

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

1. The RLVD Systems at traffic junctions across the city. This system shall capture the infractions of Red light and stop line violations at these junctions.
2. The RLVD system as defined of, all wiring connections to the traffic signal controllers and to the camera platforms. Supply all of the necessary equipment for the camera and detection system, including but not limited to: computers, ancillary camera equipment, camera housings, camera poles, warning signs and shall make the final connections to the camera. In some of the accident-prone junctions client might decide to put over speed detection system and thus Shall consider these accident prone junctions.
3. The solution proposed shall seamlessly integrate with the E-Challan system proposed under the scope of this project. The Authority shall facilitate to get access to the Vaahan and Sarathi database, to access the same through use of appropriate APIs.
4. Providing all the necessary IT infrastructure for analysis, storage & retrieval of the infraction information at ICCC or any other location as per requirement

Functional Specification for RLVD Application:

S/N	Functional Requirement	Compliance (Yes / No)

1	Proposed software should capture the License Plate of the vehicles violating the red light or stop line when the signal is Red. It should be possible to detect the signal color through image analysis or through controller integration. The system should generate 3-5 violation images of the vehicle as required.	
2	Proposed software should have an in-built tool to compose detailed evidence by stitching video clips from any IP camera in the junction including surveillance cameras in the vicinity. The system should have the functionality to export the violation evidence with water mark and encryption as per the techno-legal requirements.	
3	Proposed software should flag the RLVD event in the recorded video within the system. It should allow mapping of multiple ANPR cameras to a single evidence camera associated with the traffic junction.	
4	It should be possible to view the video from an ANPR camera and the evidence camera side-by-side for any selected violation.	
5	To assess the traffic pattern, proposed software should have the report of number of vehicles crossed during any signal state such as Green Light / Orange Light, etc. The report should be available for each arm and each signal. It should be possible to analyse the report for traffic planning.	
6	The system should generate alert when the signal light doesn't change for the pre-configured duration. The system should allow the user to set minimum and maximum time for the signal light status change.	

Red Light Violation Detection System

#	Description	Compliance (Yes / No)
1	**General**	
a.	The following Traffic violations to be automatically detected by the system by using appropriate non-Intrusive sensors technology: The system should have both provisions to detect red light status by taking the signal feed from the traffic signal controller as well as by video analytics method using another camera (Evidence Camera) focused at the red light. The Evidence camera should also be used for evidence snap generation.	
	a) Red Light Violation b) Stop Line Violation	
b.	The system should be capable of capturing multiple infracting vehicles simultaneously in Different lanes on each arm at any point of time with relevant infraction data like: a) Type of Violation b) Date, time, Site Name, and Location of the Infraction	

	c) Registration Number of the vehicle through ANPR Camera system for each vehicle identified for the infraction.	
c.	The system should be equipped with a camera system to record a digitized image and video of the violation, covering the violating vehicle with its surrounding and current state of signal (Red/Green/Amber) by which the system should clearly show the nature of violation and proof there of: - When it violates the stop line. When it violates the red signal. Besides, a closer view indicating readable registration number plate patch of the violating vehicle for court evidence for each violation. The system must have the in-built tool to facilitate the user to compose detailed evidence by stitching video clips from any IP camera in the junction (including but not limited to the red-light violation detection camera, evidence camera), and any other surveillance cameras in the vicinity of the spot of incidence. The entire evidence should be watermarked and encrypted to stand in the court of law.	
d.	The system shall be able to detect all vehicles infracting simultaneously in each lane/ arm at the junction as per locations provided. It should also be able to detect the vehicles infracting serially one after another in the same lane. The vehicles should be identifiable and demarcated in the image produced by the camera system.	
e.	The Evidence image produced by the system should be wide enough to give the exact position of the infracting vehicles concerning the stop line and indicate the color of the Traffic light at the instant of Infraction even if any other means are being used to report the color of the light.	
f.	The system should interface with the traffic controller to validate the color of the traffic signal reported at the time of Infraction to give correct inputs of the signal cycle.	
g.	The Evidence and ANPR camera should continuously record all footage in its field of view to be stored at the local base station. This should be extractable onto a portable device as and when required. The option of live viewing of evidence cameras from the locations shall be available at the ICCC. The network should have the capability to provide the real- time feed of the evidence camera to the ICCC at the best resolution possible on the available network.	
h.	The system shall be equipped with IR Illuminator to ensure clear images including illumination of the Number Plate and capture the violation image under low light conditions and night-time.	

2	**Recording & display information archive medium**	
a.	The recording and display of information should be detailed on the snapshot of the infracting vehicle as follows:	
b.	Computer-generated unique ID of each violation	
c.	Date (DD/MM/YYYY)	
d.	Time (HH:MM: SS)	
e.	Equipment ID	
f.	Location ID	
g.	Carriageway or direction of violating vehicle	
h.	Type of Violation (Signal/Stop Line)	
i.	Lane Number of violating vehicle	
j.	Time into Red/Green/Amber	
k.	Registration Number of violating vehicle	
3	**On site-out station processing unit communication & Electrical Interface**	
a.	The system should automatically reset in the event of a program hanging up and restarting on a button press. However, the system should start automatically after power failure.	
b.	The system should have a secure access mechanism for the validation of authorized personnel.	
c.	Deletion or addition and transfer of data should only be permitted to authorized users.	
d.	A log of all user activities should be maintained in the system.	
e.	Roles and Rights of users should be defined in the system as per the requirements of the client	
f.	All formats of the stored data concerning the infractions should be Non-Proprietary.	
g.	The communication between the on-site outstation processing unit housed in the junction box and the detection systems mounted on the cantilever shall be through appropriate secured technology.	
h.	The system should have the capability to transfer the data to ICCC through proper encryption in real-time and batch mode for verification of the infraction and processing of challan. Call forwarding architecture shall be followed to avoid any data loss during transfer.	

i.	If the connectivity to the ICCC is not established due to network/connectivity failures, then all data about the infraction shall be stored on-site and will be transferred once the connectivity is re- established automatically. There shall also be a facility for the physical transfer of data on the portable device whenever required. There should be a provision to store a minimum of **one week** of data at each site on a 24x7 basis.	
4	**Mounting structure**	
a.	Should be cantilever mounted and shall have a minimum of 6 mtrs height with appropriate vertical clearance under the system from the Road surface to ensure no obstruction to vehicular traffic.	
b.	It should be capable to withstand high wind speeds and for structural safety, the successful bidder has to provide a structural safety certificate from qualified structural engineers approved/ certified by Govt. Agency.	
c.	It shall be painted with one coat of primer and two coats of PU paint. The equipment including poles, mountings should have an aesthetic feel keeping in mind the standards road Infrastructure (e.g Poles, Navigation boards etc) currently installed at these locations. The equipment should look "one" with the surroundings of the location and not look out of place.	
d.	Rugged locking mechanism should be provided for the onsite enclosures and cabinets.	
5	**RLVD Application**	
a.	It should be capable of importing violation data for storage in the database server which should also be available to the Operator for viewing and retrieving the violation images and data for further processing. The program should allow for viewing, sorting, transfer & printing of violation data.	
b.	It should generate the photograph of violations captured by the outstation system which include a wider view covering the violating vehicle with its surrounding and a closer view indicating readable registration number plate patch of the violating vehicle or its weblink on notices for court evidence.	
c.	All outstation units should be configurable using the software at the Central Location.	
d.	Violation retrieval could be sorted by date, time, location, and vehicle registration number and the data structure should be compatible with the Police database structure. It should also be possible to carry out recursive search and wild card search.	
e.	The operator at the back office should be able to get an alarm of all fault(s) occurring at the camera site (e.g. sensor failure, camera failure, failure of linkage with a traffic signal, connectivity failure, Camera tampering, sensor tampering).	

f.	The automatic number plate recognition Software will be part of the supplied system, Success rate of ANPR will be taken as 95% or better during the daytime and 90% or better during the nighttime with a standard number plate.	
g.	The application software should be integrated with the E Challan software for tracing the ownership details of the violating vehicle and issuing/printing notices. Any updates of the software (OS, Application Software including any proprietary software), shall be updated free of cost during the contract period.	
h.	Image zoom function for number plates and images should be provided. In case the number plate of the infracting vehicle is readable only through the magnifier then in such cases, the printing should be possible along with the magnified image.	
i.	Various users should be able to access the system using a single sign-on and should be role-based. Different roles which could be defined (to be finalized at the stage of SRS) could be Administrator, Supervisor, Officer, Operator, etc.	
j.	Apart from role-based access, the system should also be able to define access based on location.	
k.	Rights to different modules / Sub-Modules / Functionalities should be role-based and proper log reports should be maintained by the system for such access.	
l.	Components of the architecture must provide redundancy and ensure that there are no single points of failure in the key project components. Considering the high sensitivity of the system, the design shall be in such a way as to be resilient to technological sabotage. To take care of remote failure, the systems need to be configured to mask and recover with the minimum outage.	
m.	The architecture must adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft, etc. Provisions for the security of field equipment as well as protection of the software system from hackers and other threats shall be a part of the proposed system. Using Firewalls and Intrusion detection systems such as attacks and theft shall be controlled and well supported (and implemented) with the security policy. The virus and worms' attacks shall be well defended with Gateway level Anti-virus system, along with workstation level Anti-virus mechanism. There shall also be an endeavor to make use of the SSL/VPN technologies to have secured communication between Applications and their end-users. Furthermore, all the system logs shall be properly stored & archived for future analysis and forensics whenever desired.	
n.	The evidence of Infraction should be encrypted and protected so that any tampering can be detected.	

o.	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.	
p.	System shall use open standards and protocols to the extent possible and declare the proprietary software wherever used.	
q.	The user interface should be user-friendly and provide facilities to the user for viewing, sorting, and printing violations. The software should also be capable of generating query-based statistical reports on the violation data.	
r.	The data provided for authentication of violations should be in an easy-to-use format as per the requirements of the user.	
s.	Users should be provided with means of listing the invalid violations along with the reason(s) of invalidation without deleting the record(s).	
t.	Basic image manipulation tools (zoom etc.) should be provided for the displayed image but the actual recorded image should never change.	
u.	Log of user actions is maintained in read-only mode. The user should be provided with the password and ID to access the system along with user type (admin, user).	
v.	Image should have a header/footer depicting the information about the site IP and violation details like date, time, equipment ID, location ID, Unique ID of each violation, lane number, Regn. Number of violating vehicle and actual violation of violating vehicle etc. so that the complete lane wise junction behavior is recorded including (Red Light violation and Stop Line Violation)	
w.	Number plate should be readable automatically by the software/interface. There should be a user interface for simultaneous manual authentication/correction and saving as well.	
x.	Interface for taking prints of the violations (including image and above details).	

RLVD Camera Technical Specification:

#	Parameter	Minimum Specifications or better	Compliance (Yes / No)
	Make:		
	Model:		
1	Image Sensor	1/2.8" 2MP Progressive Scan CMOS or better	
2	Day/ Night Operation	Yes with IR Cut Filter	

3	Minimum Illumination	Color: 0.03 lux or better ; B/W 0 Lux with IR	
4	Lens	5.5-62 mm (+/- 1mm) Motorized Varifocal Lens or better	
5	Electronic Shutter	1/5 to 1/50,000s or better	
6	Image Resolution	1920x1080 or better	
7	Compression	H.265 or better	
8	Frame Rate and Bit Rate	Up to 60 fps with Controllable bit rate, frame rate and Maximum Bit rate	
9	Video Streams	Minimum 4 Nos, individually configurable simultaneous streams in H.265 @ 1920x1080 & 60 Fps	
10	Angular Field of View	H: 54.58°(Wide)~5.30°(Tele) / V: 32.19°(Wide)~3.00°(Tele) / D: 61.4(Wide)~6.06(Tele)	
11	Motion Detection	Built in 8 point polygonal zones areas in the video stream.	
12	Lens/ Barrel Distortion Correction & Corridor View	Built in feature required	
13	Wide Dynamic Range	150 dB or better	
14	IR	100 Meter (Built in or External) IR.	
15	Alarm	1 Input & 1 Output	
16	Audio In	Selectable (Mic in/Line in), Supply voltage: 2.5VDC(4mA), Input impedance: 2K Ohm	
17	Audio Out	Line out, Max. output level: 1Vrms	
18	Audio Compression	G.711 u-law /G.726 Selectable G.726(ADPCM) 8KHz, G.711 8KHz G.726 : 16Kbps, 24Kbps, 32Kbps, 40Kbps AAC-LC : 48Kbps at 16KH	
19	Analytics	Defocus detection, Directional detection, Fog detection, Face detection, Motion detection, Digital auto tracking, Appear/Disappear, Enter/Exit, Loitering, Tampering, Virtual line, Audio detection, Sound classification. Can be achieved via VMS and VA	

20	Event Triggers	Alarm input, Motion detection, Analytics, Network disconnect and others	
21	Event Actions	FTP, HTTP, Email notification, Edge Storage, Alarm Output	
22	Edge Storage	Micro SD/SDHC/SDXC 1 no. slot of 512GB capacity or better with min.512GB Memory card	
23	Protocols	IPv4, IPv6, TCP/IP, UDP/IP, RTP(UDP), RTP(TCP), RTCP,RTSP, NTP, HTTP, HTTPS, SSL/TLS, DHCP, FTP, SMTP, ICMP, IGMP, SNMPv1/v2c/v3(MIB-2), ARP, DNS, DDNS, QoS, PIM-SM, UPnP, Bonjour , LLDP, SRTP	
24	Security	HTTPS(SSL) Login Authentication, Digest Login Authentication, IP Address Filtering, User access Log 802.1X Authentication (EAP-TLS, EAP-LEAP)	
25	Firmware Upgrade	The firmware upgrade shall be done though web interface, The firmware shall be available free of cost	
26	Interface	RJ 45, 100 Base TX or better	
27	Memory	1024 MB RAM, 256 MB Flash or better	
28	Enclosure	IP67, IK10 & Nema4x or better	
29	Power requirements	Vendor to specify, POE Preferred	
30	Operating Temperature	0 °C to 55 °C or better	
31	Operating Humidity	Max 90% RH or better	
32	Certification	UL, CE, FCC, BIS, NDAA	
33	Application Programmers Interface	1. The interface shall be available for integration with 3rd party analytics and applications in public domain 2. ONVIF	
34	Embedded Applications	The camera shall provide a platform allowing the upload of third-party applications into the camera	
35	Mount	Wall Mount/ Pole Mount	
36	Warranty	Min. 5 Years	
37	Privacy Masks	Minimum 4	
38	Red Light Detection	System shall be Non-Intrusive. It shall not be connected with traffic light and red light status is detected without any physical connection to traffic light.	
39	Fair System	Red light system shall be completely fair system with all evidences captured before and after the red light jumping infraction has happened.	

40	Lane Coverage	Each camera shall cover atleast one lane having width of 3.5m	
41	E-Challan	Integration with E-Challan system	

Countdown Timer

#	Parameters	Minimum Specifications or better	Compliance (Yes / No)
	Make:		
	Model:		
1	CPU	MicroController	
2	**Mechanical Specifications**		
A	Structural Material	Polycarbonate strengthened against UV rays	
B	Body Color	Light Grey/Black	
C	Dimensions	360mm x 370mm x 220mm	
3	**Display Specification**		
A	Lamp Diameter	300mm	
B	Digit Height	150 -165mm	
C	Display Type	Dual Coloured (Red & Green)	
D	No. of Digit	3	
4	**LED Specifications**		
A	LED Diameter	5mm LED	
B	Viewing Angle	30°	
C	LED Wave Length	630-640nm (Red), 505nm - 520nm (Blue- Green)	
D	LED Dice Material	AlInGap (Red), InGaN (Blue-Green)	
E	LED Warranty period	5 years	
5	**Technical Features**		
A	Power Consumption	20 - 30 Watt Per Lamp	

B	Input Power	85-260V AC, 50Hz	
C	Operating Temperature	-20 to + 60 °C	
D	Humidity	0% to 95% Relative Humidity	
E	Water & Dust Ingress	IP 67	
F	Standard	EN12966 Compliant	

Pedestrian Lamp Heads: Signal Controller Specification:

#	Component	Compliance (Yes / No)
	Make:	
	Model:	
	Key Features	
1	This pedestrian signal controller should be a 32-bit microcontroller-based unit or better.	
2	Should have GPS-based Real-Time Clock (RTC) with battery backup.	
3	Should have a minimum of 16 independent lamp outputs.	
4	Integrated Keyboard and LCD for easy junction programming	
5	Should have loop-based or Camera based detection module.	
6	Should be able to operate on 12/24 VDC and 230 VAC.	
7	Should have Ethernet- communication to have remote administration and monitoring from the central computer	
8	Should have a minimum of 16 programmable phases and stages	
9	Should have the programmable facility for Hurry calls, week plans, holiday/special day plans	
10	Should be enclosed in IP65/67-grade box and should withstand temperatures up to 60C.	
11	Should have relevant certification like ERTL/STQC/CE/FCC etc. should have minimum 5 year warranty	

SIGNAL LIGHTS

A. **Traffic lights (RED, AMBER, and Green)**

#	Component	Compliance (Yes / No)
	Make:	
	Model:	
	Single Source LED type	
1	LED retrofits should comply with the EN12368 standards or other international standards	
2	The LED signal heads are to be compliant with Class A (-15 to + 60) for use in a class A environment,	
3	Should have the luminosity of intensity of 400cd	
4	Should have a medium intensity distribution, a luminous uniformity of 1:10	
5	It should be phantom class 5	
6	Should be impact resistance to 0.51kg dropped from a height of 1.3 meters.	
7	The minimum working life of LEDs should be at least 18,000 hours	
8	Should withstand temperatures ranging from 0 Degree Celsius to 70 Degree Celsius	
9	LED retrofits used to be of low power consumption-based	
10	Size 300 mm dia. Should have minimum 5 year warranty	

Pedestrian Graphical Count down timer

#	Component	Compliance (Yes / No)
	Make:	
	Model:	
1	8-bit microcontroller based or better	
2	Housing should be made of polycarbonate and should be IP65/67	
3	Dimensions 360 mmx 370mm x 220mm	
4	Should comply with EN12699	

5	LED lifetime should be 1,00,000 Hrs. from the date of commissioning	
6	Full graphic and dual-color display	
7	The Vehicular countdown timer should be dual-color, Red for STOP or STP, and Green color for GO.	
8	These should have alternate Red and Balance Phase Time for STOP or	
9	STP in flashing. Alternate Green and Balance Phase Time for GO in flashing	
10	The Pedestrian Countdown timer should be the dual color with REDMAN & balance phase time in flashing and GREEN MAN & balance phase time in flashing. Should have minimum 5 year warranty	

Housing for Lights

#	Component	Compliance (Yes / No)
1	This is also called traffic signal aspects and should have the following features	
2	The color of the signal body and visors shall be black UV stabilized high impact or impact a. Modified Polypropylene.	
3	It should be made of polycarbonate and should have adequate mechanical strength and durability to withstand the conditions of installation, operation, and maintenance.	
4	It shall be capable of withstanding winds of up to 145 km/h.	
5	It shall be made in such a way that it could be retrofitted with a 300 mm LED light in it.	

Poles for Traffic Signals			
#	**Component**	**Minimum Specification**	**Compliance (Yes / No)**
1	Material	GI Class 'B' pipe	
2	Paint	Hot Dip Galvanized after Fabrication with Silver coating of 86 micron as per IS:2629;Fabrication in accordance withIS-2713 (1980)	
3	Height	5-10 Meters, as-per-requirements for different types of cameras & Siteconditions	
4	Pole Diameter	Min. 10 cm diameter pole (bidder to choose larger diameter for higher height)	

5	Cantilevers	Based on the location requirementsuitable size cantilevers to be considered with the pole	
6	Bottom baseplate	Minimum base plate of size 30x30x15cm	
7	Mounting facilities	To mount CCTV cameras, Switch, etc.	
8	Pipes, Tubes	All wiring must be hidden, through tubes/pipes. No wires shall be visiblefrom outside.	
9	Foundation	Casting of Civil Foundation with foundation bolts, to ensure vibration free erection (basic aim is to ensure that video feed quality is not impacted due to winds in different climaticconditions). Expected foundation depth of min.100cms. Please refer to earthing standardsmentioned in the RFP	
10	Protection	Lightning arrester at select sites as per the requirements	
11	Sign Board	Sign board describing words such as "This area under surveillance" (in English and Local language)	

Cables for Traffic Signals

#	Component		Compliance (Yes / No)
	Make:		
	Model:		
1	No's of core	7 and 14 core1.5 sq.mm. 3 Core 2.5 sq. mm.	
2	Materials	PVC insulated and PVC sheathed armored cable with the copper conductor of suitable size as specified in BOQ.	
3	Certification	ISI Marked	
4	Standards	Indian Electricity Act and Rules	
5	IS:1554	PVC insulated electric cables (heavy-duty)	

6.4.20 Automatic E Challan System:

- The proposed system is a comprehensive digital solution for Transport enforcement wing and Traffic Police delivered through an Android based mobile application and a web portal. The system will capture all challans information by infield officer using

mobile device at the time of violation and capture information will be sync to centralized server.

- The system will be integrated with Vahan and Sarathi applications and provides several user-friendly features, covering all major functionalities of Enforcement System. An end-to-end digital solution for multiple stakeholders: ease of operations for Transport Enforcement Officers/Traffic Policemen, increased visibility in operations for the State Transport department and improved support in maintaining compliance for citizens should be considered.
- The system will self-analyze the confidence level of the ANPR conversion. In case the confidence level is above user-configured threshold, the violation will be pushed automatically for eChallan generation.
- It will be possible to store the e-Challans based on the functional and legal requirements in terms of the number of days. The system will not delete the e Challans which are under legal or court procedure. The system will have postal record maintenance facility to keep track of dispatched, returned, refused, etc. e-Challans sent to the violating individuals. The e-Challan generation system will be able to generate e-Challans in local language and English. The Operator will have the option to filter the violations based on the following criteria for generation of Challans:

  a. Number of violations by the same vehicle multiple times

  b. For a particular category (e.g., 4-wheelers) of vehicles

  c. For a particular Thana / police jurisdiction

  d. Paid/Unpaid Challans

  e. Ageing Analysis of Pending Challans

- The system will generate end-of-the-day report of the e- Challans generated. The report will contain the number of e-Challans generated, number of e-Challans paid, pending e-Challans, etc. The system will have the capability to send such reports via email to the designated persons. The system will have robust search functionality to search the violations by violation types, date and time duration, police jurisdiction / thana, operator, hand held device, location, vehicle number, etc. The system will generate statistical reports in terms of bar charts based on various categories.

6.4.20.1 Challan Handheld device

Specifications	Compliance (Yes / No)
Make:	
Model:	

Processor :	latest high speed processor min 800 MHz with suitable operating System	
Memory :	512MB RAM or higher, 1 GB Flash or higher, With expandable micro SD card Capacity min 32GB	
Interface :	Interface : RS232, USB 2.0 Host USB 2.0 Client	
Wireless :	Wireless : WLAN (IEEE 802.11 b/g/n) GSM/GPRS/EDGE/CDMA should support 3G/4G/5G	
Communication:	USB 2.0, Bluetooth	
Power :	must last for minimum 6 hrs of use in the field (Rechargeable battery) suitable mechanism for charging from 220V standard AC powersupply must be provided, Vehicle charger also to be provided	
Printing method:	Width Minimum 3" Print Technology: Direct Thermal, at least 200DPI Print Speed: 60 mm per Second or better Easy paper loading mechanism Media Type: Direct Thermal Receipt Paper	
Rugged Structure	Drop Specification: 5 ft multiple drop Ingress Protection: IP 65 or better	
Camera	5MP Integrated Camera with flash or better	
Display and Keypad	Minimum 3.5" color VGA 640 x 480 resolution QWERTY keypad with long life buttons, touch screen with backlight, must also have option for virtual QWERTY keypad andshould be readable in sunlight.	
Indications	suitable indication on device for charging, low battery, connectivity etc	
Operating Conditions:	Operating Conditions: Temperature (0 – 50 deg C) 5 – 95% RH (Non condensing)	
Dimensions and Weight:	Lightweight and should be easy to hold in the palm	
Storage	expandable micro-SD card capacity min 32GB	
Global positioning System (GPS)	Integrated GPS with A-GPS	
Other Features	login through unique ID, password and biometric data captureReal time clock with Battery backup Embedded e-challan Software e-challan Application: - Required device client software should be developed and installed on each device by the vendor to perform E-challan process on line and off line mode with server as per user requirement. Operating System and application drivers: -	

	Suitable operating system.	
Accessories	User manual , Device cover casing , USB Cable and e-challan Software CD.	
Reader	Contact & Contactless Smart Card Reader and MSR reader, Fingerprint scanner, Integrated Bar Code Reader (1D/ 2D)	
Payment Interface	The device should have IPCI , EMV certified PINPAD as per RBI guideline for accepting payment through Credit / Debit card/NPCI	
Warranty	5 Years	

6.5 Enterprise Management System (EMS)

Sl. No	Technical Specification	Compliance (Yes / No)
	Make · <to be provided by the SI>	
	Model: <to be provided by the SI>	
1	**Complete end to end fault & Performance monitoring** **1. Fault & Performance Monitoring (Network, Server, Cloud, VMs, CCTV, Wi-Fi, all IP network)** **2. Network configuration & Change management** **3. Traffic analysis** **4. Assets Management** **5. Log management** **6. Network zero trust Access** **7. Reporting & Dashboarding with integration** **8. Helpdesk ITSM Tool** **9. IPAM (IP Address Management)**	
2	**The OEM should have a support center in INDIA**	
3	**The solution should be capable of running in Linux platform**	
4	**The tool must be certified by PinkVerify or equivalent for ITIL v3 on incident management, change managementand availability management processes and certificate must be provided when sought**	
5	**The solution should have dual-stack IP support (support both IPv4 and IPv6) and should be completely vendor-agnostic in nature to be able to monitor a multi-vendor environment**	
6	**The solution should be a unified system which can monitor networks, servers, apps and any IT or Non-IT Communicable device (ex.: RF device, etc.)**	
7	**The solution should be completely multi-tenant where in every module and system being used can be assigned to a specific set of users or a group of users.**	
8	**The system should be capable to retrieve and show fault, performance , inventory and SLA data in a single dynamic view with option to export the views into PDF, Word, Excel, HTML etc. formats depending on the need. System should have capability to add any additional information about the nodes via custom fields.**	

9	System should have Node Tags for device grouping and resource/interface tagging for element grouping. Apart from Node Tags additionally system should have options to do device grouping based on default fields and customer fields	
10	Provides the option to have the portal account to the end customers with restricted views limits to their specific infrastructure. System should have the capability to be implement in DMZ and non-DMZ zone with adequate security.	
11	Tool must provide Role based Access Control option	
12	The system should have an integrated ITSM tool from the same OEM. In future, it should be possible to use the service management features like Incident Logging, Viewing, Assignment, Escalation, Reporting, SLA Management etc. in the Service Manager tool GUI. The integration should be bi-directional in nature.	
13	Tool must provide intelligent Email-to-Incident feature in which tool admin has the option to allow certain domains for automatic conversion of emails to tickets. Tool should merge all subsequent email communication for a particular email-to-incident ticket into the same ticket in the form of a message thread. Tool should be intelligent enough to understand email conversation chains for merging emails to a particular incidnt. Merging logic should be not only based on TicketID but also on email sender, cc responses to that email chain	
14	Tool should be able to provide real-time Email, SMS Notification alerts to notify respective users about any changes in ticket state and status. Tool should provide Email Communication Interface to allow technicians to send replies to customers / end users from the tool GUI and Record all the Email Communication in Chronological Order	
15	The integrated ITSM module should have its own Android & IOS app	
16	System should have a bi-directional integrated NCCM tool with option to use NCCM features in future easily by enabling the license for it without having to do any additional installations. The integration should allow assets and topology to sync from the NMS module to the NCCM features for helping in Root-Cause-Analysis of faults	
17	System should have option for multiple options for discovery including IP address based discovery, IP address range discovery, CSV based discovery for bulk discovery and it should allow options to add custom fields to support customer specific data to upload during discovery	
18	The system should fetch topology via SNMP for ARP tables from routers , MAC tables from layer 2 switches, cisco Discovery Protocol, Link Layer Discovery Protocol, Foundry Discovery Protocol or SynOptics Network Management Protocol. The discovery should be automated and continuous.	
19	Discovery has to work intelligently by identifying the device in the network by the given IP range and categorize into network devices and servers with vendor and model details.	
20	Automatically learn devices that supports SNMP, HTTP, Ping, SMTP, POP3, WMI,JMX, SOAP, REST API,PDC, SSH and Telnet along with any required protocol to communicate to the devices.	
21	System should support global threshold and it should have option to define individual resource/interface statistics level threshold	
22	System should have built in self learning algorithms to auto baseline and auto calculate thresholds of components or nodes to enable tool admin to start the monitoring with zero threshold configurations	
23	Configurable parameters like frequency, data duration, resolution duration, sigma based polarity value, reset points should be available	
24	All thresholds should have set point , reset point, polarity , set point message and reset point message for ease of use.	
25	Detect & highlight faults (abnormal situations) in near real-time occurring anywhere within the monitored IT Infrastructure	

26	**Provides Filtering, De-duplication, Holding, Suppression and Correlation capability to let user focus on the critical event that affects the business and business processes**	
27	**Provides multi-level (preferably six-level) Severity definition, will handle events automatically and inform the designated person as per operational requirement**	
28	**System should support separate Rule Engine based alarms apart from the generic threshold.** **a. Should have capability to configure Device Group based, Node Based, Resources/Interface based, Aggregation link based.** **b. On Selection of Nodes/Resources/Aggregation links it have flexibility to filter based on fields available in node information** **c. Rules should have option to apply configuration on top of performance value or based on configured threshold alarms** **d. Rules should have option configure the breach based on min, max and average values** **e. Should have option to configure rules n repeat counters** **f. Should have options to select custom alarm and clear alarm messages for individual configured rules** **g. Should have option to send severity levels like error, warning and information** **h. Notifications support based on configured rules**	
29	**Provides alarm suppression with hold time and aid in prevention of flooding**	
30	**Sends alert via E-mail, SMS, Execute Batch file, SNMP Trap, XML notification, Pop-up window and Audio alert**	
31	**Monitors all traffic from all the interfaces of the network device. Provides traffic Utilization based on individual interface level, nodes level or based on the group by location, branch, departments etc.… as an Avg, Min and Max bandwidth, utilization, throughput or any custom monitoring parameters.**	
32	**Provision to change the polling interval to any frequency depending on the priority till the individual component / resource level like each interface might have the different polling interval in the same device based of the criticality and importance of service customer**	
33	**System should have capability to configure business , non-business hours or custom time polling. These configuration should be available for every device as well as every component in the device.**	
34	**Provision to disable and enable the polling of specific type of devices**	
35	**System should have capability to configure the maintenance period for any device. When device is in maintenance period there is no polling done and the SLA clock on the device is stopped.**	
36	**SLA calculation / Isolation report should be made with the consideration of both the Primary and Secondary link together instead of individual link based. The downtime calculation will be measured when both the links are down for internal reporting and link based for ISP reporting. System should provide the flexible configuration in UI itself based on user needs**	
37	**Provide a notification mechanism that allows administrator to define what notification channel to be used in different time of days, and able to trigger multiple notifications to alert multiple person and actions**	
38	**Provide standard reports that display current status of nodes and interfaces. Reports could be viewed on daily graph (5 minute average), weekly graph (1 hour average minute average), monthly graph (1 hour average) and yearly graph (1 day average)**	
39	**Provide online and offline reports that allow the user to view the present usage of their devices. Reports generates should be exportable in the format of HTML, PDF, Excel and CSV. Allows end-users to browse all reports using any web browser like Internet Explorer, Mozilla Firefox, Google Chrome etc. without the need to install any report specific software**	

40	Automatically generate daily reports that provide a summary of the IT Infrastructure as well as custom Reports and that are automatically sent by email at a pre-defined schedule to any recipient or save into any specific folder or drive.	
41	Supports instant diagnosis of the node status through Ping, Telnet and SNMPwalk	
42	Support Real-Time report generation for checking continuous reachability of target device	
43	System should provide many different types of topology representation. To perform the following: 1. Display physical connections of the different devices being monitored in the system 2. Display flat maps of the entire network or networks in a single view 3. Display customer maps based on user configurations 4. Display maps based on geo locations	
44	Automatically learn IP Networks and their segments, LANs, hosts, switches, routers, firewalls etc. and to establish the connections and to correlate	
45	Provides provision to draw & map user specific network diagram	
46	The tool should have Integrated Web based feature to build Network Diagram, No separate client window to configure network Diagram. The builder should be similar to MS Visio with all pre-loaded shapes and icons.	
47	It should be a Drag & Drop based Network Diagram builder, Dynamically Upload Images, Customizable objects to support multiple vendors, capability to export maps in an XML format and upload to any other system.	
48	Panel View a. Panel view should look similar to the actual device front panel b. System should automatically detect the device model display the right panel without any additional configuration c. Panel should show all the monitored interface with status d. Fan status with live fan icon and LED status for power	
49	Tool should have complete inventory information of the assets discovered along with an option to fetch the target network device EoL / EoS information if required	
50	Tool must support CLI-based network device configuration snapshot management including backup of configuration files, traffic logs, messages etc. , pushing configuration files to target network devices, with option to perform remote firmware upgrades.	
51	The configuration changes to be done on target network devices must follow an approval-based system wherein changes can be performed only after required approvals are passed. Tool must have in-built approval mechanism along with option to integrate with Change Management module of other ITSM tools for the approval process.	
52	Tool must provide option for target CLI-based network device vulnerability detection based on their model number and firmware version. It should also provide options to remedy the vulnerabilities with help of pre-configured scripts for certain vulnearbility types.	
53	Tool must provide option to perform standard compliance checks like PCI-DSS, NIST, DISA etc. across all target CLI-based network devices	
54	Tool must provide an option for taking remote access via Telnet / SSH to target CLI-based Network Devices with an option to record all sessions to capture all commands being executed on the remote devices. The tool must allow session relay wherein a higher-privileged user can view the ongoing CLI session of a lower-privileged user in real-time from the tool GUI. The sessions should be saved for historical analysis with flexible filter options like searching for sessions in which a particular command has been executed.	
55	The proposed monitoring solution should be able to monitor network traffic by capturing flow data from network devices, including Netflow v5 or v9, J-Flow, IPFIX, sFlow, NetStream data and also sampled Netflow data. Solution must be able to	

	store ALL flows without any rollups or loss for retention period - for security and audit purposes.	
56	Should identify which users, applications, protocols, countries, AS numbers, top routers, and top interfaces are consuming the most bandwidth	
57	System should have capability to alternatively capture traffic data via packet capture.	
58	Should be able to associate traffic coming from different sources to application names	
59	Should be able to receive flows from non-SNMP-enabled devices, like VMware vSwitch	
60	Should monitor Type of Service (ToS), Differentiated Services Codepoint (DSCP), and Per-Hop Behavior (PHB),BGP AS and NEXT HOP	
61	Should provide flow analysis with 1-minute granularity and The solution should be able to monitor up to 5 million flows per second, and should employs advanced optimization methods	
62	Tool should allow QoS monitoring of WAN links across multiple technologies like IPSLA, RPM, NQA etc. across multiple protocols like HTTP, TCP, FTP, DNS etc.	
63	QoS paramters should include link response time, link-level latency, link-level packet loss, link-level jitter, Round-Trip-Time etc.	
64	Should monitor Class-Based Quality of Service (CBQoS) to find out if traffic prioritization policies are effective and if business-critical applications have network traffic priority. Should also support CBQoS Nested policies	
65	Tool should have option to collect and store system logs from target devices including firewalls, routers, switches, WLC, servers, applications & databases	
66	Tool should have multiple filtering options for incoming system logs based on target device, log_ID, severity, level, message, OS type, application / database etc.	
67	Tool should have option to export specific syslog messages to users via email / SMS	
68	System should support VM, Hypervisor and Cluster monitoring from different vendors like VMWare, Citrix, Nutanix, Linux etc.	
69	System licensing should be based only on Physical Hosts and not charge separately for individual guest VMs running on VM Hosts	
70	System show have capability to monitor availability and performance of industry standard web server like IIS / Tomcat / Apache / Jboss, email server like Exchange / Zimbra / Lotus Notes, and databases like Oracle / MSSQL / MySQL / PostgreSQL etc.	
71	System show have capability to monitor HTTP service,HTTPS service,FTP server statistics, POP/SMTP services,ICMP services or any customer specific port based systems	
72	Cover geographically distributed networks through multi-level scalable distributed deployment architecture	
73	Ability to add new pollers at no extra cost.	
74	The tool should have option to be deployed in HA mode (High Availability) for redundancy purpose	
75	Integration should provide the option in both north as well as south bound integration on each module level. Any fault details should be able to send to third party CRM, Customer Portal, UNMS or even EMS if needed using the Trap, XML and even direct database query integration	
76	Provide open APIs in the system which can be used by customers for integrating their own systems. Integration should provide the option in both north as well as south bound integration using multiple options like RestAPI, XML, SOAP, Corba etc. on each module level. Any fault details should be able to send to third party CRM, Customer Portal, UNMS or even EMS if needed using the Trap, XML and even direct database query integration	
77	The system should allow remote access to the internal network via a Zero Trust system and no use of VPN or agents.	

78	**Only specific protocols like SSH, RDP, Telnet , VNC which are essential for remote access should be allowed**	
79	**All the actions taken during the remote access should be recorded and have ability to audit them later.**	
80	**All remote access should be authenticated and all devices a user has access should be pre-allocated**	
81	**The system should have ability to authenticate access to any device via Single sign on and password should not be exposed to users**	
82	**All CLI session should have command control, any command that is not authorized cannot be used and session should be terminated**	
83	**Administrator should be able to view the live session of any ongoing session and can terminate them also**	
84	**Any file being transferred should be via the Zero trust system. File will be scanned for virus and only then be transferred to the target location**	
85	**Time based; temporary users should be configurable in the system**	
86	**IPAM solution should have complete IP discovery, IP management with historical tracking**	
87	**IPAM should have IP Grouping, Subgrouping and role and privileged based access.**	
88	**Support both IPv4 and V6 along with IP Classes and VLSM based**	

6.6 Citizen Engagement System : Creation of Online and Mobile Applications

SMART captures the important attributes of Good Governance i.e., Simple, Measurable, Accountable, Responsive and Transparent governance.

ICT in governance has been experienced in the form of e-Governance, which redefined the way Governments work, share information, engage citizens and deliver services to external and internal clients for the benefit of both government and the clients that they serve.

Governments harnesses information technologies to reach out to citizens, business, and other arms of the government to: a)Improve delivery of services to citizens, businesses and employees b) Engage citizens in the process of governance through interaction c) Empower citizens through access to knowledge and information and d) Make the working of the government more efficient and effective

This results in enhanced transparency, convenience and empowerment; less corruption; revenue growth; and cost reduction.

Authority intends to implement a robust Smart governance & citizen services solution for delivering efficient and effective citizen centric services as well as improving municipal finance/expense management and administrative functions.

The Smart governance solution, while modular, should be capable of providing all the functionality described in this section as an integrated platform.

The SI shall ensure that all the modules under Smart Governance are integrated with the overall project. SI shall create an enabling platform to link the relevant features with the Citizen Services.

The applications designed and developed for the departments concerned must follow best practice and industry standards. In order to achieve the high level of stability and robustness of the application, the system development life cycle must be carried out using the industry standard best practices and adopting the security constraints for access and control rights. The solution should comply to the below standards as applicable:

(a) At least comply with the published e-Governance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and

(b) The Smart governance solution shall be of leading industry standards and as per requirements mentioned in IS 18006 (Municipal Governance Reference Architecture).

(c) Shall comply to applicable elements of data layer reference architecture (IS 18002) as well as IS 18000 (UNIFIED DIGITAL INFRASTRUCTURE – ICT REFERENCE ARCHITECTURE (UDI-ICTRA), Section 8

Should build an integrated Collaboration Platform to provide all citizens services on a single platform. Services that are universally accessible and that follow an international standard for accessibility and operational or to be made operational by other Government or approved agencies shall be made available through the CCP. Citizen engagement and Grievance Redressal Management Systems with back-end workflow.

The principal objective of CCP is to create one all-inclusive system which allows citizens / tourists/ visitors/ stakeholders to access various government services and information. Key functionalities of CCP include:

- Improving delivery of services to citizen and tourists, businesses and employees
- Engaging citizens/ stakeholders in the process of governance
- Empowering citizens/ stakeholders through access to information
- Improving government functioning across departments – making it more efficient and effective

The envisaged benefits post implementation of CCP include enhanced transparency and accountability, increased revenue, reduced cost, empowerment of citizen and lesser time for service delivery, ease of multi departmental operations for a cause.

By implementing CCP following benefits are envisaged,

For City Authorities

- Digital portfolio of city services
- Better citizen connect
- Efficient and effective delivery of citizen services
- Creating positive social impact
- Reduced cost of delivery of services

For Citizens

- 24*7 Service Access
- Time saving
- Improved connect with city authorities
- 24*7 information dissemination
- Multiple services on a single platform
- Chatbot

The principal objective of CCP is to create one all-inclusive system which allows citizens / tourists/ visitors/ stakeholders to access various government services and information. Key functionalities of CCP include:

- Improving delivery of services to citizen and tourists, businesses and employees
- Engaging citizens/ stakeholders in the process of governance
- Empowering citizens/ stakeholders through access to information
- Improving government functioning across departments – making it more efficient and effective

The envisaged benefits post implementation of CCP include enhanced transparency and accountability, increased revenue, reduced cost, empowerment of citizen and lesser time for service delivery, ease of multi departmental operations for a cause.

Key Functional Requirements - Collaboration Platform

City Collaboration platform should provide below information in the form of Audio/ Video/ image/ GIS map/ text.

- "About Puducherry" will provide details about Puducherry city and will have dedicated sections for about the city, history of Puducherry, how to reach, climate, local cuisines, festivals, Important Business locations, places of interest, art and craft, facts at a glance, where to stay, where to eat, places of interest, heritage spots, weekend getaways, places to visit, best time to visit, gallery (Photos & videos), etc. few of these points have been elaborated below in detail.
- "Explore City" giving details about the city, history, how to reach, cuisine, festivals, Important Business locations, places of interest, Beaches, art and craft (Add to Favorite, Get Directions, About, get there nearby and each linked with City GIS Map and Photos of concerned location)
- "Facts at a Glance" giving details about area, population, religion, linking roads, postal code, longitude, latitude, area, altitude, population, literacy rate, STD code, average rainfall, villages, language and the different seasons and reasons to visit.
- "Tourism destination" giving details on tourism experience (Add to Favourite, Get Directions/Driving Directions, About, get there nearby and each linked with City GIS Map and Photos of concerned location) heritage spots, pilgrim destination, nature discovery, heritage, highway, adventure spots, Beaches, Nearby places to visit, Places to Stay etc.
- City Collaboration Platform will provide the web-link of Tourism Development Corporation (PTDC) portal for booking the Puducherry State tourism packages.
- City has many artifacts, memoirs and items with historic perspectives and are available in designated markets in and around the many important places of interest in the city. A list of unique memoirs and the connected stores are to be listed through mobile apps showing distances from current location, etc.
- "Cultural events calendar" section will provide the list of cultural events within city including dates, venues and details of the event.
- "Tenders" will provide the list of PSCDL tenders in downloadable format.
- "Key Personnel-staff directory" will have the details (such as emails, contact information, designation, job profile, office address etc.) of PSCDL stakeholder members, Elected Political Members, Mayor, Municipal Commissioner and all Officials
- "Important GOs / Policies" section will have the list of all important and relevant government orders and policies.
- "Downloads" section will provide the list of important document in downloaded format to the user.
- "Recruitment" section will provide the current job openings in PSCDL and their stakeholders departments.
- "Educational Institutions" listings, including location, contacts, courses etc.
- "Sports Facilities" will provide the details of facilities available within the city including list of play grounds, details on in-door or out-door facilities, list of tournament / event dates etc. Please note that this section will provide only information.
- "Ward Information" section will provide the below information:
    - Municipal officers contact.
    - Water supply information / announcements.
    - Power supply information / announcements.
    - Garbage collection schedule.
    - List of schools, community centres, playing ground, parks etc. and the contacts for bookings.

- "Health Services" will provide the details of hospitals including contacts, address, emergency contacts, available facilities and OPD timings. It will also provide the list of ambulance services available in the city with contact numbers.
- "Emergency Services" module will have the contact details of below emergency services.
    - Ambulance
    - Fire
    - Police
    - Traffic

All the contacts shall support for "dial to call feature" from a page.

- "Social Networking & City-wide Collaboration" will help citizens to communicate through social networking platform such as Twitter / Facebook / WhatsApp etc.

    - Current news, events will enable citizens to get live feeds of various activities & events in the city.
    - Feedback/ inputs / opinions will help citizens to collaborate and provide inputs/ opinions on various policy related aspects, local governance aspects, feedback on specific issues etc.
    - Search tools will enables citizens / tourists to search for desired information available in the City Collaboration Platform.

Collaboration platform should be integrated with below modules but not limited below list.

- Environment information from nearest available Environment sensor.
- Citizen / Tourists can view their e-challan in case of any traffic violation.
- Integration with Property Tax System
- Water Supply and sewerage system
- Birth and Death, Marriage Registration, Trade Licensing etc.

Key Functional Requirements - Collaboration Platform

Sl. No.	Specifications	Compliance (Yes / No)
	Citizen Engagement Application	
1	The application shall accept requests or inquiries from the citizens and track those requests from different channels such as phone, e-mail, SMS, Web Portal, Chatbot, VoIP Call, Smart Phone Application (City App) & social media (Facebook, Twitter.) etc.	
2	It should integrate all service requests through Voice & IVR based system for efficiently managing the citizen grievance request	
3	The operator should be able to chat/reply to any queries raised through different channels via the same channel	
4	The application shall allow the user to select service request category type or use auto-filled information for incident creation. A unique service transaction number should be assigned for each incident after a service request is created.	

5	The application shall auto-populate fields based on previous calls or known data from other channels.	
6	The application shall capture different types of input data, including but not limited to: date, citizen profile data, issue type, issue description, time of day the grievance occurred, location, etc.	
7	The platform should have the ability to view map of service requests on top of a City GIS base map and display service requests and associated data (service request number, status, short description, field assets and workforce) on the same map.	
8	The application should provide information regarding the exact location of the service request (e.g., actual location of garbage or downed tree).	
9	The application should automatically determine duplicate requests and associate a request with multiple citizens.	
10	The application must have the ability to display the citizen's previous interactions from different channels using search feature and view citizen's previous service request status.	
11	The application should have the ability to display "top" grievance types based on historical trends ranked according to the most viewed and most relevant service request.	
12	The application should provide the operator the ability to view and attach files (such as PDF) and other documents (e.g., images)	
13	The application should prevent a request from being closed until all associated actions are completed.	
14	The application should have the ability to dispatch a service request to the workforce, a particular department or an outside agency.	
15	The application should provide a set of standard reports that will provide statistical reporting for open, closed, escalated, priority, completion time, based on address and location.	
16	The application should have a dashboard module that can give a quick and easy view to know overall Grievance details: trend, status, channels, incident trends, response of department and feedback.	
17	The application should provide the dispatch the incident to City Command Centre, City Emergency Operation Centre, relevant department application based on the nature of the grievance/complaint.	
18	The application should provide the operator with the facility to view all dialled, missed, received calls.	

19	The application should allow the administrator to define SLAs for all the incidents.	
20	The application should allow the administrator to add, edit and delete various department	
	Citizen Mobile App	
21	It shall integrate the Citizen Service request and also provide visibility to the citizen of the various city notifications.	
22	Key Features of the app should include:	
23	• Incident Reporting	
24	• Complaints Tracking	
25	• City Services – Parking, Transport	
26	• e-Governance Services	
27	• Bills Payment	
28	• News	
29	• Events	
30	• Notifications	
31	• Emergency	
32	• Chatbot	
33	The Application shall integrate Citizen Grievance and Compliant from various channels – social media through Keywords, Mobile App based reporting as a crowd source, Citizen Calls, etc.	
34	Citizen app shall provide capability to citizen to report incidents across various grievances covering emergency, garbage collection, accidents, water leakage, electricity outage etc. Such requests shall be integrated with ICCC platform, and the service delivery will be automated through the ICCC functions.	
35	City App should allow to make SOS calls with location and video snapshot	
36	City App should be capable to schedule waste collection from Citizen's location	
37	City App should allow to search the parking space across the city	
38	City App should allow to view different modes of transport available for Citizen in the city	
39	City App should allow the citizens to receive the traffic related notification and be updated about the traffic condition in selected areas	

40	City App should allow citizens to pay utility bills and taxes	
	City Web Portal	
41	It should provide a single view to the citizen for engaging with the city departments.	
42	It should provide live update of the City Service and also act as a foundation for Citizen to register the identity and download the Citizen App.	
43	It should also provide interface for the citizen to request through Email, Chat Services so that the citizen can also call for service through these channels.	
44	Email and chat services: service request and distribution to the right operators.	
45	Portal should allow citizen to use different City services by selecting services categories	
46	The Web portal should provide the citizen the facility to report Civic grievances by selecting grievance categories and subcategories by attaching Image or Video to support the Grievance request	
47	The citizen can view the history and status of all the complaints that have been requested.	
48	The Citizen should be able to see the GIS view of the city and can find POIs as when required	
49	The web portal should have Content Management System to create content and publish content and it will integrate with all public Channels for News and other feeds.	
50	The web portal should have CMS that shall provide a role-based user access mechanism where an administrator can create and manage users, user groups, roles, and role permissions.	
51	The CMS should support login module using which content authors will be able to login.	
52	Login module should have forgot password mechanism. In case user forgets the password/wish to reset a link should be sent to user's registered Email address from where password can be reset.	
53	CMS should support integration with Directory Services (supporting LDAP) to manage users and their preferences. CMS should also support latest security certificates like SSL 3.0	
54	CMS should be able to publish content to any external portal apart from its native portal	

55	CMS shall support the creation, modification, and deletion of templates to enable easy management of site and page layout and navigation	
56	CMS should contain a WYSIWYG editor and provide standard Word authoring features (also known as a Rich Text Editor) to enable an editor to add and format text, links, and images to content areas, create tabular layouts within a text area and apply styles without needing HTML skills	
57	CMS should support drag and drop feature to enable easy management of content. The CMS shall support the following minimum preview and publication functions: -	
58	a) Preview only on CMS (not visible to users)	
59	b) Save as unpublished (draft)	
60	c) Preview on Portal	
61	d) Send for approval	
62	e) Approve	
63	f) Publish after approval (i.e., after successful completion of the approval workflow)	
64	g) Unpublish (save as unpublished, not visible to users)	
65	h) Publication scheduling	
66	i) Publication expiration date (automatic unpublish)	
67	CMS shall contain a content approval workflow to enable the approval of modifications (create, modify, delete) before publication (i.e., before becoming visible to the public)	
68	CMS shall support Administrator (or a designated user with an appropriate permission level) to assign and reassign users to workflow tasks (i.e., define the targets within the workflow)	
69	CMS shall support the creation and application of styles using Cascading Style Sheets (CSS) enabling the swift alteration of the look and feel (colour, font, image size and positioning, link attributes, table properties). Graphics should be avoided altogether regarding navigation (e.g., no navigation buttons - these should be text, which gets its look and feel through CSS).	
70	CMS shall include a social media integration module that allows configurable publishing of content (pages, interactive data visualizations, images, videos) to a variety of social media (Facebook, Twitter, Google+, LinkedIn, Pinterest, Tumblr, etc. CMS should also support publishing of content specific to mobile app if required	
71	The CMS should have the capability to create and deploy content on different portals with same or different branding	

72	The CMS shall support the Unicode character set (UTF-8)	

6.7 Smart Poles

Proposed ICT Solution:

It is now proposed to install smart poles in different locations of the city which shall be in turn connected to the ICCC. The various components that are envisaged in the said smart poles are as follows:

- Fixed Box Camera
- Smart Lighting
- AQM : (Environmental Sensor, Weather Sensors, Rain Gauge Sensors)
- Public Address System
- Digital Bill Board
- Emergency call box
- Wi-Fi
- 5 G ready

Scope of work:

The scope includes procure, supply, install and commission smart poles including all civil foundation works and provide the data and power connectivity for the said poles.

6.7.1 Smart Pole Specification

No	Specification	Compliance (Yes / No)
	Make:	
	Model:	
1.	Smart pole should be able to meet city aesthetic requirement and it should visually appealing. It should easily blend-in into city street pole master plan.	
2.	Pole Height requirement is 12-15 meters. TRAI and DOT guidelines to be followed as the pole will be used as a telecom site.	
3.	It should be able to support telecom technologies like 5G, GSM, WCDMA, LTE and Wi-Fi.	
4.	It should be possible to support LED luminaries from reputed OEMs.	
5.	Smart pole should be designed as per telecom standards of India and specifically Puducherry weather conditions such as wind speed, climate, aesthetic.	
7.	The allowed diameter will be as per the BIS regulations and wind speed requirement	

8.	All cabling, cooling/heating etc should either be via/inside the pole or should be camouflaged (aesthetically concealed) so that it is not visible from outside.	
11.	The minimum power backup requirement is 1 hrs for all equipment	
12.	It should be possible to provide multiple color options as asked by city Authority as per city light pole colors	
13.	It should be possible to house radio units with integrated antenna, MW /optical transmission unit, SMPS (AC to DC convertor), batteries, controllers, power distribution etc. either inside the smart pole or should be camouflaged (aesthetically concealed) so that it is not visible from outside	
15.	It should be possible to provide light connection in daisy chain with separate MCB for lighting	
20.	The cabinet where electrical electronics equipment is store should be IP 67 compliance or better	
22.	The ambient temperature requirement is 0-50 degrees	
23.	The overall power budget for smart pole should not exceed 2KW (lights) or as per standards.	
24.	It should support minimum two light arm per smart pole. However, the same may vary depending on location to be surveyed and finalized by the selected bidder.	
25.	The minimum life requirement of above smart pole structure is 10 years	
26.	The Concessionaire should not use any banned /restricted material as per Indian regulations. Should have 5 year warranty	

6.7.2 Digital Bill Board

No	Specification
1	The Bill boards should be hanged at the height of at least 5 meters or above, however the uniformity should be maintained on all the poles. Should have minimum 5 year warranty
2	The Smart Billboard will be operated from Command & Control Center
3	It should have provision for incoming power input cables and fiber connectivity
4	It should be Vandal Proof ; IP Level IP67 or better
5	It should have display of minimum (80 Inches +/- 5%) , Rectangular shape (2mx1m)+/- 5% as per city regulations.

No	Specification
6	It should be Aesthetical & Camouflaged finish with respect to environment
7	Pixel Pitch 10 mm or Lower, Lower pixel pitch is better, LED Configuration RGB 3 in 1 SMD
8	Pixel Density Minimum 10,000 pixels per sqm or higher
9	Viewing distance Suitable for readability from 40 Mtrs. or more at the character size of 240mm, from moving vehicles
10	Viewing Angle H 140 deg / V 90 deg or better with Refresh Rate>1920 Hz or better
11	Temp Range 0 to +50 Degrees C or better; Gray Scale Processing 12 Bit or better
12	Brightness (Calibrated) 5000 cd/m2 or better; Contrast Ratio 2500:1 or better
13	Maximum Power Consumption 825 w/sqm or lower; Power Input 100 ~ 240 VAC
14	Dimming Capability Auto dimming capability to adjust to ambient light level (sensor based automatic control)

6.7.3 Environmental Sensors

Environmental pollution, particularly of the air, is nowadays a major problem that unknowingly affects lives in the cities. Air Pollution is defined as the presence of contaminants or pollutant substances in the air that Interfere with human health or welfare, or produce other harmful environmental effects and it is important that the citizens know of the air that they breathe.

Citizens & visitors to City can enjoy unique experiences that keep them feeling good by knowing city's environment condition at different locations.

Environmental Management solutions can be used to determine the quality of air (And water, SWM, Energy,) and the environmental parameters to enable a deeper understanding of the polluting sources like vehicles, industries, construction or natural reasons etc.

It is recommended to deploy Environment Sensing Units spread across a region, to create a larger data pool leading to better understanding of spatial and temporal trends in air pollution to take measures for corrective actions.

Key Issues

Rapid urbanization, which strains basic infrastructure, coupled with more frequent and extreme weather events linked to global climate change is exacerbating the impact of environmental threats. Common environmental threats include flooding, tropical cyclones (to which coastal cities are particularly vulnerable), heat waves and epidemics.

Owing to the physical and population density of cities, such threats often result in both devastating financial loss and deaths. Making cities more resilient against these environmental threats is one of the biggest challenges faced by city authorities and requires urgent attention.

Indicative Key Outcomes and KPIs

- Improved monitoring of city environmental Parameters
- Temperature, Humidity
- Ambient Light
- Level of Noise Pollution
- CO, NO2.
- Mosquito density
- Water quality of public surface water bodies
- City to add/ update based on city objective.
- Improved communication with citizens through other city solutions like City App, PA system, ECB etc. based on city environmental parameters
- Improved management of pandemic situations in the city

Key components

A typical Environment Management solution may consist of the following components. One may not need all of these or may be even more than these based on the technology and design used.

Sensors to measure the pollutants and other environmental parameters

Electronic displays to communicate the measured levels to the citizens

IoT gateways, network switches, copper, fiber optic or wireless connectivity to interconnect the local system components and also to the datacenter/cloud.

Desktop application for administration, operation and service/repair.

Functional Requirements

The SI shall;

a) Install environment sensors (as per the functional requirement) to display environment related information at various strategic locations through variable message display (VMD) system.
b) The environment sensors shall be integrated with the ICCC to capture and display/ provide feed on Temperature, Humidity, Pollutants like So[X], No[X], Co[X], PM2.5, PM10, Noise Pollution, etc. The data it collects should be location-marked.
c) Various environment sensors should sense the prevailing environment conditions and send the data to the ICCC where real time data resides and the same shall be made available to various other departments and applications for decision making.
d) This information should be relayed instantaneously to signage – large, clear, digital-display screens which let citizens know regarding the prevalent environmental conditions.
e) Environmental sensors recorded data shall be used by Smart Environment Mobile application to enable user for alarm management and notification of environmental details on real time basis.
f) Mobile app should be developed for Grievance Redressal of Citizen – where citizen can take the picture, upload the same with Geo Tagging. The complaint should be

automatically forwarded to the respective staff, with escalation within specified timelines supported with multilingual text to speech, speech to text and speech to speech systems.

g) The system should provide ability to ;

i. View Air Quality Index across city, levels of various constituents (CO, CO2,SO2,NO2, PM10) etc.
ii. Correlate the data emanating from various Environmental sensors in different areas of city with respect to city mobility/traffic
iii. Communicate the levels of AQI and Noise in locality to citizens, businesses and industry on daily basis via Citizen Mobile App.
iv. View the hotspots across various areas in city where high noise cases are reported by citizens
v. Predict the poor quality of air and water on various dimensions like timelines, seasons where there is high density of markets, industry or shops.
vi. Spread awareness at chronic location/spots identified over VMD, website, mobile app, WhatsApp etc.
vii. Allocate and monitor noise complaint to the on-field squad to take intervention as per defined SoPs.
viii. View the heat-map of noise pollution over different dimensions
ix. Educate the masses using bulk SMS, email and messages about best practices
x. Send the aggregated data of AQI and Noise to concerned authority to address the problems through policy.
xi. Address the noise issue by issuing advisory to local businesses, marriage gardens etc.
xii. View hospitals and staff/beds/medicine availability in real time.
xiii. Provide City wide Hot-Spot Analysis based on lab reports.
xiv. Correlate cause like the impact of water quality, air quality, stress on diseases reported at primary, secondary and tertiary care.
xv. Do the predictive analytics over the past data to predict the outbreak of disease in community
xvi. Coordinate with Hospitals, Labs and on-field staff in real time using handheld devices etc. Ability to coordinate with Hospitals, Labs and on-field staff in real time using handheld devices etc.
xvii. View heat-map of different diseases on different dimensions over city maps
xviii. Provide awareness drive for citizens in targeted areas through email, SMS, WhatsApp, VMD etc. as per preventive healthcare SoPs
xix. Coordinate with Sanitation Department and other line department to take corrective action.

The Sensors should be ruggedized to be deployed in open air areas on streets and park . They should be able to read and report at least the following parameters

- Temperature, Humidity
- Ambient Light, Sound
- CO, NO2
- Mosquito density

Install environment sensors (as per the functional requirement) to display environment related information at various strategic locations through variable message system
● **The environment sensors shall be integrated with the ICCC** to capture and display/ provide feed on Temperature, Humidity, Pollutants like SoX, NoX, CoX, etc PM2.5, PM10, Noise Pollution. The data it collects is location-marked.

● Various environment sensors shall sense the prevailing environment conditions and send the data to the integrated control system where real time data resides and the same shall be made available to various other departments and applications for decision making.

● Then this information is relayed instantaneously to signage –large, clear, digital-display screens which let citizens know regarding the prevalent environmental conditions.

● The data should be collected in a software platform that allows authorized software applications to read that data. Various environment sensors shall sense the prevailing environment conditions and send the data to the integrated control system where real time data resides and the same shall be made available to various other departments and applications for decision making.

● SI can also make use of the nearby Variable messaging displays wherever possible (need to be finalized post detailed survey of locations).

● The sensor management platform should allow the configuration of the sensor to the network and location details etc.

Functional Requirements (AQM on smart Pole and standalone Environmental Sensor)

S. No.	Description	Compliance (Yes / No)
1	Shall be ruggedized enough to be deployed in open air areas on streets and park	
2	Environmental Sensor station shall be housed in a compact environmentally rated outdoor enclosure. It shall be an integrated module which shall monitor overall ambient air, noise quality, weather etc.	
3	Mounting of the environmental sensor module shall be co-located on streetlight pole or shall be installed on a tripod/standalone pole.	
4	Environmental sensor station shall monitor following parameters and include the following integrated sensors inside one station: • Carbon Monoxide (CO) sensor • Ozone (O3) sensor • Nitrogen Dioxide (NO2) sensor • Sulphur Dioxide (SO2) sensor • Carbon Dioxide (CO2) sensor • Particulate/SPM Profile (PM10, PM2.5, and TSP) sensor • Temperature sensor • Relative Humidity sensor • Wind Speed sensor • Wind Direction sensor	

	• Rainfall sensor • Barometric Pressure sensor and • Noise sensor	
5	Solution shall display trends of environmental parameters based on user specific time periods.	
6	Data shall be collected in a software platform that allows third party software applications to read that data.	
7	Solution shall display real time and historical data in chart and table views for dashboard view of the Client.	
8	Alarms shall be generated for events where the environmental parameters breaches the safe or normal levels.	
9	The sensor management platform shall allow the configuration of the sensor to the network and also location details etc.	
10	The platform shall comprise of an Industrial PC running latest version OS and compatible software.	
11	Data logging with central Monitoring System will be through GPRS/TCP-IP from all the AQMS system and shall have an ability to program and log channels at different intervals and shall have a capability of averaging and displaying real time data and averaged data over a period of 1 min, 10 min, 30 min, 1 hr, 4 hr, 8, hr, 24 hr and so on.	
12	Real time or averaged data can be viewed quickly and easily through a remote interface on the central computer.	
13	System shall be able to perform nested calculations vector averaging and rolling averages	
14	The platform shall have a feature for viewing instantaneous and historical data in the form of tables and graphs either locally or from a remote client.	
15	Data retrieval from CMS via USB and DVD shall be possible.	
16	Generation of reports for pollution load, wind rose etc.	
17	Alarm annunciation of analyzer/sensor in abnormal conditions	
18	The environment sensors shall be integrated with the integrated command and control centre system to capture and display/ provide feed. The data it collects is location-marked.	
19	Various environment sensors shall sense the prevailing environment conditions and send the data to the integrated control system where real time data resides and the same shall be made available to various other departments and applications for decision making.	
20	Information shall be relayed to signage – large, clear, digital-display screens which let citizens know regarding the prevalent environmental conditions.	
21	Further environmental sensors recorded data shall be used by Mobile application to enable user for alarm management and notification of environmental details on real time basis.	

Technical Requirements

S. No.	Description	Compliance(Yes/No)
1	**Carbon Monoxide (CO) Sensor** • CO sensor shall measure the carbon monoxide in ambient air • Range of CO sensor shall be between 0 to 1000 PPM • Resolution of CO sensor shall be 0.001 PPM or better • Lower detectable limit of CO sensor shall be 0.040 PPM or better • Precision of CO sensor shall be less than 3% of reading or better • Linearity of CO sensor shall be less than 1% of full scale or better • Response time of CO sensor shall be less than 60 seconds • Operating temperature of CO sensor shall be 0°C to 60°C • Operating pressure of CO sensor shall be ±10%.	
2	**Ozone (O3) Sensor** • O3 Sensor shall measure the ozone in ambient air • O3 Sensor shall have a range of at least 0-1000 PPB • Resolution of O3 sensor shall be 0.001 PPM or better • Lower detectable limit of O3 sensor shall be 0.001 PPM or better • Precision of O3 sensor shall be less than 2% of reading or better • Linearity of O3 sensor shall be less than 1% of full scale • Response time of O3 sensor shall be less than 60 seconds • Operating temperature of O3 sensor shall be 0°C to 60°C • Operating pressure of O3 sensor shall be ±10%	
3	**Nitrogen Dioxide (NO2) Sensor** • NO2 Sensor shall measure the Nitrogen dioxide in ambient air • NO2 Sensor shall have a range of at least 0-10 PPM • Resolution of NO2 sensor shall be 0.001 PPM or better • Lower detectable limit of NO2 sensor shall be 0.001 PPM or better • Precision of NO2 sensor shall be less than 3% of reading or better	

	• Linearity of NO2 sensor shall be less than 1% of full scale • Response time of NO2 sensor shall be less than 60 seconds • Operating temperature of NO2 sensor shall be 0°C to 60°C • Operating pressure of NO2 sensor shall be ±10%	
4	**Sulphur Dioxide (SO2) Sensor** • SO2 Sensor shall measure the Sulphur dioxide in ambient air • SO2 Sensor shall have a range of at least 0-20 PPM • Resolution of SO2 sensor shall be 0.001 PPM or better • Lower detectable limit of SO2 sensor shall be 0.009 PPM or better • Precision of SO2 sensor shall be less than 3% of reading or better • Linearity of SO2 sensor shall be less than 1% of full scale • Response time of SO2 sensor shall be less than 60 seconds • Operating temperature of SO2 sensor shall be 0°C to 60°C • Operating pressure of SO2 sensor shall be ±10%	
5	**Carbon Dioxide (CO2) Sensor** • CO2 Sensor shall measure the carbon dioxide in ambient air • CO2 Sensor shall have a range of at least 0-5000 PPM • Resolution of CO2 sensor shall be 1 PPM or better • Lower detectable limit of CO2 sensor shall be 10 PPM or better • Precision of CO2 sensor shall be less than 3% of reading or better • Linearity of CO2 sensor shall be less than 2% of full scale • Response time of CO2 sensor shall be less than 60 seconds • Operating temperature of CO2sensor shall be 0°C to 60°C • 6Operating pressure of CO2 sensor shall be ±10%	
6	**Particulate Profile Sensor** • Particulate profile sensor shall provide simultaneous and continuous measurement of PM10, PM2.5, SPM and TSP (measurement of nuisance dust) in ambient air	

	• Range of PM2.5 shall be 0 to 230 micro gms / cu.m or better • Range of PM10 shall be 0 to 450 micro gms / cu.m or better • Lower detectable limit of particulate profile sensor shall be less than 1 µg/m3 • Accuracy of particulate profile sensor shall be <± (5 µg/m3 + 15% of reading) • Flow rate shall be 1.0 LPM or better • Operating temperature of the sensor shall be 0°C to 60°C • Operating pressure of the sensor shall be ±10%	
7	**Temperature Sensor** • Temperature sensor shall have the capability to display temperature in °Celsius • Temperature range shall be -10° to +80°C • Sensor accuracy shall be ±0.3°C (±0.5°F) or better • Update interval shall be 10 to 12 seconds	
8	**Relative Humidity Sensor** • Range of relative humidity sensor shall be 1 to 100% RH • Resolution and units of relative humidity sensor shall be 1% or better • Accuracy of the sensor shall be ±2% or better • Update interval shall be less than 60 seconds • Drift shall be less than 0.25% per year	
9	**Wind Speed Sensor** • Wind speed sensor shall have the capability of displaying wind speed in km/h or knots • Range of sensor shall be 0-60 m/s • Accuracy of wind speed sensor shall be ±5% or better • Update interval shall be less than 60 seconds	
10	**Wind Direction Sensor** • Range of the wind direction sensor shall be 0° to 360° • Display resolution shall be 16points (22.5°) on compass rose, 1° in numeric display • Accuracy shall be ±3% or better TR 6.70 Update interval shall be 2.5 to 3 seconds	
11	**Rainfall Sensor** • Rainfall sensor shall the capability of displaying level of rainfall in inches and milli meter	

	• Daily Rainfall range shall be 0 to 99.99" (0 to 999.8 mm) • Monthly/yearly/total rainfall range shall be 0 to 199" (0 to 6553 mm) • Accuracy for rain rates shall be up to 4"/hr (100 mm/hr) or ±4% of total • Update interval shall be less than 60 seconds • 0.02" or (0.5mm) of rainfall shall be considered as a storm event with 24 hours without further accumulation shall end the storm event	
12	**Barometric Pressure Sensor** • Barometric pressure sensor shall have the capability of displaying barometric pressure in Hg, mm Hg and hPa or mb • Range of barometric pressure sensor shall be 540 hPa or mb to 1100 hPa or mb • Elevation range of the barometric pressure sensor shall be -600 m to 4570 m • Uncorrected reading accuracy shall be ±1.0 hPa or mb at room temperature or better • Equation source of the sensor shall be Smithsonian Meteorological tables • Equation accuracy shall be ±0.01" Hg (±0.3 mm Hg, ±0.3 hPa or mb) or better • Elevation accuracy shall be ±10' (3m) to meet equation accuracy specification or better. • Overall accuracy shall be ±0.03" Hg (±0.8 mm Hg, ±1.0 hPa or mb) or better. • TR 6.85 Update interval shall be less than 60 seconds	
13	**Noise Sensors** • Noise sensor shall detect the intensity of the ambient sound in a particular area • Noise Sensors shall be installed for the outdoor applications • Noise sensor shall be able to identify the areas of high sound intensity ranging from 30 dBA to 120 dBA • Noise sensor shall have resolution of 0.1 dBA	
14	Integration with ICCC platform, City Portal and Mobile applications	

6.7.4 Emergency Call Box:

No	Specification	Compliance (Yes / No)
1	ECBs to be installed one each at smart poles.	

No	Specification	Compliance (Yes / No)
2	They shall mostly be mounted on a pole in a housing with a canopy along with the ECB.	
3	The unit shall preferably have a single button which when pressed, shall connect to the ICCC or to the nearest/any of the control room having the local control console.	
4	These should also be capable of being used for Public Address.	
5	The PA control desk to be used for communicating with ECB	
6	Construction: Cast Iron/Steel Foundation, Sturdy Body for equipment	
7	Call Button: Watertight Large backlit Rectangular Push Button, Visual Feedback for button press and call indication	
8	Connectivity: Ethernet	
9	Sensors: For tampering/ vandalism	
10	IP66 as per EN 60529, IK09 Protection EN 62262 or better	
11	Operating Temperature 0 to 60° C	
12	Speaking Distance as per site requirement	
13	Inbuilt Class D Amplifier, 99db SPL	
14	Minimum 3 Inputs and 2 Output relay contacts	
15	ECB should be able to make calls to the PA system	
16	Transmission Bandwidth 16000 Hz	
17	Front panel: stainless steel of minimum 3 mm	
18	Software Client for making/receiving Calls to ECB	
19	Automatic Volume Control, Call recording	

6.7.5 IoT Gateway Specification

Sl.No.	Description	Compliance (Yes / No)
1	Should be Linux / Windows latest version based operating system powered gateway or microcontroller based gateway.	

2	Gateway routers Single Board Computer running at 1.2GHz or better. Should have a 1GB RAM	
3	The receiver on the gateway should use a 867 Mhz or higher range and follow a multi hop mesh networking protocol	
4	The gateway should periodically update the central management server at ICCC about the diagnostics status of each sensor, LED, controller and display	
5	The gateway should use secure http protocol to communicate with the cloud server	
6	The gateway should be able to control the sensors or IOT devices	
7	The gateway should ensure the display data sync at all locations and floors where they are placed	
8	Should have Wi-fi on board, Ethernet connector on board	
9	Should have Bluetooth Low Energy (BLE) on board for future tech integration	
10	Should have multiple USB ports for communication via USB GSM/3G/4G dongle	
11	Should use micro SD port for loading your operating system and storing data	
12	Should have a Micro USB power source (up to 2.4 Amps)	

6.7.6 Public Address System

Sl.No	**Minimum Specification**	**Compliance (Yes / No)**
	Make :	
	Model:	
1	IP based PAS to be used for automated announcements or for paging announcements from ICCC or from the local area as per city traffic regulations. Should have 5 year warranty	
2	Each site will have multiple speakers connected to one IP amplifier	
3	A local paging microphone ("Control Desk, Local") shall also be provided for doing local announcements	
	Outdoor Horn Speaker	
	Technical Specifications	
1	Speaker – Minimum 30 Watts	
2	Protection – IP66 and preferably IK10 or better	
3	Frequency Range – 350 to 10Khz	

4	Maximum Sound pressure level @1 m – 110 db or above	
5	Operating Temperature - -10 to + 55 C	
6	Construction – ABS Self Extinguishing	
	IP PA Amplifier	
	Technical Specifications	
1	**Amplifier: 120 Watt or above, Class D**	
2	Should have the capability to control individual PAS i.e. to make an announcement at select location (1:1) or multiple locations (1: many). The PAS should also support both, Live and Recorded inputs	
3	Native IP connectivity, no convertors to be used	
4	0 to 55 C Temperature rating for Amplifier	
5	Frequency Response: 70 Hz to 15000 Hz for Amplifier	
6	Minimum 2 Inputs and 1 Output relay contacts in Amplifier for connecting external beacon	
7	Speaker: Minimum 3 Speakers 30 W capacity per location	
8	Line Monitoring Facility for speakers	
9	180-240 V mains input supply	
10	Compliant: CB/CE/EN/UL and BIS/IEC	
	Control Desk	
	Technical Specifications	
1	Should have the capability to control individual PAS i.e. to make an announcement at select location (1:1) or multiple locations (1: many).	
2	Noise cancelling in built microphone with audio monitoring	
3	Frequency range – 200Hz – 16Khz	
4	Display – 8 lines X 14 characters or better	
5	Connectivity- IP Based, POE powered	
6	Amplifier – Inbuilt 2.5W or better class D	
7	Operating temperature - 0 to 50C	
8	It should have RJ-45 Information Outlet, Minimum Dual Port (1 Uplink and 1 downlink)	
	PAS Central Software	
	Specifications	

1	The system shall deliver pre-recorded and live messages to the loudspeakers attached to them for public announcements.	
2	The system shall contain an IP based amplifier and uses power that could drive the speakers.	
3	The system shall also contain the control server that could be used to control/monitor all the components of the system that includes Controller, Calling Station & Amplifier.	
4	Central Server operating on 2 or more network interfaces 1Gbps or more data rate Compliance – UL 62368-1	
5	Integration with ICCC and any other component if required	
	PAS Central Server	
	Technical Specifications	
1	Central Server operating on authorized operating system	
2	2 network interfaces	
3	1Gbps data rate	
4	Compliance – UL 62368-1	

6.7.7 City Public Wi-Fi

It is proposed to set up city wide public Wi-Fi across Puducherry City at the designated locations and connected to ICCC using the OFC proposed. The minimum expected Public Wi-Fi systems specifications are as follows. Outdoor AP should have controller license from day one and should be integrated with WLC at DC.

Sl. No	Technical Specification	Compliance (Yes / No)
	Make	
	Model	
1	Access Points proposed must include dual radios (2.4 GHz and 5 GHz) and should cover a distance of 250 meters in open area. Outdoor (IP67 rated or better) Wi-Fi6 802.11ax WLAN AP with Tilt bracket & PoE Injector	
2	The access point should be light weight and should support installations on walls or light poles without disturbing the aesthetics of the area.	
3	LED should be available for activity indication	
4	The Access Point should have auto-sensing 100/1000 Mbps RJ45 port.	
5	Must support 2x2 multiple-input multiple-output (MIMO) with Radio 1: 2.4GHz: 2x2 with 2SS or better and Radio 2: 5GHz: 2x2 with 2SS	
6	Should have dual Radios and should support 200 clients	
7	Should support 1 Gbps data rates on dual concurrent radio operations	

8	Should support 1024-QAM, and 20/40/80 MHz Channels	
9	Minimum conducted transmit power shall support 23 dBm or more on both 2.4 and 5 GHz.	
10	AP shall have integrated/ external antenna with minimum gain of 5dBi or more for 2.4 GHz and 5dBi or more for 5 GHz radios for Omni Directional Antenna device.	
11	The access point or the controller should support DHCP relay	
12	Must have a dynamic or smart RF management features which allows WLAN to automati-cally and intelligently adapt to changes in the RF environment	
13	WLAN Solution should support Mesh capabilities	
14	Along with a controller the Access Points should support fast roaming feature	
15	The access point should provide wireless IPS sensor support on both radios	
16	The WLAN Solution should support IP filtering	
17	WLAN Solution must support Application Visibility/Control	
18	WLAN Solution must support WPA3, WPA2 (CCMP, AES, 802.11i), WPA2 with open access public WLAN.	
19	Security solution must provide Rogue AP detection and protection	
20	System should support Authentication via 802.1X, mac authentication to local database or external RADIUS Server.	
21	For troubleshooting purposes, the administrator should have the ability to remotely packet capture and / or 802.3 frames from an access point without disrupting client access	
22	WLAN solution should provide features that provides no touch AP discovery, adoption, provisioning and should be from same OEM	
23	WLAN solution should provide features that provides other management functions including AP management and configuration, firmware push and statistics reporting	
24	Must support telnet and/ or SSH login to Aps directly for troubleshooting flexibility	
25	Access point should have Integrated PoE and power injector Support	
26	AP shall Support Surge Suppression of up to 4 Kv.	
27	Operating Temperature: 0°C to 65°C and Operating Humidity up to 90% RH non-condensing.	
28	The Access Points should support WMM, WMM-UAPSD, 802.1p, Diffserv and TOS	
29	Support for Voice-over-wireless LAN (VoWLAN), quality of service (QoS).	
30	Access point must be supported for a minimum of 5 years by the hardware vendor with software updates and upgrades without additional cost.	

6.8 Geographical Information System

It is envisioned that location-based GIS applications are critical for PSCDL and plays major role in disseminating information & data to stakeholders, visitors / tourists. Keeping view of this it is proposed to deploy integrated GIS Engine in ICCC Platform which can be further integrated with the MAPs like Google, Open Street Etc.

- It should be possible to visualize all the Assets (Sensor, Devices, Vehicles, Cameras, other city resources) on map.
- The Assets must be provided as layers with ability to switch these layers and visualize the assets of only selected layers.
- The GIS Maps should provide interactive visualization of travel time and traffic based on the sensor data and data ingested from 3rd party sources.
- GIS Platform shall support GIS Maps in following file format PDF, JPG, PNG, Vector PDF Map, Web Map Service (WMS), GeoJson defined by the Open Geospatial Consortium (OGC), Google Map-aerial; terrain, Bing Map, aerial, satellite, hybrid, ArcGIS/ESRI and Open Platform GIS Applications etc
- GIS platform should provide a picture-in-picture map view capability,
    - Upon the availability of GPS positioning of a file, the user should be able to quickly alternate between the video and map view within the video player.
    - The application must be able to ingest and present either a static location (e.g., for a fixed camera) or dynamic location (e.g., for mobile cameras) that allows users to validate the location where the video was recorded at the time of the event.
- GIS platform should support different layers like
    - Ward Boundary Layer
    - Zone Boundary Layer
    - Street Boundary Layer etc.

6.9 Flood Sensors & Alert System

a) Proposed ICT Solution:

The storm flooding usually creates havoc and panic situation to the people residing in urban areas. High intensity rainfall events and flooding in urban areas are increasing every year. In the past two decades, migration to urban areas and rise in urban population in cities are experiencing a tremendous growth. Urban flood scenario is increasingly witnessed due to rapid urbanization in the city. Flood disaster is causing huge economic and social losses and has resulted in disturbed daily living for the public.

The proposed Flood Sensors & Alert System shall consist of

1. Flood alerts integrated with ICCC

The proposed methodology shall be developed for ~~Urban~~ Flood Sensors and Alerts System have two stages.

Stage 1: Rainfall and Runoff module

Stage 2: Flood Alert

The flood monitoring warning dissemination system: It is proposed to install Flood Sensors. District at locations covering a geographical spread of 64 Sq. Km of city area. It is proposed to install Flood sensors in the identified areas like major canals and junctions.

The rain water level data (in millimeters) is recorded at every 15-minute interval by default and configurable as required and will be transmitted to the application server through telemetric GPRS enable system. These water level data shall be used to validate the depth of water obtained as an output from hydrologic model. The data on Temperature, Relative Humidity, Wind Speed, Wind Direction, Rainfall Intensity and amount of Rainfall from telemetric rain gauges and weather sensors are also being collected every 15 minutes and must be configurable as required. The near-real time data collected through the network shall be analyzed, and real time maps and reports shall be generated. A GIS and ground truth analysis along with historical flood event study in the city shall be conducted for finalizing and mapping of frequently flood vulnerable locations.

Warning System – Published over ICCC

The high intensity rainfall alerts and Flood forecast, warnings, Reports and Advises shall be disseminated through email, Social media, SMS to the mobile phones of Zonal heads, ward level officers of city corporation and also to all the connected line department in the city.

To disseminate the flood forecast and warnings to the city public, A dashboard shall be developed and integrated with ICCC would be the single interface which shall give the insight about urban flooding in the city. To disseminate weather related information, forecast and related advises directly to the general public a 24x7 to City Mobile app. The near-real time data collection, report generation and dissemination shall help the City administrative authorities in planning and executing disaster management and mitigation plans at microlevel and finally reducing the risks involved due to the flood disasters.

Major scope of Early Warning and Dissemination System:

1. Warning and Dissemination system development in collaboration with DRDM.
2. Mobile application for citizens & Dashboard development for administrators.
3. Integration with ICCC.

S. No.	Description
1.	Flood monitor must be capable to monitor flood levels in water bodies, streams and rivers
2.	Flood monitoring application must be integrated with flood sensors and should be able to communicate with them.
3.	Flood monitoring application must be web based with mobile app
4.	The system should be able to send accurate and instant warnings to make informed decisions
5.	The measured data should be sent to flood monitoring application
6.	The flood monitoring application should have intuitive dashboards providing real-time monitoring information
7.	The flood monitoring application must be able to integrated with various third party applications via APIs
8.	The application must be able to do real-time continuous measurement
9.	The application must be able to send instance notifications via SMS, Email and/or push notifications to a mobile app
10.	The solution should also provide a mobile app working in at least Android or iOS

11.	The application must provide intelligent analytics based on data captured
12.	The application must have custom reporting capabilities
13.	The application must be able to provide forecasts and trends
14.	The application must be able to provide real-time notifications
15.	The application must be able to be deployed on cloud or on-premise

Technical Specifications

Sl.No	Component	Description	Compliance (Yes / No)
	Make:		
	Model:		
	Body		
1	Build	Polymer/Metal	
	Range Options		
2	Max Range	3 ft (91cm)	
		30 ft (9.1m)	
		50ft (15.2m)	
	Communication Capability		
3	Wireless		
	GSM	2G/3G/4G/5G/NB-IOT	
	LoRa	865-867 MHz	
	Wi-Fi	802.11 b/g//n (2.4GHz)	
	Wired		
	Ethernet	1-Port 10/100 FE PHY	
	RS485	Modbus Protocol	
	Power Options		
4	Input	230V, 50 Hz	

		Solar Powered	
	Operating Environment		
5	Temperature	-0 to 60° C	
	Humidity	0% to 100% RH	

6.10 City Surveillance System

Primarily the function of police, these refer to operations to enhance the safety of the public and provide necessary surveillance information to Police for both reactive and predictive policing. CCTV surveillance has been an important component across multiple cities with increasing usage of video analytics to aide police in spotting potential incidents and managing them as they happen.

Key Issues

- The main challenges of surveillance in urban ecosystem are as follows:

- The rate of urbanization is increasing and with city growth comes an increase in crime and safety concerns due to concentrated populations
- Lack of surveillance cameras on a Pan City basis results in delays in crime detection and response
- Riots and vandalisms go undetected on a real time basis in lieu of absence of CCTV cameras at important places
- Lack of intra department real-time coordination, with voice and multimedia services
- Need for intelligent analytical capabilities by police
- Fragmented decision making due to lack of inter-departmental collaboration
- Citizens do not have access to a dedicated Emergency Response System

Indicative Key Outcomes and KPIs

- Supporting law enforcement agencies in 24x7 surveillance and monitoring
- Emergency Services Response Time: Average response time for Emergency Services o Number of CCTV cameras installed in the city per unit of road length
- Number of recorded crimes per lakh population
- Extent of crimes recorded against women, children and elderly per year o Location wise analysis of crimes in the city
- Creation of emergency corridor/ passage for passing of fire response / police/ ambulance teams
- Proactive identification of security issues leveraging intelligent analytics from the surveillance system
- Supporting active response during emergency & disaster situations
- Providing secured access to video at any time from any network location
- Situation/Rule based alerts based on user inputs
- Automated response based on events including communication of alerts to relevant authorities like Fire, Hospitals, etc. for swift response in case of emergencies;
- Access to historic video data for investigative purposes
- Improved Crowd management and Security Breach handling

Surveillance System:

I. The Surveillance System shall be a fully distributed solution, designed for large multi-site and multiple server installations requiring 24/7 surveillance.
II. The solution shall offer centralized management of all devices, servers and users.
III. 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
IV. The Surveillance System shall support distributed viewing of any camera in the system using Video walls or big screen displays
V. The Surveillance System shall support alarm management. The alarm management shall allow for the continuous monitoring of the operational status and event-triggered alarms from system servers, cameras and other external devices
VI. 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. (e.g., integrating alarm management to initiate SMS, E-Mail, VoIP call etc.)
VII. Rule Management: 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.
VIII. 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

Video Management Capabilities

The system shall allow an operator to view live / recorded video from any camera on the IP Network.

It should allow switching of video streams across the system.

ICCC/Police personnel shall have followed access to the video feeds of the cameras of their jurisdiction:

- Viewing rights to all the live Camera Feeds

- Viewing rights to the stored feeds
- Access to view Alerts / Exceptions / Triggers raised
- Trail Report 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
- Advanced search based on various filters like alarm / event, area, camera, etc.
- Event Handling Capabilities:
- The camera shall be capable of recording an event as pre and post event images to on-board SD Media Card and share it with ICCC
- Events may be triggered using camera motion detection or from an external device input such as a relay.
- Support for various type of Logs such as System Log, Audit Log Alert Log Event Log should be available.

Recording and Storage:

- For incidents that are flagged by the Police, Authority or any court order, the video of the relevant portion from all relevant cameras should be stored/archived separately for investigation purposes and a committee at Authority can decide when this video feed can be deleted

  Audit trail of the system to be maintained on permanent basis / as per the backup policy defined.

  The Recording System shall run independently of the Video Management system and continue to operate in the event that the Management system is off-line.

Investigation Scene Rebuilding

- It should be possible to select the cameras for synchronized and simultaneous archived viewing. It should be possible to record the videos being rendered from these cameras into a single video. Such a single video should support up to eight such cameras in vertical, horizontal or overlay fashion. An easy feature of cloning the time stamp from one camera to multiple other cameras for synchronous archived viewing should be available.

- For quick investigation of the alerts, it should be possible to configure cameras in small functional group/s. In case of an alert in any one camera in the group, live video from other cameras in the group should be popped up automatically on the operator screen.

The system should enable tracking of the vehicle on a GIS map to locate any suspicious / identified vehicle. The Cameras should transmit quality video feed (clear, un-blurred, jitter free, properly lit, unobstructed, etc.).

The network design should ensure that the Packet losses are less than 0.5%.

Integration with ECB and Citizen App for SOS Management should be available.

Integration with ICCC

Integration of all the IT systems and solutions deployed for the Surveillance management with ICCC should be through APIs

The alerts generated in ICCC should be handled in a coordinate manner with following;

a. Rule engine module for event/alarm handling
b. SOP (Standard Operating Procedure) tool for administrator to configure the SOP responses based on each alert.
c. Integration with the Incident Management system for the users to log in the incidents and the alerts, view the report from the module about the incidents etc.
d. Alert processing such as Acknowledging the alert, emergency response, SOP for the alert.
e. Connecting the next steps as per the SOP like informing Police\Fire departments based on the incident etc.

Technical Requirements

c)Proposed ICT Intervention.

The core objective is to create a supporting mechanism for the city agencies through 24x7 surveillance and monitoring throughout the city as well as enable proactive identification of issues leveraging intelligent analytics from the surveillance system.

This module proposes implementation of a holistic City Asset Surveillance and Service monitoring system across the city including:

- Installation of PTZ cameras, Fixed Box cameras
- Centralized AI based intelligent Video analytics at data center for all the cameras installed
- Centralized AI based intelligent Video analytics for all the feeds received from Department of Police cameras, where these will provide the feed of CCTV cameras up to ICCC data centre.
- Develop a full-fledged command and control center for ensuring 24X7 monitoring and enabling effective action to be taken in case of law and order, Municipal services disruption , emergency disaster situations
- Integration with existing safety & surveillance systems already implemented like existing cameras installed, existing command & control centre as Police Station, etc.

It is proposed to have surveillance cameras and a dedicated video analytic system for incident monitoring based on events. Further, with a view to share the video to other Stake Holders as well a dedicated VMS is being proposed with a distributed architecture.

6.10.1 Video Management System:

General Requirements

#	Technical Specification	Compliance (Yes/ No)
	Make :<to be provided by the bidder>	
	Model :<to be provided by the bidder>	
1	The VMS architecture should support centralized or de-centralized deployment. The VMS should be modular in design and should have components such as Management Server, Recorder Server, Streaming Server, Database Server and Integration Server.	
2	All the communication among the servers and clients should be secured and the VMS should support the SSL /TLS communication. It should have option of encryption with AES 128/256 and RSA 1024/2048 encryption standards. The VMS should also support secure communication between the camera and the server using SRTP/RTSP protocols. The VMS software should have been tested for vulnerabilities and should have been penetration tested as per the OWASP guidelines. Certificates from the CERT – IN empaneled auditor from the respective country of origin clearly indicating the encryption and VAPT test should be available.	
	System Architecture	
1	The Video Management Software should be enterprise class application based on client-server architecture and should support unlimited cameras by augmenting recorder, management and database servers.	
2	The single master server should handle unlimited cameras, unlimited recording servers and unlimited users.	
3	The VMS should be compatible with Microsoft Windows/Unix/Linux Operating Systems.	
4	The VMS should run on all the leading virtualisation platforms.	

5	VMS should be agnostic to database servers For example it should work on Microsoft SQL, MySQL, PostgreSQL and Oracle. It should also support NoSQL databases.	
6	VMS should have ONVIF Profile S, G , M and T compliance. Certificate to this effect should be available on the ONVIF website.	
7	The VMS should work on Commercially off the Shelf hardware and storage systems.	
8	The VMS should have an independent media streaming service which can be installed on a separate server to support scaling up of the clients without affecting the recorder server performance.	
9	The VMS should have manual and automatic mode of assigning cameras to the available recorder servers. In automatic mode, the cameras should be assigned based on the compute capability of the recorder server. In manual mode, the system should allow the administrator to assign the cameras to a recorder server.	
10	The VMS should provide multiple redundancy options in the platform for the following components:	
11	The VMS should have a provision for adding Master and Auxiliary Master Server to provide the native failover functionality. As a failsafe configuration, the system should work with limited functionality, without affecting the recording of cameras, even without the Master server.	
12	The VMS shall provide redundant recorder server for single or a group of recorder servers. In case of the failure of the Recording Server, the VMS should automatically assign the cameras on the failed recording server to other operational recording servers on the network. The camera recordings shall be synchronized back to the original Recording Server once it is back online.	
13	Each recorder server should have independent storage configuration for local and network storage including NAS, SAN storage and Object Storage from popular cloud platforms such as Amazon AWS, Microsoft Azure, Wasabi, etc. Option of mirroring the storage of camera feeds should be available in the system. Back up storage on cloud/DC secondary storage for 60 days post local storage of 30 days.	

14	The VMS should have configurable DC-DR Functionality. The system should have configurable data retention policies for each DR setup to select what data to move and how long the data to be retained in DR before recycling the storage space.	
15	The VMS should have multiple options for selecting the business continuity requirements. Following options should be available in an easy to configure grid such as	
16	Data Replication Policy grid should allow selection of data such as video data, event messages and incident alerts, event video and the video segments tagged by the operator. It should be possible to select all or a group of cameras for such replication.	
17	The Business Continuity Policy should allow selecting all or a group of cameras which should switch over to DR for recording and viewing of videos.	
18	The user access policy should allow the granular control for various categories of users for functions such as login to the DR site, live video viewing and recorded video replay.	
19	The VMS should have federated architecture with centralised monitoring of the videos, video analytics and system health alerts.	
20	The VMS should have a unified API interface to expose various system functionalities, including, but not limited to, Analytics event alerts, live and archived video, PTZ control, system health alerts over HTTP protocol to external systems such as Integrated Command and Control Application,	
21		
22	The VMS should support unicast and multicast streaming for live viewing and recording functions.	
	Centralized Management	

1	The VMS should support multi-site deployments with centralized monitoring of the videos, video analytics and system health alerts. The centralised monitoring platform shall have the following features:	
2	Should support matrix view at full framerate with support for H.265, H.264, MPEG4 and MJPEG video compression.	
3	Drag and drop of cameras and live viewing of cameras from a mix of cameras from all the locations, group of locations, single location.	
4	Support digital zoom of the cameras from central site.	
5	Control remote PTZ cameras from central monitoring client application and digital zoom on remote fixed or PTZ cameras.	
6	Ability to pick and choose the selected cameras from remote sites.	
7	Ability to search and retrieve the archived video from the remote site with intelligent motion based search	
8	Download multiple video segments from multiple sites easily	
9	Multi-layer maps with support for static maps or GIS maps.	
10	System health dashboard for all connected systems.	
11	Central site management features with Role based User management, dynamic site management, video feeds aggregation, event information management and distribution, system administration with full audit trail and logs	
12	Shall support secure and encrypted transmission of video files to cloud as per requirement.	
13	Receive alerts from the remote site with event metadata received first and then the users can request image and video clips to ensure effective bandwidth management.	
14	Dashboard of all connected devices and the health status of the devices.	
15	Resource utilization of the system and statistical reports for the remote sites.	
16	Camera SLA report with camera connection and uptime information	
17	Scheduling of reports	
	Cloud Readiness of the VMS	

1	The VMS should be cloud deployment ready and agnostic to the cloud environment - be it a private, public or a hybrid cloud. It should work on the bare metal servers of the cloud solution providers with in-built intelligent video streaming and resource orchestration services. The VMS should allow using various tiers of object storage to optimize the storage requirements and data retrieval times. The VMS should be capable to integrate with Video Analytics functions powered by the Artificial Intelligence and Deep Learning technologies on cloud infrastructure.	
2	The VMS should allow adding network storage location by giving path to the network storage device and authentication credentials. This feature should also allow adding storage locations on the cloud platforms such as AWS, GCP, Azure, Wasabi etc.	
3	The VMS should have native support for Object Storage from popular cloud platforms such as Amazon AWS, Microsoft Azure, GCP, Wasabi, etc. The system should support pushing the recorded video file on a definable schedule to the Object Storage.	
	Information Security	
1	The system should have multiple levels of authentication and access control mechanisms: A. Role based Authentication B. Session control using encrypted tokens C. User stickiness to a particular hardware workstation D. Dual Factor Authentication with provision to receive the OTP via text message on the registered mobile of the user and through the registered email address E single sign-on based on LDAP and Active Directory.	
2	System configuration data should be stored in encrypted files with checksum and there should be user selectable encryption algorithms such as MD5, RSA and SHA.	
3	The data at rest should be stored in a encrypted format.	

4	The videos downloaded from the system should be watermarked with an option to export with non-tamper format.	
5	The software should maintain audit trails of user interaction	
6	The system should have built-in audit tool which generates reports such as report describing health of network connectivity and the throughput of storage devices against each server.	
7	The software should be OS agnostic.	
8	Data in the system should encrypted with either MD5 or SHA256 cryptographic hash functions and video data are stored in encryptedformat when at rest	
	Storage & Recording Functions	
1	The VMS should allow creation of customised recording profile with day and hour granularity and an option to add recording profile for special days. It should be possible to create unlimited recording schedules with option of selecting various streams, Frame rate and compression available from the cameras. The recording configuration should have the following options:	
	- Redundant recording	
	- Edge recording	
	- Selection of SRTP or RTSP protocols	
	- Recording schedule based on motion only recording, FIFO and specific retention period.	
2	Each recorder server in the system should have independent configuration for database and storage servers.	
3	The VMS should periodically check the gaps in live recording of the cameras and should check with the on-board storage of the camera. In case of a gap, the VMS should synchronize the video recording on the on-board storage with the VMS storage. Such synchronized storage should be displayed with different color for quick attention of the operator.	
4	The event and the associated video clips should have the facility to be marked for non-delete flag to protect the event and metadata from being wiped out by the data retention policy. Additional option should be available	

	not to delete the event till a specific date. After that, the event should be wiped out as per the data retention policy.	
5	The system shall have the capability of recording video at a lower frame than is received from the camera (frame rate reduction mode).	
6	VMS should support H.265, H.265+, H.264, and MJPEG streams for both Live view and Recording.	
7	The client should offer below three options for operator-specific recordings:	
8	Record Matrix Videos: Record a matrix of the videos being displayed on the screen.	
9	Record Stitched Videos: Stitch and record the stitched video matrix either in horizontal or vertical direction. Any number of cameras can be added in the stitched video.	
10	Record Screen: Record the entire screen of the operator including any matrix of cameras visible and other desktop activity being performed by the user outside of the VMS client. This functionality can be achieved using in-built or third party tools.	
	General VMS Functions	
1	The system, once configured, should work seamlessly, without any configuration, after the server/s pass through the power on-off cycle.	
2	The VMS should offer feature rich desktop client for Microsoft Windows and Linux OS. It should also have a browser agnostic web client and mobile client available on Android and IOS platforms.	
3	The VMS should have site-wide, hierarchical tree of cameras visible to all the operators with appropriate rights and should also have operator specific, unlimited hierarchical grouping of cameras as per the area or functions.	
4	The VMS should allow grouping of cameras as per the Group Name or Location for flexibility of camera management.	
	VMS User Management & Administration	
1	The VMS should support Microsoft Active Directory or Lightweight Directory Access Protocol (LDAP) for enterprise wide user management.	

2	For additional security and accountability, it should be possible to restrict the operator to a particular workstation.	
3	The VMS should allow addition of new user based on five different profiles. It should be possible to assign various configuration and operation functions for each profile as required in a user-friendly matrix view.	
4	The VMS should seek answers for the multiple selectable security questions to each user logging-in for the first time. The answers to the security questions should be validated by the VMS in case the user wants to change the password. The VMS should not allow using the last three passwords while selecting the new password.	
5	The system should have collaborative vigilance functions. It should offer chat room for exchange of information such as text messages, user selectable files, archived video link, camera layouts, incident snap, clip and VA alerts for collaboration among the operators. The chat window should show color coded status for messages which are sent, delivered and read. The administrator should have access to all the messages being exchanged among the operators. To assist in collaborative investigation of an event, the operator should have the function of sharing the camera matrix with a mix of live as well as playback videos to the fellow operators or to the Supervisor. This function should also allow sharing an event along with event video, stitched video of a matrix recorded on the operator workstation, any other video clips received from external sources, etc.	
6	The system should allow camera permissions to the users based on individual camera, group of cameras and all cameras.	
7	VMS should allow the Administrator to import any active users screen on the video pane by drag and drop to watch the operator's activity on-line in a matrix layout. Operator should be able to drag a user group on the screen to watch their desktop activity at one go. Administrator should be able to record the matrix view for the desired duration if required.	
	VMS Client and Operator Functions	
1	The unified VMS client should provide all the configuration functions for Video Management Server, Video Recorder Servers, Storage and Video Analytics for creating rules.	

2	The VMS should allow multi-monitor support for the client workstation. It should allow setting up of different layouts on different monitors such as camera matrix, map view, VA alerts view, for example.	
3	It should be possible to select cameras for synchronised and simultaneous archive viewing. It should be possible to record the videos being rendered from these cameras into a movie clip. This operation should be possible in a matrix recording or stitched recording options.	
4	The VMS should retain the VMS client screen state (including Video Analytics alert window, message window, Video Matrix, etc.) in case of an accidental shut down of the machine and should offer the exact same screen to the operator upon logging back into the system.	
5	The client should have configuration option to view the live videos directly from camera or from the media server. In case of the video feed coming directly from the camera, the live view should be available even if the servers are not reachable.	
6	The live view window of a particular camera should allow the operator to view the archived video. The operator should be able to go back in the time by selecting quick shortcuts for 5, 10, 20, 30 seconds, 1, 5 minutes, 1, 5 hours. Operator should also be able to select the exact date and time though the calendar widget.	
	Virtual Workspace Functions	
1	The VMS should present the functional dashboard of the system to the operator like a virtual workspace. The Dashboard should allow the operator to view and manage the cameras, operator specific camera matrix views as per the functional requirements, map views for the geo-aware vigilance, video analytics alerts, and information and alerts from the integrated devices.	
2	When the operator drags a camera group on to the virtual workspace, the VMS should dynamically select and display the number of tiles in the virtual matrix based on the number of cameras available in the group.	
3		

4	It should be possible for the operator to configure the virtual workspace using the virtual matrix by assigning the matrix to display alerts and information from a combination of systems such as live and archived videos,	
	Map Functions	
1	The VMS should support geo-aware vigilance with the use of layered maps using standard picture files, City GIS maps and online maps such as Google, Bing, OpenStreetMap's. It should be possible to drag and drop the cameras on the map for easy navigation. In case of multi-layered maps, the system should show all the available maps in a drop down list for easy selection. The VMS should allow viewing of live and playback videos, event notifications on the map view with event tracking functionality from multiple cameras.	
2	The VMS should support a geo-fence based vigilance functionality. The VMS should show the cameras within the selected geo-fence. It should be possible to associate a base camera within the geo fence with other neighborhood cameras to form a group for situational awareness of the neighborhood. In case of an alert in the base camera, live feeds from all the cameras in the group should be popped up. The window should show the live video and the alert video clip from the base camera where the alert is generated, the neighborhood cameras and the location of the incident on the map within the same window.	
3	It should be possible to export the map view to the desired screen in case of multiple screens available. The system should show all the available screens in a dropdown.	
4	The system should have an easy to use pencil tool /similar easy to use feature to quickly select the cameras on the map (static or GIS) for simultaneous viewing for both live and playback videos.	
5	It should be possible to forward the map view including the camera streams, live or playback to another user in the system for easy collaboration of geo-spatial viewing.	
6	The map view should allow searching of the camera by name or IP address to quickly find out the camera on the map. This is useful in emergency situations when an operator wants to pull the live video on the screen quickly.	
7	The VMS should show event notification from the cameras on the map itself. The operator should be able to click on the event notification of a particular	

	camera on the map and the VMS should open the event window on the operator screen.	
	Investigation and Tracking Functions/Video Synopsys Tool.	
1	The operator should be able to recreate a scene by arranging the cameras and their respective time-stamped archived videos. The operator should be able to save such a recreated scene through collection of cameras for quick access and should also be able to share such collection to the other users or supervisors.	
2	The operator should be able to associate all neighborhood-view cameras to a base camera for tracking an activity for investigation. When an alert is generated in the base camera, the VMS should pop up a screen widget/ similar easy to use interface which shows live video of the base camera, playback of the base camera from the pre-buffer of the alarm and live view of the associated cameras along with the map view. This entire screen should be used for forensic investigation and should be recorded as all-in-one evidence for export and sharing. This event window should be configured to pop-up on the event hot-spot monitor.	
3	The VMS should allow tracking the movement of a suspect or a motorcade through live view from the cameras on the map by using a simple pencil tool/similar easy to use feature on the screen. With the tool/feature, the operator should be able to draw a line on the map touching one or more cameras and the cameras touched/selected by the tool/feature should appear for live view on the screen.	
4	The VMS should have PTZ camera control options in a separate PTZ control widget. The widget should show all the available presets, allow pan, tilt and zoom of the camera, and also allow creation of a preset. It should also support 3-axis USB joysticks for PTZ camera control.	
5	The VMS should allow creation of a PTZ tour based on the presets available from the PTZ camera. The VMS should allow setting the hover time for each preset depending on the functional requirement. It should be possible to attach such a tour to any of the associated video analytic use case. The creation of a PTZ tour should be the function of the VMS without any external dependency	

6	The system should offer multiple playback mechanisms (including single frame playback) for ease of auditing and investigation, including zooming and panning simultaneously.	
7	The system should allow ease of tagging of exceptions/audit/investigation findings and creating an institutional library of the same for future reference.	
8	The VMS on integration with Video Analytics software should provide forensic search operation based on the powerful attribute search analytics feature. The operator can select any person in the camera field of view and search for the appearance of the selected person based on the attire attributes in the selected cameras for the selected duration. The attribute search should show persons with matching attributes in a grid. It should be possible to click on any match to view the playback video of that instant.	
9	The VMS on integration with Video Analytics software should allow the operator to select an unidentified object with a selection tool on the screen to identify who left the object in the scene. The analytic should search the video and show the video frame when someone left the object in the scene.	
	Event and Alert Functions	
1	The VMS should allow sending the event alert to the designated person or a group of designated persons through SMS or Email. These rules should be available with configurable priority of the alert.	
2	The VMS should allow monitoring of archived video of the selected camera under categories such as events, motion or continuous recording. The VMS should also show a report of cameras indicating recording status for the selected duration, critical video data and Incident Video data.	
3	Live events should be shown on the event hotspot monitor and retained for the configured time. This should alert the operator of the current events. The unattended events should be queued to be taken up by the operator one-by-one later.	
4	The events dashboard should be available with multiple filter parameters such as - by camera, by use case, by camera groups, and the easily selectable duration such as today, last 7 days, last 30 days, and calendar widget, etc.. Reports should be exported in formats such as excel and CSV. The dashboard should also have the graphical representation of the reports in terms of the bar charts and pie charts.	

5	It should be possible to pass the specific alarm intimation to specified users rather than sending all alarms to every user.	
	Camera Management and Viewing Functions	
1	VMS should allow configuring the cameras in multiple groups independently. It should be possible to assign all, single or multiple groups to operators. At least 100 such groups should be possible with an unlimited number of cameras in each group. It should be possible to assign camera/s to single or multiple groups simultaneously.	
2	The operator should have the ability to use digital zoom where the zooming is performed on any number of cameras simultaneously - for live and playback videos. This functionality should be the default for fixed cameras. The use of digital zoom should not affect the recording.	
3	Client viewer should allow the same camera to be viewed on multiple display tiles; one may be digitally zoomed, or on high resolution stream.	
4	The VMS should allow restricting the users who are authorized to view the camera feeds to a single camera and to the group of cameras.	
5	The system should allow creation of operator specific camera groups comprising of live video views and archived video views. It should be possible to share such groups with other users and administrators. The recipient of such information should be able to see the exact layout of live view and archived video view.	
6	The camera matrix for live and archived videos should support simultaneous viewing of cameras in multiple grids ranging from 2x2 to up to 8x8 and should allow operator to configure as per requirement . A simple click should allow enlarging any of the cameras in the multi-screen displays into a full screen and full resolution display of the camera. On clicking again on the enlarged display, multi-screen display should reappear.	
7	The VMS should allow the operator to create multiple camera matrix comprising of live and archive videos from multiple cameras and create a sequence of such multiple matrix to be displayed in a cycle with configurable display duration for each matrix. It should be possible to export such a sequence to any of the connected cameras or the video wall.	

8	It should be possible to drag and drop cameras from the camera directory to the display screen.	
9	The Client Viewer should offer the capability of browsing recordings from cameras on the same panel where other cameras are displayed live.	
10	VMS should have smart management of video streams from camera. It should select lower resolution stream when viewed in a matrix and should automatically switch to the high resolution stream when viewed full screen.	
11	The Client Viewer should display a time line for each camera to represent recorded video sequences. The Client Viewer should indicate whether the video was recorded due to motion activation or recorded without motion or pre and post alarm video. The time line band should be highlighted based on the camera view selected in the display.	
12	The camera type should be shown with specific camera icon and the state should be displayed in different colours to indicate whether the camera is in live mode, in recording mode, in stopped mode or video analytics alerts.	
13	From the Client Viewer it should be possible to:	
14	Bookmark an important event for easy search and retrieval later.	
15	Bookmark the display layout with selected distribution of cameras across the panel with a mix of live and archived video.	
16	Use sound notifications and external annunciators for attracting attention to detected motion or events.	
17	Get quick overview of sequences with detected motion.	
18	Get quick overviews of detected alerts or events.	
19	The Client Viewer should have the capability to receive multicast streams if a preset number of clients are requesting the same live view camera. The Operator should have the option to configure the system to always receive unicast streams at the discretion of the system administrator. The system should have the capability to detect if the network becomes unreliable and to automatically switch to unicast to ensure that the operator is able to receive video.	
	The Client Viewer should have the following audio functions at specified locations.	

1	The Client Viewer should allow an operator to play live audio from a camera's microphone and play back recorded audio. The audio on/off option should be available on the camera display matrix for each camera.	
2	The operator should have a "press to talk" option which should send the microphone input from the operator out to the speaker attached to the camera. The microphone button should be available on the camera display matrix for each camera.	
3	The VMS should have integration with the IP speakers and should be able to send the audio message for the selected IP speaker.	
4	It should be possible to export the video clip of selected duration for export. The VMS should allow export of a single video clip or multiple clips to a cart. For downloading a single clip, it should have encryption option for the exported clip and should ask to select the export format such as AVI, MJPEG, MP4 and AVF.	
	Video Export Functions	
1	It should be possible export the video clip in a tamper-proof format by adding watermark and encryption to the exported video to verify the authenticity of the video.	
2	Export of single frame of video in BMP, GIF, TIF, JPG and PNG formats and export of video files in commonly used video formats and Print images, with optional comments.	
3	VMS should allow the users to download multiple segments of the video from single or multiple cameras from the archive with an option to tag each downloaded segment with text messages. The Video segments should be downloaded in a single folder along with excel spreadsheet where details of each of the video segments are listed as hyperlinks to the exported video.	
4	The Client Viewer should allow an operator to export audio together with video in the AVI or other standard format.	
	Web and Mobile Clients	
1	The VMS should have web client which should work on all the leading browsers immaterial of the operating system.	

2	The VMS should have mobile client for Android and IOS platforms and should be available from the respective Play Store and App Store.	
3	The web application should support HLS and MJPEG streaming.	
4	It should be possible to track mobile app users on GIS map from a central location. The Mobile App user should be able to track the other Mobile App users on the GIS Map.	
5	It should have view link sharing within authenticated users from the web application. The VMS web interface user can forward video link URL by email to another user.	
6	The mobile client should allow uploading of the snaps and video clips from within the application to the central VMS. The central VMS should show the uploaded snaps and videos from the mobile users.	
7	The VMS should have push notifications for the alerts for the mobile and web clients to push the event notifications from the central VMS. The alert notification should also stream the video clips associated with the alert.	
	Health Monitoring, Audit Trail, Problem Reporting Functions	
1	The system should support CCTV video footage auditing & investigation to reduce the data size for disaster recovery purposes , Create a well-categorized searchable institutional library & Report in PowerPoint/Word/PDF/Excel	
2	The system should have capability to sit as a 'stack' over any live or recorded video feed from multiple cameras and convert the same into images by capturing screenshots in the background, at an interval of one or more seconds, thereby reducing the number of frames to be viewed, i.e., creating a summary without missing any scene, and creating huge reduction of data size for disaster recovery	
3	The desktop client should show system health dashboard with vital system parameters for Database Server, Recorder Servers, Local Workstation and all the available storage locations. The client should show real time CPU Core Usage and RAM Utilization.	
4	The system should be able to generate incident/audit finding reports in PowerPoint that deliver data analytics (business intelligence) in Excel.	

5	The system should be able to import any kind of photo/image and offer a template for easy sharing of mugshots in Word/PDF.	
6	The system should allow ease of tagging of exceptions/audit/investigation findings and creating an institutional library of the same for future reference.	
7	The VMS should show the real time workstation CPU and Memory utilization on the screen along with the color changing System Health Status icon which indicates real time health updates from the surveillance system.	
8	The systems should have following features for reporting and system health:	
9	Camera SLA report showing uptime, recording percentage, recording status, critical events, incident video, etc.	
10	Detailed listing of all active or incoming alarms with filtering options time period, alarm source, operator and alarm state.	
11	Generate audit trail reports by incident.	
12	Give full audit trail of the user activities in the system.	
13	The system log should be searchable by Level, Source and Event Type.	
14	The Audit Log should record remote user activity searchable by User name, Audit ID, Source and Location	
15	The Alert Log should record alerts triggered by rules and searchable by Alert type, Source and Event type	
16	The Event Log should record event-related information searchable by Service Name, Source and Event Type	
17	The Rule Log should record rules in which the Make new <log entry> action been specified (searchable by Service name, Source, Event type and Rule name)	
18	The VMS should allow raising support tickets from the Help menu. It should be possible to attach a screenshot of the error for effective communication of the problem being reported.	
19	The VMS should allow recording of the desktop activity into a movie clip to effectively explain the problems being faced to report the support related issue.	

20	The VMS should allow the administrator or an operator to record an activity happening in multiple cameras into a single movie clip which help in improving the security function and the security SOP creation activity.	
21	The VMS should allow the administrator to record the screen activity into a movie clip to create visual manual to explain various functionalities to the new users for training purpose.	
22	API and Integration Functions	
23	The VMS should be able to integrate with external devices such as various types of Cameras, Access Control, Perimeter Intrusion Detection, IP Speakers, , etc.	
24	The system should be able to push the images to the user's cloud. Such images can also be used to train AI models.	
25	The VMS should show integrated devices in a list on the operator screen. The events generated from the integrated devices should be available for viewing.	
26	The VMS should allow easy configuration options to connect to the external devices for integration and should also have granular control on the alert types to receive based on the information exposed by the external devices through the API or SDK calls.	
27	The VMS should provide an Open API based integration gateway without any additional cost or licensing. The API should be able to send the information about various aspects of the VMS system to the external application requesting the information. The API should provide functions such as:	
28	Find servers, registered users, alert types and alerts, available channels, channel ID, count, status, type, PTZ cameras and PTZ controls, get event count, event search, event snap ID, event video clip, camera live video play, playback video play, trigger an event, activate or suspend a device, etc.	
29	The API should support HTTPS based REST API with cryptographic controls to establish secure connection between web and mobile users.	

Video Analytics :

Below functionalities can be achieved on integration of VMS with in-built/third party VA.

- System shall have the capability to provide various alarms & triggers and should notified if any incidence/violation happens.
- The System shall be a real-time video analytics engine that utilizes advanced image processing algorithms to turn video into actionable intelligence.
- The system shall facilitate creating multiple zones and lines in a single scene to trigger various alerts
- The system shall allow the configuration of applicable rules and manage them
- The system shall also enable editing the Zones and lines to the desired shape or size.
- The triggers generated by the applied rules shall provide visual indicators to identify the event. Such as a Green colored Bounding Box changing the Bounding Box colour to Red on event
- The system shall enable detecting rules in the defined areas (zones/ lines)
- The system shall provide functionality for configuring timelines for various events such as Crowd Detection, Loitering Detection etc.
- The system shall allow classification of different objects like animals, vehicles and people
- VAS should allow to add, edit, delete or disable and enable Policies.
- System shall have a sophisticated rule-based engine with powerful analytics capabilities that provides automatic event notification.
- Proposed system needs to have the capability to deploy intelligent video analytics software on any of selected cameras. This software should have the capability to provide various alarms & triggers.
- Following video analytics and features should be supported based on licensing:

Perimeter Trip wire/Crossing Virtual line
• Should capture zoomed image of the object causing the Perimeter Breach and raises appropriate alarm.
• Should also stores the time duration between the pre and post event of the Perimeter Breach.
• Should have the Option Drawing Single/Multiple Lines along with Defining Logic for the Multiple Lines.
Loitering Detection
• Should automatically detect objects/Person that has moved continuously within the camera field of view for a configurable period of time.
• The VA System should have the capability to detect loitering incidents in crime hotspot areas.
AI Based Unattended Object Detection
• Should detect and generate an alert highlighting Suspicious detected when carried into the scene and planted by a person as well as when dropped or thrown into the scene for a Period of time that is considered suspicious by the user.
• Should be able to Detect Multiple object that are left Stationary in a Scene, the System shall be to detect multiple objects each with its own timer as per the predefined detection time. Alarms of each Individual Objects Abandoned shall be alerted Individually.

• The VA should be intelligent to understand the existing objects within the camera field of view and should generate an alert only when a new object is detected for more than the preconfigured duration of time.
AI Based Classification of objects like person, vehicle, or animals
• VA can perform object classification once the camera has been calibrated. Object classification is based on properties extracted from the object including object area and speed.
AI Based Tripwire/intrusion detection
• Detection of intruder entering/exiting a given area of interest.
• Once verified and confirmed by operator that it is a rouge object, the system shall be able to track the person across various cameras and to find the origin of such person.
AI Based Camera Tampering Detection
• 1. Alert to be generated when camera is tampered by way of change of Field of view of camera, blurring of view, blocking of view by cloth or obstruction, camera disconnection, blinding of camera by laser or flashlights.
• 2. Once alert is generated, the incident should be flagged, and system should have the capability to trace the person responsible for the sabotage in other cameras and send notification to concerned authority.
AI Based asset protection, Grouping, crowding and Person waving.
AI based no helmet detection, Triple ride detection, no seat belt detection and accident detection
System must be capable to support below use cases **Garbage Bin Full and Cleared Detection** **Detection of Debris on the Road** **Detection of Stray Animals on Road**
Attribute search Analytics (Search person by Dress , Attire, appearance , age etc)
Video Summarisation

6.10.2 City Surveillance fixed Camera Specifications

#	Parameter	Minimum Specifications or better	Compliance (Yes / No)
	Make:		
	Model:		
1	Image Sensor	1/2.8" 2MP Progressive Scan CMOS or better	
2	Day/ Night Operation	Yes with IR Cut Filter	
3	Minimum Illumination	Color: 0.015 lux or better ; B/W 0 Lux with IR	
4	Lens	Auto IRIS 2.8-12 mm (+/- 1mm) Motorized Varifocal Lens or better	
5	Electronic Shutter	1/10 to 1/12,000s or better	

6	Image Resolution	1920x1080 or better	
7	Compression	H.265 or better	
8	Frame Rate and Bit Rate	Upto 60 fps with Controllable bit rate, frame rate and Maximum Bit rate	
9	Video Streams	Minimum 4 Nos, individually configurable simultaneous streams in H.265 @ 1920x1080 & upto 60 Fps	
10	Angular Field of View	H: 119.5°(Wide)~27.9°(Tele), V: 62.8°(Wide)~15.7°(Tele), T: 142.1°(Wide)~32.0°(Tele)	
11	Motion Detection	Built in 8 point polygonal zones areas in the video stream.	
12	Lens/ Barrel Distortion Correction & Corridor View	Built in feature required	
13	Wide Dynamic Range	150 dB or better	
14	IR Viewable Length	50 Meter or better (Built in or External) IR	
15	Alarm	1 Input & 1 Output	
16	Audio In	Selectable(Mic in/Line in), Supply voltage: 2.5VDC(4mA), Input impedance: 2K Ohm	
17	Audio Out	Line out, Max. output level: 1Vrms	
18	Audio Compression	G.711 u-law /G.726 Selectable G.726(ADPCM) 8KHz, G.711 8KHz G.726 : 16Kbps, 24Kbps, 32Kbps, 40Kbps AAC-LC : 48Kbps at 16KH	
19	Analytics	Can be achieved via VMS and VA: Defocus detection, Directional detection, Fog detection, Face detection, Motion detection, Digital auto tracking, Appear/Disappear, Enter/Exit, Loitering, Tampering, Virtual line, Audio detection, Sound classificationand others.	
20	Event Triggers	Alarm input, Motion detection, Analytics, Network disconnect	
21	Event Actions	FTP, HTTP, Email notification, Edge Storage, Alarm Output, Handover	
22	Edge Storage	Micro SD/SDHC/SDXC minimum of 512GB capacity or better	
23	Protocols	IPv4, IPv6, TCP/IP, UDP/IP, RTP(UDP), RTP(TCP), RTCP,RTSP, NTP, HTTP, HTTPS, SSL/TLS, DHCP, FTP, SMTP,	

		ICMP, IGMP, SNMPv1/v2c/v3(MIB-2), ARP, DNS, DDNS, QoS, PIM-SM, UPnP, Bonjour , LLDP, SRTP	
24	Security	HTTPS(SSL) Login Authentication, Digest Login Authentication, IP Address Filtering, User access Log 802.1X Authentication(EAP-TLS, EAP-LEAP)	
25	Firmware Upgrade	The firmware upgrade shall be done though web interface, The firmware shall be available free of cost	
26	Interface	RJ 45, 100 Base TX or better	
27	Memory	1024 MB RAM, 256 MB Flash or better	
28	Enclosure	IP67,IK10 & Nema4x or better	
29	Power requirements	Vendor to specify, POE Preferred	
30	Operating Temperature	-30 °C to 55 °C or better	
31	Operating Humidity	Max 90% RH or better	
32	Certification	UL, CE, FCC,BIS, NDAA	
33	Application Programmers Interface	1. The interface shall be available for integration with 3rd party analytics and applications in public domain 2. ONVIF	
34	Embedded Applications	The camera shall provide a platform allowing the upload of third party applications into the camera	
35	Mount	Wall Mount/ Pole Mount	
36	Warranty	Minimum 5 Years	
37	Defog	Available	

6.10.3 City Surveillance PTZ Camera Specifications

S. No.	Description	Desired Parameter	Compliance (Yes / No)
	Make:		
	Model:		
1	Imaging Device	1/2.8" 2MP Progressive scan CMOS or better	
2	Resolution	1920x1080, 1280x1024, 1280x960, 1280x720, 1024x768, 800x600, 800x448, 720x576, 720x480, 640x480, 640x360, 320x240 or better	
3	Max. Framerate	H.265 or better/H.264: Max. 60fps/50fps(60Hz/50Hz) MJPEG: Min. 30fps/25fps(60Hz/50Hz)	
4	Min. Illumination	Color: 0.02Lux(F1.6, 1/30sec) BW: 0Lux(IR LED)	
5	Focal Length (Zoom Ratio)	4.45~222.4mm or better 30x Optical Zoom, 10X digital zoom or better	
6	Max. Aperture Ratio	F1.6(Wide)~F6.5(Tele)	
7	Angular Field of View	H: 58.6°(Wide)~1.23°(Tele) / V: 34.8°(Wide)~0.71°(Tele)	
8	Lens Type	DC auto iris, Varifocal or better	
9	Pan Range	360˚ Endless	
10	Pan Speed	Preset: 400˚/sec, Manual: 0.024˚/sec~250˚/sec	
11	Tilt Range	95˚(-5˚~90˚)	
12	Tilt Speed	Preset: 250˚/sec, Manual: 0.024˚/sec~250˚/sec	
13	Sequence	Preset(300ea), Swing, Group(6ea), Trace, Tour, Auto Run, Schedule	
14	Preset Accuracy	±0.2˚	
15	Day & Night	Auto(ICR)	
16	Backlight Compensation	BLC, HLC, WDR, SS+C42DR	
17	Wide Dynamic Range	120dB or better	
18	Digital Image Stabilization	Support (built-in gyro sensor)	
19	Defog	Available	

20	Motion Detection	8ea, polygonal zones Support	
21	Privacy Masking	24ea, rectangular zones	
22	White Balance	ATW / AWC / Manual / Indoor / Outdoor	
23	Electronic Shutter Speed	Minimum / Maximum / Anti flicker (2~1/12,000sec)	
24	Analytics	Defocus detection, Directional detection, Fog detection, Face detection, Motion detection, Digital auto tracking, Appear/Disappear, Enter/Exit, Loitering, Tampering, Virtual line, Audio detection, Sound classification, Shock detection and others. Can be achieved via VMS and VA	
25	Serial Interface	RS-485	
26	Alarm I/O	Input 4ea / Output 2ea	
27	Alarm Triggers	Analytics, Network disconnect, Alarm input	
28	Alarm Events	File upload via FTP and e-mail Notification via e-mail SD/SDHC/SDXC or NAS recording at event triggers Alarm output PTZ Preset	
29	Audio In	Selectable(mic in/line in) Supply voltage: 2.5VDC(4mA), Input impedance: 2K Ohm	
30	Audio Out	Line out, Max. output level: 1Vrms	
31	IR Viewable Length	500m or better	
32	Auto Tracking	Available	
33	Ethernet	RJ-45(10/100BASE-T), SFP(Optional)	
34	Video Compression	H.265/H.264: Main/Baseline/High, MJPEG	
35	Audio Compression	G.711 u-law /G.726 Selectable G.726(ADPCM) 8KHz, G.711 8KHz G.726: 16Kbps, 24Kbps, 32Kbps, 40Kbps AAC-LC: 48Kbps at 16KHz	
36	Bitrate Control	H.264/H.265: CBR or VBR MJPEG: VBR	
37	Streaming	Unicast (20 users) / Multicast Multiple streaming (Up to 10 profiles)	
38	Protocol	IPv4, IPv6, TCP/IP, UDP/IP, RTP(UDP), RTP(TCP), RTCP, RTSP, NTP, HTTP, HTTPS, SSL/TLS, DHCP, FTP, SMTP, ICMP, IGMP, SNMPv1/v2c/v3(MIB-2), ARP, DNS, DDNS, QoS, PIM-SM, UPnP, Bonjour	

39	Security	HTTPS(SSL) Login Authentication Digest Login Authentication IP Address Filtering User access log 802.1X Authentication (EAP-TLS, EAP-LEAP)	
40	Application Programming Interface	ONVIF	
41	Edge Storage	Micro SD/SDHC/SDXC 2 no. slot of 512GB capacity each or better with minimum 512GB memory card.	
42	Operating Temperature / Humidity	minus 50°C~+55°C / Less than 90% RH	
43	Ingress Protection Shock and Vibration Resistance	IP66, IK10	
44	Input Voltage	24VAC, HPoE	
45	Power Consumption	24VAC: Max. 92W HPoE: 60W	
46	Certification	UL, CE, FCC, BIS, EMC, UL CAP, NDAA	
47	Warranty	Minimum 5 years	

6.11 Smart Kiosks

S. No.	Indicative Requirement Description	Compliance (Yes / No)
	Make:	
	Model:	
1	Self Service Kiosks shall have integrated:	
	· Emergency Call Box function (with Camera and Microphone)	
	· MIFARe or equivalent Card Reader	
	· Contact less EMV Card reader	
	· Touch Screen for availing services with in-built interactive platform	
	· Speaker	
	· Onscreen Keyboard	
	· Printing of any receipts and bus tickets etc.	

	· Kiosk structure (shell)	
	· 3G/ 4G /5G/ Wi-Fi Module	
	· QR code / Bar code Interface	
	All these components shall be supplied as part of the integrated multi services digital kiosk.	
2	Self-service Tourist Information Kiosk shall be fixed units, embedded inside the ground that shall be weather-proof	
3	The design of Kiosk terminal shall be based on the City's heritage theme	
4	The Emergency Call Button (ECB) shall have the capability to trigger emergency communications with Integrated Command and Control Centre (ICCC). As the Emergency Call Button is pressed, the call should land up to the operator at ICCC from where it may be routed to the concerned department.	
5	The ICCC shall able to monitor the video of the user who triggered the ECB. Automatic video recording shall be enabled when ECB button is pressed at Self-service Tourist Information Kiosk.	
6	The user-interface panel shall built-in capacitive touch screen for interactive purposes including but not limited to:	
	· **City Guide**: This component displays the city information, about city, business hubs etc. Places near me services which may include hotels, government offices, shops, tourist attraction, etc.	
	· **Tourist Destination**: This component displays the list of tourist destinations in the city along with the navigation map	
	· **View Hotels**: This component displays the list of hotels in the city with facilities and tariffs etc. with relevant filters	
	· **View Restaurants**: This component displays the list of hotels in the city with facilities and tariffs etc. with relevant filters	
	· **View Tourist Packages**: This component describes the available tourist packages	
	· **Helpline**: This component displays the helplines of Police, Fire, Ambulance, Railways enquiry, Public Transport and Tourist Information Centre etc.	
	· **Events**: This component shall have schedule of events in the city with facility to book the tickets online	
	· **Emergency call:** This component shall allow registered users to make emergency call to the nearest police station based on the current location of the app user	

	· **Public Transport Route**: This component shall list Public transport route and schedule	
	· **Content Management to be available to admin users**: This component be used to create, update, delete content. It also covers review and approval of content by the respective content owner	
	· Weather related information	
7	Self-service Tourist Information Kiosk shall have capabilities for making digital payments for:	
	· Tickets for the events around the city	
	· Hotel accommodation	
	· Railway and Bus tickets	
	The selected Agency is required to use third party portal integration for Hotel, Travel and Event ticket booking services.	
8	Self-service Tourist Information Kiosk shall have in-built receipt/ticket printer having the functionality of printing of receipts, any other tickets, etc.	
9	Self-service Tourist Information Kiosk shall have the space for providing the static advertisement. For publishing of any advertisement, necessary approvals shall be obtained from Purchaser	
10	Self-service Tourist Information Kiosk shall be multilingual i.e. it shall support languages such as English, Hindi and regional language	
11	Self-service Tourist Information Kiosk shall be upgradable through a central system remotely over internet	
12	It shall be possible to monitor critical parameters related to health of kiosk device remotely using the network.	
13	Battery Backup of minimum 1 Hour	
14	Shall accept all the leading RBI approved wallets and UPI payments	
15	Kiosk enclosure shall have the space to house all the hardware equipment required for the Kiosk including switches, batteries, printer for receipts and other associated accessories.	
	All the wiring shall be concealed within the Kiosk enclosure and shall not be visible from outside	
16	**Kiosk Content Management Application:**	
	Following functionality is envisaged in the Kiosk Content Management Application:	

	·Provide role-based user access mechanism where an administrator can create and manage users, user groups, roles, and role permissions	
	·Shall provide login module using which content authors will be able to login and enable the creation, modification, and deletion of templates to enable easy management of Kiosk User interface/site and page layout and navigation	
	·Shall provide a WYSIWYG (What you see is what you get) editor and provide standard Word authoring features (also known as a Rich Text Editor) to enable an editor to add and format text, links, and images to content areas, create tabular layouts within a text area and apply styles without needing HTML skills	
	·Shall support drag and drop feature to enable easy management of content. The editor shall support the following minimum preview and publication functions: -	
	• Preview only on content editor (not visible to users)	
	• Save as unpublished (draft)	
	• Preview on Portal	
	• Send for approval	
	• Approve	
	• Publish after approval (i.e. after successful completion of the approval workflow)	
	• Unpublish (save as unpublished, not visible to users)	
	• Publication scheduling	
	• Publication expiration date (automatic unpublish)	
	• Shall contain a content approval workflow to enable the approval of modifications (create, modify, delete) before publication (i.e. before becoming visible to the public)	
17	• Shall support Administrator (or a designated user with an appropriate permission level) to assign and reassign users to workflow tasks (i.e. define the targets within the workflow)	
	• Layout and content shall be managed separately (i.e. it must be possible to create and edit content without having to amend or create a template)	
	• Shall support creation of navigation, breadcrumb and sitemap that will be published and rendered on Kiosk User Interface	
	• Shall support version control (check-in, check-out, number of versions) and it must be possible to restore previous versions of a content item	

	• Shall support creation of content in different languages (namely English, Hindi & regional language	
	• Shall support hierarchical creation of sites (i.e. parent/child sites in the same domain) and enable the child site to either inherit the look & feel of the parent site or have its own style and branding	
	• Shall be capable of storing and categorizing documents, images, video and audio files.	
	• CMS shall support the creation of an alert in response to a specific event, such as:	
	• Content amendment	
	• Content expiration date approaching	

6.12 Local Processing Units (LPU):

Sl.No	Specification	Compliance (Yes /No)
	Make :<to be provided by the bidder>	
	Model :<to be provided by the bidder>	
1	Local Processing Unit shall be of Aluminium Alloy Casing	
2	Compute: Intel Core i7, 7th Gen or better	
3	LPU should have 2*Intel I210AT PCIe Gig. Ethernet	
4	It shall support GPU Intel® HD Graphics 630 min.	
5	Memory- DDR4 up to 16GB	
6	Display Port- 1 nos. VGA, 1 nos. HDMI, 1 nos. DP	
7	It shall support Secondary Storage 1*1TB 3.5"SATA HDD	
8	It shall support USB- 6 nos. USB 3.0 and 2 nos. USB 2.0	

6.13 External IR Illuminator (Optional)

Technical Specifications -External IR Illuminator		
Sr. No.	**Item Description**	**Compliance (Yes/No)**
1	Type: External IR illuminator with high performance LED (42 Pcs. high brightness IR LED), high efficiency, energy saving and environmental protection.	
2	Wavelength: ≥850 nm (Infrared)	
3	Coverage Area: 1 Lane (standard for ANPR), up to 4 lane for surveillance	
4	Illumination Range: up to 100 Mtrs.	
5	Protection Level: IP66, IK10	
6	IR Power: 80 W	
7	Adjustable angle to appropriately focus at the number plate.	

	Beam Angle: multiple options- 10 degree (standard), 15, 30, 45 degrees	
8	Surge level: Common mode 6KV, Differential mode: 3 KV	
9	Certifications: CE, FCC, RoHS, Eye Safety test report	
10	Protection function: Transient over peak suppression	
11	Housing material: Die-casting aluminium alloy	
12	User Interface: RS485	
13	Working Temperature: -40 +70 C (working humidity 10% - 95%)	
14	Proposed IR Illuminator should be IP66, IK10, CE, FCC, RoHS and Eye & Skin safety test report IEC-62471 certified.	

Power- Voltage Input: DC6~48V

Sl.No	Specification	Compliance (Yes /No)
	Make :<to be provided by the bidder>	
	Model :<to be provided by the bidder>	
1	AC Input: External Adapter (Option)	
2	Voltage Input: 100VAC~240VAC@50~60Hz	
3	Temperature- -20°C ~ 70°C	
4	It shall withstand vibrations	
5	It shall withstand shock	
6	Hardware / software should have minimum 5 year warranty	

6.14 Network Connectivity - OFC

It is proposed to setup city wide OFC network connectivity as the field components increases data transfer, size also increases hence there is need for fast data transfer with high availability.

Surveillance and Security

In order to improve the quality of life for residents, the first step is safety for any city to evolve as a Smart City. In the past few years, implementation of surveillance cameras has improved public safety and prevented crime. However, today new types of sensors are installed and those are way too advanced than basic surveillance cameras and requires high data transmitting speed. Thus, Fiber optics play a very crucial role here.

Traffic Control

Traffic is one of the most significant challenges in the cities that are experiencing rapid growth. Thus, the need for fiber Optics is increasing, as it's used at many places in order to tie together the enormously complex networks that control sensors like the Automatic traffic lights, Variable message sign board,

cameras and ATCS systems technology. The sensors at Junctions and video with analytic functionality provide real-time data on Traffic congestion while the traffic control cameras are connected by fibre optics to the transport authority. They can monitor traffic in real time, making the control centre more efficient and intelligent for them to increase or reduce the frequency of green lights according to the traffic conditions.

Integrated Command and Control Center

ICCC can be connected with City field components through fiber optic internet. ICCC have the ability to provide centralized services, security, climate control, etc. Here fiber optic cables provide the best means of handling this data and transmitting it around a facility.

Cities around the globe have been transforming from traditional to smart cities that will benefit everyone. Fibre optics and IoT are substantial and helping us get one step closer to this reality. Reliability, security and speed are key to the efficient implementation of Smart cities and IoT and fibre optics are one of the first real time solutions available today.

Network Layers

Street Layer

All the access layer devices like outdoor network access points, cameras for surveillance, environmental sensors, VaMS, PAS including other Smart city initiatives will connect to ruggedize industrial grade access switches in street cabinets and will create street layer architecture. Street layer architecture should be built considering the harsh outdoor deployment environment and should be flexible to connect various devices/ sensors to the citywide transport network.

City Network Layer

The city network layer aggregates street access switches and access points and connects to the data center and other locations used for monitoring and managing the infrastructure. Network layer will create transport network for City and will laid down the foundation for all the present and future urban services. This layer will provide City scalability to both expand existing services and roll out new services as and when required without any dependency on any service provide bandwidth operation cost. Also this layer provides the flexibility to run multiple concurrent services with required segregation and prioritization.

Data Center Layer

The data center layer includes all our WAN routers, core switches, servers, and storage resources for citywide applications and service. Data center layer will be the heart of City operation will host all the Citizen services and provide the centralized processing for the same.

Considering the above requirement new OFC network is proposed as per BoM.

7 Approach and methodology to be adopted for implementation:

- The SI shall first carry out a detailed survey to identify & finalize the locations, requirements vis-a-vis proposed solutions.
- Post completion of Survey the SI shall consult the various Stake Holder of the project, in consultation with the Authority, and revalidate the scope mentioned in this document. Upon freezing the scope requirement, the SI shall detail out the final functional requirement for each of the proposed ICT intervention and get a sign off from the user department and the Authority.
- Post finalization of the SRS and FRS the SI shall submit a High-Level Design Document which shall cover the broad architecture and a solution document for each of the proposed ICT interventions. The HLD will comprise of the compute, storage and the OS requirements.

- Post HLD, the SI shall be submitting the Low-Level Design Document with the good for construction drawing, network connectivity drawing, LPU details, if any, API for integration, communication protocol etc.
- Upon approval of LLD by the Authority, the SI shall implement the said ICT intervention.
- While implementing the ICT intervention the SI shall adopt the following:

Scalability - The system should also support both vertical and horizontal scalability. There must not be any system-imposed restrictions on the upward scalability in number of field devices, or other smart city components. The Applications proposed for various vertical solutions shall be capable of handling 50% growth for the next 5 years. SI shall clearly quantify the expansion capabilities of the application software without incurring additional cost.

Availability -. The SI shall make the provision for high availability for all the services of the system. Redundancy has to be considered at the core components level. The SLA for various solutions is explained under each solution itself .

Security- The architecture must adopt an end-to-end security model that protects data and the infrastructure from malicious attacks, theft, natural disasters etc. SI must make provisions for security of field equipment as well as protection of the software system from hackers and other threats. Attacks and theft should be controlled and well supported (and implemented) with the security policy. The 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.

Field equipment installed through this Project would become an important public asset. During the contract period of the Project the SI shall be required to repair / replace any equipment if stolen / damaged/faulty. Appropriate insurance cover must be provided to all the equipment supplied under this project.

The security services used to protect the solution shall include: Identification, Authentication, Access Control, Administration and Audit and support for industry standard protocols. The solution should provide for maintaining an audit trail of all the transactions and should also ensure the non-repudiation of audit trail without impacting the overall performance of the system. The overarching requirement is the need to comply with ISO 27001 standards of security. The application design and development should comply with OWASP top 10 principles. All the field devices will be X.509 certified for compliance to policy change management and to ensure that there is no default password.

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. Network should be auto/manual configurable for various future requirements for the ease of maintenance / debugging.

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.

Open Standards - Systems should use open standards and protocols to the extent possible

Single Sign On- The application should enable single-sign-on so that any user once authenticated and authorized by system is not required to be re-authorized for completing any of the services in the same session. For employees of the department concerned, the browser-based application accessed on the intranet, through single-sign-on mechanism, will provide access to all the services of the departments concerned (based on their roles and responsibilities), Help module, basic and advanced reporting etc. Similarly, for external users (citizens, etc), based on their profile and registration, the system shall enable single-sign on facility to apply for various services, make payments, submit queries /complaints and check.

Support for PKI based Authentication and Authorization- The solution shall support PKI based Authentication and Authorization, in accordance with IT Act 2000, using the Digital Certificates issued by the Certifying Authorities (CA). In particular, 3 factor authentications (login id & password, biometric and digital signature) shall be implemented by the SI for officials/employees involved in processing citizen services.

Interoperability Standards- Keeping in view the evolving needs of interoperability, especially the possibility that the solution shall become the focal point of delivery of services, and may also involve cross-functionality with the e-Government projects of other departments / businesses in future, the solution should be built on Open Standards. The SI shall ensure that the application developed is easily integrated with the existing applications. The code does not build a dependency on any proprietary software, particularly, through the use of proprietary 'stored procedures' belonging to a specific database product. The standards should:

At least comply with the published e-Governance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and

Be of leading industry standards and /or as per standards mentioned in the technical specifications

Application Architecture

a. The applications designed and developed for the departments concerned must follow best practice and industry standards. In order to achieve the high level of stability and robustness of the application, the system development life cycle must be carried out using the industry standard best practices and adopting the security constraints for access and control rights. The various modules / application should have a common Exception Manager to handle any kind of exception arising due to internal/ external factors. Standards should (a) at least comply with published e-Governance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in (updated from time-to-time); and (b) be of leading industry standards and /or as per standards mentioned in the technical specifications

ii. The modules of the application are to be supported by the Session and Transaction Manager for the completeness of the request and response of the client request. The system should have a module exclusively to record the activities/ create the log of activities happening within the system / application to avoid any kind of irregularities within the system by any User / Application.

iii. SI shall design and develop the Smart City System as per the Functional and System requirement specifications finalized.

iv. The Modules specified will be developed afresh based on approved requirement.

8 Lifecycle of implementation of ICT intervention:

Following are the main activities to be carried out I:

1. Project Planning, execution and Management
2. Assessment and Gap analysis of requirement for all smart city components under scope.
3. Solution Design, System Customization and development for all components mentioned in this volume.
4. ICT items Procurement, deployment and commissioning
5. Site Preparation including required civil work, LAN Networking
6. Application and general awareness Training
7. Business Process Reengineering for the selected applications/ services, if required
8. STQC Certification
9. UAT & Go live

10. Capacity Building
11. Technical Support
12. Operation & Maintenance (O&M) for 5 Years.

9 Detailed Technical and Non-Technical Manpower:

The project requires being setup initially in an implementation phase spanning about nine months and to be operated and maintained for a further 60 Months period to transform the departments of stakeholders of PSCDL into a fully digitized way of operations. This requires a highly skilled expertise in all the envisioned ICT technical function areas both during the implementation phase and in the operations and maintenance phase.

The Key experts are listed in the table below along with their functional roles and an approximate period of implementing the envisioned solution.

To implement and successfully execution of project below is the man months required for both Implementation and O&M phase

1	**Manpower for Implementation Phase and O&M**	**TYPE**	**UoM**	**QTY**
1.1	Project Manager - 1 no	Service	Number	1
1.2	Solution Architect and Cloud expert - 1 no	Service	Number	1
1.3	ICCC / command center Expert - 1no	Service	Number	1
1.4	Network Architect - 1 no	Service	Number	1
1.5	Security Infrastructure and CCTV specialist - 1 each	Service	Number	1
1.6	GIS Expert - 1 no	Service	Number	1
1.7	Data Management Expert / Analyst - 1 no	Service	Number	1
1.8	Business Analyst/Use case/SOP Expert - 1 no	Service	Number	1
1.9	Server / Storage/ Database Expert - 1 no	Service	Number	1
1.10	ITMS & ATCS Expert - 1 no	Service	Number	1
1.11	Electrical Engineer - 1 Person	Service	Number	1
1.12	Electrical Technician - 2 Person	Service	Number	2
1.13	OFC Expert - 1 no	Service	Number	1
1.14	Helpdesk operator (20 no)	Service	Number	20
1.15	Security staff (4 no)	Service	Number	4

1.16	Civil Technician - 2 person	Service	Number	2
1.17	Civil Engineer - 1 no	Service	Number	1
1.18	Field Engineer - 5 Persons	Service	Number	5
1.19	Office staff, Reception (3 no)	Service	Number	3

10 Use cases to be deployed / integrated:

#	**Use cases to be deployed**
1	ICCC Platform
2	Intelligent Traffic Management System
3	City Surveillance with video analytics
4	Variable Message Display
5	PA system
6	Environmental Sensors
7	Smart Poles (with CCTV, Wi-Fi, AQM, Smart Street Light, ECB, PA, Digital Billboard)
8	Citizen Mobile App and Web Portal with Tourist/Visitors platform
9	City Data Collaboration Platform
10	Smart Kiosk
11	Smart Parking (Additional Deployment as per requirement of DRDM/ PSCDL)
12	EMS
13	Flood monitoring through Flood sensors and cameras
14	GIS Platform
15	OFC
16	Social Media
17	Chat bot
18	Digital assistant Application with ICCC platform Integration
19	Configurable Dashboard

Sl.No	**Integration of Existing Applications**
1	Applications hosted by NIC
2	E-Governance Platform (Property Tax, Building Approval, Birth/Death, Marriage etc.,)
3	Electrical SCADA
4	e-Health
5	Websites hosted by Puducherry Municipality and Oulgaret Municipality
6	Solid waste Management
7	Water/ Sewage SCADA
8	ERSS (Dial 100/112)
9	Applications hosted by Disaster Management
10	Transport Monitoring Centre
11	Integration with RTO
12	Any other integration as suggested by the Puducherry authorities (up to 12 months from the date of issue of LOA to the SI)

10.1 Digital Assistant Application

In order to ensure that the impact of Smart City investments impacts the common man and creates smart livelihoods a platform for enabling unemployed youth to be digital entrepreneur is envisaged While connectivity is the first stage of digital inclusion , enabling digital transactions would be the right metric to evaluate the access to digital services . Statistics indicate that only about 3% of the population actually carry out transactions and reap the benefits of digital world.

It is proposed to depute one technical engineer at one of the smart kiosk location as " Digital assistant "to assist the local community to carry out transactions on the net for E-governance services, tickets, assisted E-commerce , last mile aggregation services and " Phygital " interface for other upstream services such as finance , credit , health care etc.

11 Training, Audit and Change Management Plan:

Training and Change Management is highly critical component for implementation of Smart City Solutions. The objective of Training and Change Management initiatives is to empower the direct users and other stakeholders of DRDM and Puducherry Smart City Corporation Limited to optimally use the system and ensure achievement of end objectives of various Smart City Solutions.

In order to strengthen the staff, structured capacity building programs shall be undertaken for multiple levels in the organizational hierarchy like foundation process/ soft skills training to the staff for pre-defined period. Also, refresher trainings for integrated Command Control Centre, City Operation Staff and designated departments shall be a part of Capacity Building. It is important to understand that training needs to be provided to each and every staff personnel of ICCC. These officers shall be handling emergency situations with very minimal turnaround time. Some directions with regards to the training and change management plan which will need to be prepared by the implementing solution provider are as follows:

1. Appropriate training shall be carried out as per the User Training Plan prepared in detail stating the number of training sessions to be held per batch of trainees, course work for the training program, coursework delivery methodologies and evaluation methodologies in detail.
2. End user training shall include all the equipment including but not limited to all the applications and infrastructure at ICCC, ITMS, Safety and Surveillance and other smart solutions. End user training shall be conducted at a centralized location or any other location as identified by PSCDL.
3. Imparting operational and technical training to internal users on solutions being implemented to allow them to effectively and efficiently use the surveillance system.
4. Preparation of the solution specific training manuals and submit the same to purchaser for review and approval. Training Manuals, operation procedures, visual help-kit etc. shall be provided in English language.
5. Ensuring that all concerned personnel receive regular training sessions, from time to time, as and when required. Refresher training sessions shall be conducted on a regular basis.
6. An annual training calendar shall be prepared and shared with the Client along with complete details of content of training, target audience for each year etc.
7. Updating training manuals, procedures manual, deployment/Installation guides etc. on a regular basis (Quarterly/ Biannual) to reflect the latest changes to the solutions implemented and new developments.
8. Ensuring that training is a continuous process for the users. Basic computer awareness, fundamentals of computer systems, basic, intermediate and advanced application usage modules shall be identified by the solution provider.
9. Systematic training shall be imparted to the designated trainees that shall help them to understand the concept of solution, the day-to-day operations of overall solution and maintenance and updating of the system to some extent. This shall be done under complete guidance of the trainers provided by the solution provider.
10. Training sessions and workshops shall comprise of presentations, demonstrations and hands-on mandatorily for the application modules.

12 Proposed Governance Model:

The proposed project governance structure would comprise the following:

- High level steering committee, Board members of PSCDL, DRDM and Senior Executives of RailTel
- Project specific working group, comprising the respective departmental functional, RailTel Project Manager and select team members for the respective module(s).
- Core team members, domain specialists and designated counterpart staff from PSCDL/ concerned Government Agency for individual modules.
- Support team

The steering committee would meet once every month to take important decisions and approve any strategic decisions to ensure timely implementation and address identified bottlenecks. The project specific working groups would convene on a weekly or a bi-weekly basis to discuss progress and address any issues pertaining to implementation.

13 Exit Management Under Contract Completion:

1. Provide a comprehensive exit management plan.
2. Before 6 months prior to the contract ending, RailTel shall ensure through SI fully train Puducherry Authorities' staff or any other agency designated by Puducherry Authorities who is designated to take over the maintenance of the System.
3. The SI shall ensure through SI for transferring all the knowledge regarding the Systems, technically and operationally to enable the new agency/ Puducherry Authorities to carry out the requisite functions.
4. All latest operations & technical manuals, configuration files, software, licenses, as-built drawings etc. shall be handed over to Puducherry Authorities at least 3 months before contract completion.
5. The Parties may, if mutually agreed, extend the contract in accordance with the terms and conditions.
6. All source codes, backup data, Puducherry Authorities specific information shall be handed over to Puducherry Authorities as part of exit management.
7. All ICT systems shall be properly handed over to Puducherry Authorities in operational state as part of exit management.
8. The SI shall ensure through SI be responsible for providing the tools for import /export of VMs & content and the SI shall ensure through SI be responsible for preparation of the Exit Management Plan and carrying out the exit management / transition.
9. SI shall ensure through SI be responsible for migration of the VMs, data, content and any other assets to the new environment and ensuring successful deployment and running of the Puducherry Authorities' solution on the new infrastructure by suitably retrieving all data, scripts, software, virtual machine images, and so forth to enable mirroring or copying to industry standard media
10. The format of the data transmitted from the cloud service provider to the new environment created by the Puducherry Authorities should leverage standard data formats whenever possible to ease and enhance portability.
11. The SI shall ensure through SI transfer the organizational structure developed during the Contract Duration to support the delivery of the Exit Management Services. This will include: Document, update, and provide functional organization charts, operating level agreements with Third-Party contractors, phone trees, contact lists, and standard operating procedures. Transfer physical and logical security processes and tools, including cataloguing and tendering all badges and keys, documenting ownership and access levels for all passwords, and instructing Puducherry Authorities or its authorized representative in the use and operation of security controls.
12. Retain the data at the end of the Contract.
13. Once the exit process is completed, remove the data, content and other assets from the cloud environment and destroy the VM, Content and data of Puducherry Authorities.
14. The ownership of the data generated upon usage of the system, at any point of time during the Contract or expiration of the Contract, shall rest absolutely with Puducherry Authorities.

15. This sets out the provisions, which will apply on expiry or termination of the Master Service Agreement, the Project Implementation, Operation and Management SLA.
16. 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.
17. The Parties shall ensure that their respective associated entities carry out their respective obligations set out in this Exit Management Schedule.

14 Detailed work Phases and considerations

14.1.1 Phase 1(Implementation Phase)

14.1.1.1 Requirement Survey Phase

The SI must perform the detailed assessment of the IT Solution requirements as mentionedin this RFP. Based on the understanding and its own individual assessment, SI shall develop & finalize the System Requirement Specifications (SRS) in consultation with RAILTEL / DRDM/ PSCDL and its representatives. While doing so, SI at least is expected to do following:

i. SI shall develop the FRS and SRS documents.
ii. SI shall develop and follow standardized template for requirements capturing and system documentation.
iii. SI must maintain traceability matrix from SRS stage for the entire implementation.
iv. SI must get the sign off from the various departments of Puducherry.
v. Prior to starting the site clearance, the SI shall carry out survey of field locations as specified in Annexure VIII, for buildings, structures, fences, trees, existinginstallations, etc.
vi. All existing road signs which are likely to be affected by the works are to be carefully taken down and stored. Signs to be re-commissioned shall be cleaned, provided withnew fixings where necessary and the posts re-painted in accordance with PSCDL guidelines. Road signs, street name plate, etc. damaged by the SI during their operation shall be repaired or replaced by SI at no additional cost.

14.1.1.2 Design Phase

The SI shall build the solution as per the Design Considerations detailed in **Section 6.** The solution proposed by SI should comply with the design considerations requirements as mentioned therein.

14.1.1.3 Project Development Phase

Software (Configuration and Customization). Following need to be adhered:

1) SI will be responsible for supplying the application and licenses of related software and installing the same so as to meet project requirements.
2) The SI shall perform periodic audits to measure license compliance against the number of valid End User software licenses consistent with the terms and conditions of license agreements, volume purchase agreements, and other mutually agreed upon licensed software terms and conditions. The SI shall report any exceptions to license terms and conditions at the right time to PSCDL/DRDM. However, the responsibility of license compliance solely lies with the SI. Any financial penalty imposed on PSCDL/DRDM during the contract period due to license non-compliance shall be borne by SI.

3) SI shall also supply any other tools & accessories required to make the integrated solution complete as per requirements. For the integrated solution, the SI shall supply:

    a) Software & licenses.
    b) Supply tools, accessories, documentation and provide a list of the same. Tools and

accessories shall be part of the solution.

c) System Documentation: System Documentation both in hard copy and soft copy to be supplied along with licenses and shall include but not limited to following. Documentation to be maintained, updated and submitted to PSCDL/DRDM/RailTel regularly:
   - Functional Requirement Specification (FRS)
   - High level design of whole system
   - Low Level design for whole system / Module design level
   - System Requirements Specifications (SRS)
   - Any other explanatory notes about system
   - Traceability matrix
   - Technical and product related manuals
   - Installation guides
   - User manuals
   - System administrator manuals
   - Toolkit guides and troubleshooting guides
   - Other documents as prescribed by PSCDL/DRDM/RailTel
   - Quality assurance procedures
   - Change management histories
   - Version control data
   - SOPs, procedures, policies, processes, etc. developed for PSCDL/DRDM/RailTel
   - Programs
   - Entire source codes
   - All programs must have explanatory notes for understanding
   - Version control mechanism
   - All old versions to be maintained
   - Test Environment
   - Detailed Test methodology document
   - Module level testing
   - Overall System Testing
   - Acceptance test case

These documents need to be updated after each phase of project and to be maintained updated during entire project duration. The entire documentation will be the property of PSCDL/DRDM.

14.1.1.4 Integration Phase

The Command-and-control center should be integrated with feeds of all component under the ICCC Project. The SI shall provide the testing strategy including traceability matrix, test cases and shall conduct the testing of various components of the software developed/customized and the solution-as-a-whole. The testing should be comprehensive and should be done at each stage of development and implementation.

14.1.1.5 Go-Live Preparedness and Go-Live

i. SI shall submit signed-off UAT report (issue closure report) ensuring all issues raised during UAT are being resolved prior to Go-Live.

ii. SI shall ensure that Go –Live criteria as mentioned in User acceptance testing of Project is met and SI needs to take approval from the Authorities on the same.

14.1.1.6 Project Management & Facilities Management Services

The SI will be required to provide facilities management services to support the PSCDL/DRDM/RailTel and stakeholder department officials in performing their day-to-day functions related to this system.

SI is required to depute a dedicated, centralized project management and technical team for the overall project management and interaction with PSCDL and stakeholder departments.

14.1.1.7 Provision of the Operational Manpower & Contact Center

Manpower to view the various data feeds and call center operations at ICCC
The SI is required to provide suitable manpower to monitor the data feeds ICCC and support PSCDL/DRDM/RailTel, Traffic Police and other stakeholder departments for operationalization of smart solutions of the project. The exact role of these personnel and their responsibilities would be defined and monitored by PSCDL/DRDM/RailTel and respective departmental personnel. SI shall be required to provide such manpower meeting following requirements:

i. All such manpower shall be minimum graduate pass
ii. All such manpower shall be without any criminal background / record.
iii. PSCDL/DRDM/RailTel 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.
iv. SI shall have to replace any person, if not found suitable for the job.
v. All the manpower shall have to undergo training from the SI for at least 15 working days on the working of project. Training should also cover dos & don'ts and will have few sessions from PSCDL/DRDM/RailTel and Stakeholders/End User Department officers on right approaches for monitoring the feeds & providing feedback to PSCDL/DRDM/RailTel, Stakeholders/End User Department officers and other associated government agencies.

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

14.1.1.8 Basic Infrastructure Services

Following services shall be provided by the SI under the basic infrastructure services:

i. Ensure availability of the infrastructure (both physical and IT) including but not limited to Power, Cooling, Racks, Storage and other peripheral equipment installed at the time of Project commissioning as per the SLAs.

ii. Ensure scalability in terms of availability of racks and supporting infrastructure.
iii. Proactive and reactive maintenance, repair and replacement of defective components (physical and other peripheral IT infrastructure) installed for the Project through this RFP. The cost for repair and replacement shall be borne by the SI.
iv. Any component (Physical & IT installed at the time of Project commissioning) that is reported to be faulty / non-functional on a given date should be either fully repaired or replaced by temporary substitute (of equivalent configuration) within the time frame agreed upon in the Service Level Agreement (SLA).
v. Proactive monitoring of the entire basic infrastructure installed.
vi. SI shall maintain records of the maintenance of the basic infrastructure and shall maintain a logbook on-site that may be inspected by the PSCDL/DRDM/RailTel, Police department and other stakeholder departments/end users at any time.

14.1.1.9 Network Monitoring Services

The activities shall include:

i. SI shall provide services for management of ICCC Project to maintain performance at optimum levels on a 24 x 7 basis.
ii. SI shall monitor and administer the network.
iii. SI shall create and modify VLAN, assignment of ports to appropriate applications and segmentation of traffic.
iv. SI shall carry out break fix maintenance of the LAN cabling or maintenance work requiring civil work.

14.1.1.10 Integration Testing

This shall be a black-box testing role primarily to ensure that the application to be deployed does not disrupt the Puducherry operations and affect other Puducherry infrastructure in terms of performance and security. The technical tasks to be carried out shall be as follows:

i. Functional Testing: Ensuring that the application functionality as described by the PSCDL/DRDM/RailTel, Police department and other stakeholder departments/end users. The functional testing of application will necessarily be minimal as this is a core responsibility of the Supplier.
ii. Performance Testing: Ensuring that the application meets expressed performance requirements on the Puducherry servers by using performance test tools and performance monitoring tools.
iii. Security Testing: Testing for exploitable application security weaknesses that undermine the application security or the security of the infrastructure.

14.1.1.11 Vendor Management Services

The activities shall include:

i. Coordination with all the project stakeholders to ensure that all Puducherry activities are carried out in a timely manner.

ii. SI shall coordinate and follow-up with all the relevant vendors to ensure that the issues are resolved in accordance with the SLAs agreed upon with them.
iii. SI shall also ensure that unresolved issues are escalated to respective departments.
iv. SI shall maintain database of the various vendors with details like contact person, telephone nos., escalation matrix, response time and resolution time commitments etc.
v. SI shall draw a consolidated quarterly SLA performance report across vendors for consideration of the PSCDL/DRDM/RailTel, Police department and other stakeholder departments/end users.

14.1.1.12 Network Management

The objective of this service is to ensure continuous operation and upkeep of the Network infrastructure of the project including all active and passive components. The selected SI shall be responsible to coordinate with Network Service Provider for network related issues between ICCC, DC and other sub systems. The services to be provided for Network Management include:

i. Ensuring that the network is available 24x7x365 as per the prescribed SLAs for the 5 years of operations after final acceptance testing of all equipment's and services.
ii. Attending to and resolving network failures and snags.
iii. Support and maintain the overall network infrastructure including but not limited to LAN passive components, routers, switches etc.
iv. Configuration and backup of network devices including documentation of all configurations.
v. 24x7x365 monitoring of the network to spot the problems immediately.
vi. Provide information on performance of Ethernet segments, including capacity utilization and error statistics for the segment and the top-contributing hosts, WAN links and routers.
vii. Ensuring timely information to the PSCDL/DRDM/RailTel, Police department and other stakeholder departments/end users pertaining to issues of Network Backbone

14.1.1.13 Physical Infrastructure Management and Maintenance Services

All the devices that will be installed in the Project as part of the physical infrastructure should be SNMP enabled and shall be centrally and remotely monitored and managed on a 24x7x365 basis. Industry leading infrastructure management solution should be deployed to facilitate monitoring and management of the Infrastructure on one integrated console. The physical infrastructure management and maintenance services shall include:

i. Proactive and reactive maintenance, repair and replacement of defective components (IT and Non-IT/ Hardware and Software). The cost for repair and replacement shall be borne by the SI.
ii. The SI shall have to stock and provide adequate onsite and offsite spare parts and spare component to ensure that the uptime commitment as per SLA is met. To provide this service it is important for the SI to have back to back arrangement with the OEMs. The SI needs to provide a copy of the service level agreement signed with the respective OEMs.
iii. Component that is reported to be down on a given date should be either fully repaired or replaced by temporary substitute (of equivalent configuration) within the time frame indicated in the Service Level Agreement (SLA). In case the selected SI fails to meet the above standards of maintenance, there will be a penalty as specified in the SLA.

iv. The selected SI shall also maintain records of all maintenance of the system and shall maintain a logbook on-site that may be inspected by the PSCDL/DRDM/RailTel, Police department and other stakeholder departments/end users at any time.

14.1.2 Phase-2 (Operations and Maintenance)

Success of the Project would lie on how professionally and methodically the entire Project is managed once the implementation is completed. From the SI perspective too, this is a critical phase since the quarterly payments are linked to the SLA's in the post implementation phases. SI shall provide operations and maintenance services for the software, hardware and other IT and Non-IT infrastructure installed as part of the project after Go-Live for a period of 5 years. Warranty period of the product supplied under project i.e. hardware, software, IT/Non-IT etc., will be considered after phase wise Go-Live.

14.1.3 Project Management and Governance

14.1.3.1 Project Management Office (PMO)

A Project Management office will be set up during the start of the project. The PMO will, at the minimum, include a designated full time Project Manager from SI. It will also include key persons from other relevant stakeholders including members of PSCDL/DRDM/RailTel and other officials/representatives by invitation. The operational aspects of the PMO need to be handled by the SI including maintaining weekly status, minutes of the meetings, weekly/monthly/project plans, etc.

PMO will meet formally on a weekly basis covering, at a minimum, the following agenda items:

i. Project Progress
ii. Delays, if any – Reasons thereof and ways to make-up lost time
iii. Issues and concerns
iv. Performance and SLA compliance reports;
v. Unresolved and escalated issues;
vi. Project risks and their proposed mitigation plan
vii. Discussion on submitted deliverable
viii. Timelines and anticipated delay in deliverable if any
ix. Any other issues that either party wishes to add to the agenda.

During the development and implementation phase, there may be a need for more frequent meetings and the agenda would also include:

i. Module development status
ii. Testing results
iii. IT infrastructure procurement and deployment status
iv. Status of setting up/procuring of the Helpdesk, DC hosting
v. Any other issues that either party wishes to add to the agenda.

Bidder shall recommend PMO structure for the project implementation phase and operations and maintenance phase.

14.1.3.2 Helpdesk and Facilities Management Services

The SI shall be required to establish the helpdesk and provide facilities management services to support the PSCDL/DRDM/RailTel and stakeholder department officials in performing their day-to-day functions related to this system.

The SI shall setup a central helpdesk dedicated (i.e. on premise) for the Project, which shall be supported by individual smart city command centres, implemented and proposed to be setup under Puducherry Smart City Programme. This helpdesk would be operational upon implementation of the Project. Providing helpdesk/support services from a shared facility of any other party/provider is not permitted.

Functional requirements of the helpdesk management system fully integrated with the enterprise monitoring and network management system. The system will be accessed by the stakeholder department officials for raising their incidents and logging calls for support. The detailed service levels and response time, which the SI is required to maintain for provisioning of the FMS services are described in the Service Level Agreement of this Tender.

SI shall deploy Manpower during implementation and O&M phases. The deployed resource shall report to PSCDL/DRDM/RailTel's Project In-charge for Smart City Project and work closely with Program Management Office of the project. Following are the minimum resources required to be deployed in the Project, however SI may deploy additional resources based on the need of the Project and to meet the defined SLAs in this RFP:

Note: Numbers provided for staff providing 24*7 support is excluding relievers.

14.1.3.3 Project Monitoring and Reporting

The SI shall circulate written progress reports at agreed intervals to PSCDL/DRDM/RailTel and other stakeholders. Project status report shall include Progress against the Project Management Plan, status of all risks and issues, exceptions and issues along with recommended resolution etc.
Other than the planned meetings, in exceptional cases, project status meeting may be called with prior notice to the Bidder. PSCDL/DRDM/RailTel reserves the right to ask the bidder for the project review reports other than the standard weekly review reports.

14.1.3.4 Risk and Issue management

The SI shall develop a Risk Management Plan and shall identify, analyze and evaluate the project risks, and shall develop cost effective strategies and action plans to mitigate those risks.

The SI shall carry out a Risk Assessment and document the Risk profile of PSCDL/DRDM/RailTel based on the risk appetite and shall prepare and share the PSCDL/DRDM/RailTel Risk Register. The SI shall develop an issues management procedure to identify, track, and resolve all issues confronting the project. The risk management plan and issue management procedure shall be done in consultation with PSCDL/DRDM/RailTel.

The SI shall monitor, report, and update the project risk profile. The risks should be discussed with PSCDL/DRDM/RailTel and a mitigation plan be identified during the project review/status meetings. The Risk and Issue management should form an agenda for the Project Steering Committee meetings as and when required.

14.1.3.5 Governance procedures

SI shall document the agreed structures in a procedure's manual.

14.1.3.6 Planning and Scheduling

The SI will prepare a detailed schedule and plan for the entire project covering all tasks and sub tasks required for successful execution of the project. The SI has to get the plan approved from PSCDL/DRDM at the start of the project and it should be updated every week to ensure tracking of the progress of the project.

The project plan should include the following:

i. The project breaks up into logical phases and sub-phases;
ii. Activities making up the sub-phases and phases;
iii. Components in each phase with milestones;
iv. The milestone dates are decided by RailTel in this RFP. SI cannot change any of the milestone completion dates. SI can only propose the internal task deadlines while keeping the overall end dates the same. SI may suggest improvement in project dates without changing the end dates of each activity.
v. Key milestones and deliverables along with their dates including those related to delivery and installation of hardware and software;
vi. Start date and end date for each activity;
vii. The dependencies among activities;
viii. Resources to be assigned to each activity;
ix. Dependency on PSCDL/DRDM/RailTel

14.1.3.7 License Metering / Management

The SI shall track software usage throughout the IT setup so as to effectively manage the risk of unauthorized usage or under-licensing of software installed at the ICCC. This may be carried out through the use of standard license metering tools.

14.1.4 Change Management & Control

14.1.4.1 Change Orders / Alterations / Variations

i. The SI agrees that the requirements given in the Bidding Documents are minimum requirements and are only indicative. The SI would need to fetch out the details at the time of preparing the design document prior to actual implementation. It shall be the responsibility of the SI to meet all the requirements of technical specifications contained in the RFP and any upward revisions and/or additions of quantities, specifications sizes given in the Bidding Documents required to be made during execution of the works, shall not constitute a change order and shall be carried out without a change order and shall be carried out without any time and cost effect to Purchaser.

ii. Further upward revisions and or additions required to make SI's selected equipment and

installation procedures to meet Bidding Documents requirements expressed and to make entire facilities safe, operable and as per specified codes and standards shall not constitute a change order and shall be carried out without any time and cost effect to Purchaser.

iii. Any upward revision and/or additions consequent to errors, omissions, ambiguities, discrepancies in the Bidding Documents which the SI had not brought out to the Purchaser's notice in his bid shall not constitute a change order and such upward revisions and/or addition shall be carried out by SI without any time and cost effect to Purchaser.

14.1.4.2 Change Order

i. The Change Order will be initiated only in case (i) the Purchaser directs in writing the SI to include any addition to the scope of work covered under this Contract or delete any part of the scope of the work under the Contract, (ii) SI requests to delete any part of the work which will not adversely affect the operational capabilities of the facilities and if the deletions proposed are agreed to by the Purchaser and for which cost and time benefits shall be passed on to the Purchaser, (iii) the Purchaser directs in writing the SI to incorporate changes or additions to the technical specifications already covered in the Contract.

ii. Any changes required by the Purchaser over and above the minimum requirements given in the specifications and drawings etc. included in the Bidding Documents before giving its approval to detailed design or Engineering requirements for complying with technical specifications and changes required to ensure systems compatibility and reliability for safe operation (As per codes, standards and recommended practices referred in the Bidding Documents) and trouble free operation shall not be construed to be change in the Scope of work under the Contract.

iii. Any change order as stated in this RFP comprising an alteration which involves change in the cost of the works (which sort of alteration is hereinafter called a "Variation") shall be the Subject of an amendment to the Contract by way of an increase or decrease in the schedule of Contract Prices and adjustment of the implementation schedule if any.

iv. If parties agree that the Contract does not contain applicable rates or that the said rates are inappropriate or the said rates are not precisely applicable to the variation in question, then the parties shall negotiate a revision of the Contract Price which shall represent the change in cost of the works caused by the Variations. Any change order shall be duly approved by the Purchaser in writing.

v. Within ten (10) working days of receiving the comments from the Purchaser or the drawings, specification, purchase requisitions and other documents submitted by the SI for approval, the SI shall respond in writing, which item(s) of the Comments is/are potential changes(s) in the Scope of work of the RFP document covered in the Contract and shall advise a date by which change order (if applicable) will be submitted to the

Purchaser.

14.1.5 Testing and Acceptance Criteria

i. SI shall demonstrate the following mentioned acceptance criteria prior to acceptance of the solution as well as during project operations phase, in respect of scalability and performance etc. The SI may propose further detailed Acceptance criteria which the PSCDL/DRDM will review. Once PSCDL/DRDM provides its approval, the Acceptance criteria can be finalized. In case required, parameters might be revised by PSCDL/DRDM in mutual agreement with bidder and the revised parameters shall be considered for acceptance criteria. A comprehensive system should be set up that would have the capability to log & track the testing results, upload & maintain the test cases and log & track issues/bugs identified.

ii. The following table depicts the details for the various kinds of testing envisaged for the project:

Note:

a. Bidder needs to provide the details of the testing strategy and approach including details of intended tools/environment to be used by SI for testing in its technical proposal. RAILTEL / DRDM/ PSCDL does not intend to own the tools.

b. The SI shall work in a manner to satisfy all the testing requirements and adhere to the testing strategy outlined. The SI must ensure deployment of necessary resources and tools during the testing phases. The SI shall perform the testing of the solution based on the approved test plan, document the results and shall fix the bugs found during the testing. It is the responsibility of SI to ensure that the end product delivered by the SI meets all the requirements specified in the RFP. The SI shall take remedial action based on outcome of the tests.

c. The SI shall arrange for environments and tools for testing and for training as envisaged. Post Go-Live; the production environment should not be used for testing and training purpose. If any production data is used for testing, it should be masked, and it should be protected. Detailed process in this regard including security requirement should be provided by the SI in its technical proposal. The process will be finalized with the selected bidder.

d. All the Third-Party Auditors (TPA) as mentioned above will be appointed and paid by RAILTEL / DRDM/ PSCDL directly. All tools/environment required for testing shall be provided by the SI.

e. STQC/Other agencies appointed by RAILTEL / DRDM/ PSCDL shall perform the role of TPA. SI needs to engage with the TPA at the requirement formulation stage itself. This is important so that unnecessary re-work is avoided, and the audit is completed in time. The audit needs to be completed before Go-Live of different phases. SI needs to prepare and provide all requisite information/documents to third party auditor and ensure that

there is no delay in overall schedule.

f. The cost of rectification of non-compliances shall be borne by the SI.

14.1.6 Factory Testing

SI shall have to submit Factory Test Certificate for the below mentioned materials before the actual supply of the items.

i. Cable
ii. Pole
iii. Signal Aspects

Authorized representative from RAILTEL / DRDM/ PSCDL will visit the manufacturing plant of the product subject to present in India. Authorized representative will check the testing process.

14.1.7 Final Acceptance Testing

The final acceptance shall cover 100% of the I Project, after successful testing by the RAILTEL / DRDM/ PSCDL, Police Department, other stakeholders/end user department or its PMU; a Final Acceptance Test Certificate (FAT) shall be issued by the RAILTEL/ DRDM/ PSCDL to the SI.

Prerequisite for Carrying out FAT activity:

i. Detailed test plan shall be developed by the SI and approved by RAILTEL / DRDM/ PSCDL. This shall be submitted by SI before FAT activity to be carried out.
ii. All documentation related to ICCC Project and relevant acceptance test document (Including IT Components, Non-IT Components etc.) should be completed & submitted before the final acceptance test to the RAILTEL / DRDM/ PSCDL.
iii. The training requirements as mentioned should be completed before the final acceptance test.
iv. Successful hosting of Application, NMS and MIS Software.
v. For both IT & Non-IT equipment's / software manuals / brochures / Data Sheets / CD / DVD / media for all the Puducherry Project supplied components.

The FAT shall include the following:

I. All hardware and software items must be installed at respective sites as per the specification.
II. Availability of all the defined services shall be verified.
III. The SI shall be required to demonstrate all the features / facilities / functionalities as mentioned in the RFP.
IV. The SI shall arrange the test equipment required for performance verification and will also provide documented test results.
V. The SI shall be responsible for the security audit of the established system to be carried out by a certified third party as agreed by RAILTEL / DRDM/ PSCDL.

Any delay by the SI in the Final Acceptance Testing shall render him liable to the imposition of appropriate Penalties. However, delays identified beyond the control of SI shall be considered appropriately and as per mutual agreement between RAILTEL / DRDM/ PSCDL

and SI. In the event the SI is not able to complete the installation due to non-availability of bandwidth from the bandwidth service providers, the Supplier and RAILTEL / DRDM/ PSCDL may mutually agree to redefine the Network so the SI can complete installation and conduct the Final Acceptance Test within the specified time.

15 Annexure III: Project Milestones and Payment Schedules for Implementation

Project Implementation and Timelines

Payments will be paid to SI on awarding the contract on back-to-back basis on receipt of payments against the invoices submitted by SI.

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

T = Date of signing of Contract Agreement

G= Go-Live Date

The Payment schedule and milestones are divided into two phases:

i. Implementation phase
ii. Operations and maintenance phase

Based on findings of the Feasibility Study done by the SI, the SI may propose a change in the number of sites or individual units to be deployed in each phase as well as overall scope and a consequent change in phasing. PSCDL also retains the right to Suo-moto change the number of sites or individual units to be deployed for each scope item. The final decision on change in phasing and related change in payment schedules shall be at the discretion of PSCDL.

Milestone	Payment Milestones for Implementation	Payment Schedule	Time Schedule	Deliverable
M1	Contract / Work Order	NA	T	NA
M2	Project Kickoff	NA	T + 7 days	NA
M3	Site Survey	NA	T + 1 month	1. Project Implementation Plan. 2. Site Survey report 3. Final BoQ 4. Inception Report
M4	Solution design signoff	NA	T + 45	1. Functional Requirement

			days	Specification document 2. System Requirement Specification document 3. Requirements Traceability Matrix 4. High Level Design documents 5. Low Level Design documents
M5	Supply of IT and Non-IT Infra and systems pertaining to all the Solution components.	70%% of the Capex Cost on pro-rata Basis	T + 3 months	1. Infra and Systems delivery report (delivery challan). 2. Material inspection report signed by the Authority. 3. Tax Invoice 4. Packing list 5. QA/COQ 6. Inspection Certificate 7. Consignee receipt 8. Warranty Certificate of OEM 9. Insurance certificate 10. Certificate duly signed by firm certifying that equipment/materials being delivered are new and conformed to technical specification 11. Undertaking for fall clause
M6	Installation and Commissioning of 1. General Surveillance. 2. ITMS 3. Other Smart solution	15%of the Capex Cost	T + 5 months	Installation and commissioning certificate duly signed by RailTel official, Customer and SI.

	components 4. OFC Connectivity 5. ICCC 6. Any other CAPEX items.			
M8	Completion of Integration of Smart devices and existing applications with ICCC and Go-Live	15% of the Capex Cost	T + 6 months	1. UAT report 2. Training Completion report 3. Go-live certificate.
M9	Operations and maintenance	100% of the Opex cost	5 years from Go-Live	100% of the Opex cost equally spread across quarterly payments from Go-Live .

Note:

i. In cases of fire or any major accidents caused due to the negligence, omissions and commissions of the SI in any of the installations, the liability is on SI for his commissions and omissions in the interim and final ICCC, DC deployments and operations during the O&M phase of sixty months.

ii. It is fixed by a third party auditor on the part of the SI, the claims shall be a minimum of the loss fixed by any third party auditor including the loss of lives, data, equipment, etc. added cumulatively on dues from the SI and will be recovered from the SI.

iii. Single component / multiple components Go-Live shall be awarded on successful completion of the respective component(s) and integration of respective component with ICCC.

iv. In case of partial achievement of the project milestone, the payment shall be made proportionately.

v. SI is required to provide comprehensive O&M of 5 years from the date of Go-Live provided for multiple components / single component outlined in the RFP.

vi. All payments to the Implementation Vendor shall be made upon submission of invoices along with necessary approval certificates from the concerned Authority like PSCDL/DRDM.

Mobilization Advance

The Authority will, if requested by the CONTRACTOR, make mobilization advance payments of 10(%) percent of the Awarded Contract Value to the CONTRACTOR to assist in defraying the initial expenses that will necessarily be incurred by the CONTRACTOR for mobilization and design. The Mobilization Advance will be given to the CONTRACTOR with Simple Interest of 10 % (Percent) per annum.

The Advance payment will be made in two equal instalments of 5% (five percent) of the contract price.

Advance payment will be paid only after CONTRACTOR submitting unconditional and irrevocable Bank guarantee for an amount equivalent to 110 % (one Hundred and Ten percent) of each instalment.

The Authority's Representative shall issue an Interim Payment Certificate for the first instalment.

The Authority will make payment of the First instalment of the mobilization advance only after the CONTRACTOR has fulfilled the following conditions:

a) Execution of the Form of Agreement by the parties hereto and submission of Performance Security by the CONTRACTOR.

b) Mobilized the Project Manager for the Contract.

c) Established and staffed a functional design liaison office at Puducherry city.

After the first instalment of the advance payment has been utilized as per the approved Programme, and to the satisfaction of the Authority's Representative, the CONTRACTOR may then apply for the Second instalment.
The Authority will make payment of the Second installment after the CONTRACTOR has successfully fulfilled the following conditions:
a) Submitted the proposed Implementation Programme for approval by the Authority's Representative.

b) Submitted, for approval by the Authority's Representative, mobilization/ deployment schedules for:
i. CONTRACTOR's key personnel required for managing, executing and supervising the Works,

ii. CONTRACTOR's Plant, Machinery and Equipment required for executing the Works; and

iii. Procurement Schedule for materials to be incorporated into the Permanent Works.
c) Submitted a Cash Flow Forecast for approval by the Authority's Representative.

d) Submitted a list of proposed, suppliers and manufacturers, along with their credentials, for approval by the Authority's Representative.

e) Submitted details of funds mobilized by himself as per the Cash Flow Forecasts.

f) Actual deployment of: (i) such Personnel, (ii) Machinery and Equipment,

g) Established the fully furnished Site office.

h) Placed confirmed orders for supply of major items of material which is to be incorporated into the Permanent Works as per the approved procurement schedule.

i) Commenced construction work at the Site in accordance with the approved construction program.

Deduction of Mobilization Advance: Mobilization advance shall be deducted starting from Second Interim Payment certificate @ of 10 % (Percent) of the certified amount of Interim payment certificate and to be recovered fully prior to the time when 90 percent (90%) of the work is completed.
A bank Guarantee of 110 (%) percent against the Mobilization advance is to be submitted. The mobilization advances and interest on it shall be adjusted and recovered in the Interim Payment Certificates raised by the Contractor for the work completed as mentioned above. The bank Guarantee submitted against mobilization advance has to be valid till completion of the work. In case, the Contractor fails to mobilize necessary manpower, machinery, materials and any necessary procurement or purchase to start the preliminary work, the bank guarantee against mobilization advance may be forfeited and will lead to the termination of contract.

15.1 Quality Assurance

A thorough quality check is proposed for the Puducherry Project and its modules, as per standard Software Development Life Cycle (SDLC). SI is expected to lay down a robust Quality Assurance program for testing of the developed application for its functionality, performance and security before putting in production environment. The program must include an overall plan for testing and acceptance of system, in which specific methods and steps should be clearly indicated and approved by RAILTEL & PSCDL. SI is required to incorporate all suggestions / feedback provided after the elaborate testing of the system, within a predefined, mutually agreed timeline. SI must undertake the following:

i. Outline the methodology that will be used for testing the system.
ii. Define the various levels or types of testing that will be performed for system.
iii. Provide necessary checklist/documentation that will be required for testing the system.
iv. Describe any technique that will be used for testing the system.
v. Describe how the testing methodology will conform to the requirements of each of the functionalities and expected outcome.
vi. Indicate / demonstrate to RAILTEL & PSCDL that all applications installed in the system have been tested.

16 Annexure V : Guidelines

Common guidelines regarding compliance of the system / equipment:

i. The functional requirements and technical specifications provided in the below sections and at other sections in this RFP are indicative and carry guiding rule. The SI is free to offer products and solutions which meet requirements of the RFP focusing on the outcome, future scalability, security, reliability and adherence to specified SLA under this RFP, in line with applicable standards & best practices adopted in the industry. The SI is encouraged to design an Optimised solution which is technically superior, innovative, proven, better in terms of functionality and is cost effective. Any specified parameters mentioned in the scope/technical requirement in the RFP may be considered if it is required for meeting current & future requirements during the contract period. The SI is fully responsible for the specified outcome to be achieved.
ii. The specifications mentioned for various IT / Non-IT components are indicative requirements and should be treated for benchmarking purpose only. SIs are required to undertake their own requirement analysis and may propose higher specifications that are better suited to the requirements.
iii. In case of addition/update in number of license for the Integrated Command and Control Centre (ICCC) software and VMS licenses for Cameras, the SI is required to meet of technical specifications contained in the RFP and for the upward revisions and/or additions of licenses is required be made as part of change order and cost would be commensurate to the itemized rate approved at the LOI issuance.

iv. Any manufacturer and product name mentioned in the Tender should not be treated as a recommendation of the manufacturer / product.

v. None of the IT / Non-IT equipment's proposed by the SI should be End of Life product. It is essential that the technical proposal is accompanied by the OEM certificate in the format given in Volume I of this Tender, where-in the OEM will certify that the product is not end of life product & shall support for at least 6 years from the date of Bid Submission.

vi. All IT Components should support IPv4 and IPv6

vii. Technical Bid should be accompanied by OEM's product brochure / datasheet. SIs should provide complete make, model, part numbers and sub-part numbers for all equipment/software quoted, in the Technical Bid.

viii. SI should ensure that only one make and model is proposed for one component in Technical Bid for example all Traffic Surveillance cameras must belong to a single OEM and must be of the same model etc.

ix. SIs should ensure complete warranty and support for all equipment from OEMs. All the back-to back service agreements should be submitted during the contract whereas MAF for all the equipment from OEMs shall be shared along with the Technical Bid as per Format given in the RFP.

x. All equipment, parts should be original and new.

xi. The user interface of the system should be a user friendly Graphical User Interface (GUI).

xii. Critical core components of the system should not have any requirements to have proprietary platforms and should conform to open standards.

xiii. For 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. Before hosting the application, it shall be subjected to application security audit (by any of the CERTIN empanelled vendors) to ensure that the application is free from any vulnerability; and approved by the Police Department.

xiv. All the Clients Machines / Servers shall support static assigned IP addresses or shall obtain IP addresses from a DNS/DHCP server.

xv. The Successful SI should also propose the specifications of any additional servers / other hardware, if required for the system.

xvi. The indicative architecture of the system is given in this volume. The Successful SI must provide the architecture of the solution it is proposing.

xvii. The system servers and software applications will be hosted in Data Centers as specified in the Bid. It is important that the entire set of Data Center equipment are in safe custody and have access from only the authorized personnel and should be in line with the requirements & SLAs defined in the Tender.

xviii. The Servers provided should meet industry standard performance parameters (such as CPU Utilisation of 60 percent or less, disk utilisation of 75 percent or less). In case any non-standard computing environment is proposed (such as cloud), detail clarification needs to be provided in form of supporting documents, to confirm (a) how the sizing has been arrived at and (b) how SLAs would be met.

xix. SI is required to ensure that there is no choking point / bottleneck anywhere in the system (end-toend) and enforce performance and adherence to SLAs. SLA reports must be submitted as specified in the Bid without fail.

xx. All the hardware and software supplied should be from the reputed Original Equipment Manufacturers (OEMs). Department reserves the right to ask replacement of any hardware / software if it is not from a reputed brand and conforms to all the requirements specified in the tender documents.

xxi. Cameras, Network Video Recorder (NVR) and the Video Management / Video Analytics Software should be ONVIF Core Specification '2.X' or 'S' compliant and provide support for ONVIF profiles such as Streaming, Storage, Recording, Playback, and Access Control.

xxii. SI shall place orders on various OEMs directly and not through any sub-contractor / partner. All licenses should be in the name of the RAILTEL & PSCDL

xxiii. Technical Solution and Architecture : All the components of the Technical Architecture which should comply with the published eGovernance standards, frameworks, policies and guidelines available on http://egovstandards.gov.in and leading industry standards.

xxiv. Consider architecture design with respect to scalability, inter-operability , availability, manageability and comply with framework Smart City (K-15016/61/2016-SC-1, Government of India, and Ministry of Urban Development)

17 Annexure VI Security – General Guidelines

17.1 Security Framework

The Bidder shall develop Security Framework aimed at building a secure and resilient security space for citizens and stakeholders of Smart City. The Framework shall be designed to protect information and infrastructure; build capabilities to prevent and respond to attacks; and minimize damages through coordinated efforts of institutional structures, people, processes, and technology. Framework shall cover security architecture.

17.2 Security Policy

The policy shall address security of hardware and software, along with the connectivity between the field device and the respective application software. The bidder shall ensure to develop and implement Standard Operating Procedures for smooth Operations and Maintenance of IT infrastructure.

17.3 Security Governance

1. The Bidder shall conduct Risk Assessment and prepare Risk Treatment Plan for the IT applications and infrastructure deployed in smart city ecosystem.
2. The Bidder shall facilitate management reporting in form of dashboard covering Risk Assessment results along with risk treatment plan and timeline to the smart city management.
3. The Bidder shall implement all the controls as identified during the Risk assessment and treatment plan as per the agreed

17.4 Smart City IT Asset Management

1. The Bidder shall utilize automated asset management tools to prepare the information asset register (IAR) for all IT assets deployed in the Smart city. The IAR shall capture criticality, rating, classification, owner and custodian of the Asset.
2. The Bidder shall develop and implement an appropriate set of procedures for information labelling and handling in accordance with the classification scheme proposed in the security policy of smart city.

17.5 Physical & Environmental Security

4. The bidder shall implement and manage physical security of IT assets of smart city, which shall include, as a minimum: locks, alarms, surveillance equipment, sensors, access control systems (biometrics), etc. The bidder shall also design processes and procedures for same.
5. The Bidder shall ensure that all the equipment, information or software shall not be taken off-site without appropriate authorization.

17.6 Access Control

1. The Bidder shall ensure that users shall be provided single sign on functionality if required for the applications and solutions deployed in Smart City.
2. The smart city solution should support multiple authentication methods such as Username password, two factor authentication, digital certificate and biometric based authentication.
3. The solution should be capable of being deployed on mobile devices deployed for smart city
4. Solution should have the capability to define access based on time of day, day of week or by group or user defined access.
5. The smart city solution should have the functionality to provide authentication based on the role.
6. Remote access to all smart city IT users shall be securely managed.
7. The smart city solution should be able to deploy and configure the approved password policy and should provide the feature to configure the logs.

8. The smart city solution should have the option of blocking multiple sessions for the user.
9. All smart city applications should support role based access control to enforce separation of duties.
10. The application deployed in smart city should display the last login status (successful/unsuccessful, time) to the user and should not store authentication credentials on client computers after a session terminates
11. All smart city solution should be compliant with Indian IT Act, 2000 and Amended IT Act, 2008

17.7 Communications and Operations Management

1. Bidders must ensure that the IT systems in the smart city infrastructure are open, scalable and interoperable. The deployed systems must operate within 4 layers – Sensory layer, communication layer, data layer and application layer adhering to relevant security controls as mandated by the MoUD guidelines.
2. Bidders shall ensure that all the interfaces between IoT devices, field sensors, device applications and storage deployed in smart city are encrypted using appropriate protocols, algorithm and key pairs.
3. All transport link communication must be encrypted and sensitive data both in rest and transit is to be secured using encryption.
4. Bidders must ensure that all the changes made to the smart city infrastructure incl. of IoT field devices, sensors and related applications should be tracked and recorded in order to enable security monitoring of the infrastructure. The maintained logs should be systematically collated, enabling the access of critical information as per date, fortnight, month, quarter, year etc.
5. Bidders should ensure that separate environments are maintained for production, test and development for smart city infrastructure and solutions to reduce the risks of unauthorized access or changes.
6. Bidders must ensure that smart city IT systems are designed in such a way that only authenticated users have access to the smart city database. Also, the provision of access has to be routed only through designated applications.
7. Bidders must ensure that sensitive data is stored in the smart city database in an encrypted format thereby curtailing the database administrator from reading or modifying the stored sensitive data.
8. Bidders must ensure that the smart city architecture should include a VPN solution enabling designated users to access necessary applications and functions from remote applications.
9. Bidders must enable for the maintenance of an audit trail to record all the administrator, user level activities including the failed attempts thereby enabling a robust high level security monitoring of the smart city security infrastructure.
10. Bidders must ensure that the smart city components – Network elements, Operating system, Applications etc. are in sync and adhere to a singular master clock. Thereby ensuring an appropriate logging/ time stamping of incidents and bolstering smooth operation of the smart city.

11. Bidders must ensure that adequate security controls are deployed against the tampering of log information and unauthorized access to the smart city infrastructure such as the data center, IoT device control room etc.
12. Bidders must ensure that platforms hosted in the central data center support multi-tenancy with adequate authentication and role based access. This can be achieved by utilizing Authentication and privilege management technology thereby controlling the access of data as per user privileges.
13. Bidders must ensure that the smart city architecture accounts for latency issues for the flow of data between devices. Suitable protocols should be utilized to minimize data flow latency upon management of heterogeneous data.
14. Bidders must strictly make sure that the communication between IoT field devices and their respective management applications happens only over a data layer (digital platform). Thereby enabling this designated layer to be the one true source of data abstraction, normalization and correlation.
15. Bidders must ensure that the smart city IT infrastructure including the Wi-Fi network adheres to relevant and applicable security standards and protocols. Also, bidders must make sure that the Application Program Interfaces (APIs) are published and the IT systems run on standard protocols.
16. Bidders must ensure that the smart city architecture end-to-end has adequate security controls to enforce safety, privacy and integrity of confidential data. Necessary controls must be deployed to protect the integrity of data flowing into the control systems and other critical infrastructure.
17. Bidders must enable for wireless/ broadband architecture used in the smart city infrastructure to interface with other/citywide wireless networks thereby enabling interoperability.
18. Bidders must ensure that IoT field devices and sensory equipment operating within the smart city periphery connect only to authorize wireless networks. Secure Wi-Fi guidelines as prescribed by the Department of Telecom must be followed.
19. Bidders must make sure that the wireless layer of the smart city network is appropriately segmented, bifurcating the network into various trusted zones. Thereby segregating public and utility networks via VPN (Virtual private networks), ensuring that the traffic from internet users is not routed into sensor networks and vice versa.
20. Bidders must enable for the authentication of the sensory equipment during the provisioning of the sensors and connection into the smart city infrastructure.
21. Bidders must ensure that the data aggregators used for enabling the interoperability between field IoT devices and sensors functioning on different protocols incorporate appropriate authentication and encryption at the aggregator gateway when field devices are not capable of authenticating /encrypting critical information.
22. Bidders must ensure that the IoT field devices and sensory equipment deployed in smart city periphery must not have a physical interface for administration. System and Network monitoring should be only performed remotely thereby ensuring local cyber-attacks/ tampering of field devices is curtailed.

23. Bidders must ensure appropriate network segregation. The smart city data center must be systematically segmented into multiple zones. Each zone must have a dedicated functionality. IoT field devices and sensory equipment must be connected to a completely separate network isolated from public networks and other private networks.
24. Bidders must make sure that the internet facing segment of the data center must incorporate a DMZ (Demilitarized zone), where customer application servers would be located. Predefined ports must be assigned for enabling the communication between the customer application servers and utility application servers to facilitate the access/transfer of data.
25. Bidders must ensure that Smart city data centers are well equipped with adequate security controls to protect the confidentiality, integrity and accessibility of critical data. The center should consider including cyber security systems such as firewalls, Intrusion detection & Intrusion prevention systems, Web Application Firewalls, Behavioral analysis systems for anomaly detection, Correlation engine, Denial of Service prevention device, Advanced Persistent Threat notification mechanism, Federated identity, access management system etc.
26. Bidders must ensure that the proposed smart city architecture provides for:
    i Automatic and secure firmware updates
    ii Device logging and auditing capabilities
    iii Vendor self-certification for non-existence of backdoors, undocumented and hard coded accounts.
    iv Bidders shall ensure that Data encryption at rest shall be implemented using departments managed keys, which are not stored in the cloud.

17.8 Information Systems Acquisition, Development and Maintenance

1. The Bidder shall prepare the detailed technical security requirement as part of the 'Software Requirement Specification' document with secure coding guidelines for development of applications for smart city.
2. The Bidder shall incorporate validation checks into smart city applications to detect any corruption of information through processing errors or deliberate acts.
3. The Bidder shall obtain information about technical vulnerabilities of information systems being used in smart city, evaluate the exposure to such vulnerabilities, and take appropriate measures to address the associated risk.
4. The bidder shall implement maintenance and repair process of smart city IT assets in timely manner, with approved and controlled tools.

17.9 Business Continuity Planning and Disaster Recovery

1. The Bidder shall implement and operate Disaster Recovery site for the Smart city infrastructure and related IT & OT applications. IT & OT applications and processes should be supported from the disaster recovery site.

2. The Bidder shall define Business Continuity and Disaster Recovery plan and will perform the testing on a yearly basis

17.10 nformation Security Audits

The bidder shall ensure Information security audits of the smart city infrastructure and related applications by a CERT-In empaneled vendor. VA/PT (Vulnerability assessment and Penetration Testing) activities, audits and application security testing must be carried out on once-a-year basis ensuring optimal operation and security of the smart city infrastructure and applications. Teams carrying out the audit exercise must be different from the implementation teams. Systematic actionable need to be derived post audits and necessary changes need to be made periodically.

17.11 Awareness Training

The bidder shall deploy appropriate resources to support periodic awareness training based on latest standards of ISMS in consultation with the Authorities. The trainings must focus on educating relevant employees (including privileged users, third party, senior management etc.) on necessary security practices and processes to be followed in order to maintain the Confidentiality, Integrity and Availability of critical data.

17.12 Security Controls for Cloud Services

The security controls for creating and managing cloud services shall comply with the following guidelines. Empanelment of Cloud Service Offerings CSPs facilities/services shall be compliant with regulative directives and industry best practices. The SLA shall be based on the guidelines issued by Government Departments on contractual terms related to Cloud Services (MeitY guideline dated 31/03/17). The security controls should include the following:

1) The CSP should be empaneled by MeitY for providing cloud services. The CSPs facilities/services shall be certified to be compliant to the following standards: ISO 27001, ISO 27017, ISO 27018, ISO 20000-9, ISO/IEC 20000-1 & PCI DSS.
2) The CSP/Service Provider shall comply or meet any security requirements applicable to CSPs/Service Providers published (or to be published) by MeitY or any standards body setup / recognized by Government of India from time to time and notified to the CSP/Service Providers by MeitY as a mandatory standard.
3) The CSP/Service Provider shall meet all the security requirements indicated in the IT Act 2000, the terms and conditions of the Provisional Empanelment of the Cloud Service Providers and shall comply with the audit criteria defined by STQC.
4) Incident Management shall be managed by CSP / third party.
5) Periodic secure code review shall be performed for cloud applications.

6) Data encryption at rest / transit depending on sensitivity of data shall be implemented using departments managed keys, which are not stored on the cloud.
7) The CSP will undertake to treat information passed on to them as classified. Such Information will not be communicated / published / advertised by the CSP to any person/organization without the express permission of the Department.
8) CSP shall inform all security breach incidents to Smart City management on real time.
9) CSP shall ensure data confidentiality and mention Sub-contractual risk shall be covered by CSP.
10) E-Discovery shall be included as clause in SLA with CSP. It is the process of locating, preserving, collecting, processing, reviewing, and producing Electronically Stored Information (ESI) in the context of or criminal cases/proceedings or investigation. Logging and reporting (e.g., audit trails of all access and the ability to report on key requirements/indicators) must be ensured.
11) The Law Enforcement Agency as mandated under any law for the time being in force may seek access to information stored on cloud as provided by the Service Provider. The onus shall be on the CSP to perform all due diligence before releasing any such information to any such law enforcement agency.
12) CSP must ensure location of all data related to smart cities in India only.
13) The Cloud Service Provider's services offerings shall comply with the audit requirements defined under the terms and conditions of the Provisional Empanelment of the Cloud Service Providers (or STQC /MEITY guidelines. The Audit, Access and Reporting Requirements should be as per the terms and conditions of the Provisional Empanelment of the Cloud Service.
14) CSP's exit Management Plan shall include - Transition of Managed Services & Migration from the incumbent cloud service provider's environment to the new environment and shall follow all security clauses for smooth transition.
15) SLA with CSP shall cover performance management & dispute resolution escalation. Guidelines on Service Level Agreement issued by MeitY lists out the critical SLAs for cloud services.
16) Identification and problem resolution (e.g., helpline, call center, or ticketing system) mechanism must be defined.
17) Change-management process (e.g., changes such as updates or new services) must be defined.
18) Appropriate segregation of Virtual Private Cloud (VPC) security rules defined as part of firewall to restrict access, Role based access management, Logging and monitoring shall be ensured.
19) VPN gateway must be setup to ensure controlled access, appropriate security rules must be employed to encrypt outward data flow, IDS, IPS, API Gateways to be setup and ELB logs to be maintained for any activities and access and exceptions to carried out in the cloud setup, Database logs to be routed as part of the Logging VPC setup.
20) Digital Certificate shall be implemented for secure access.

21) Web Application Firewall must be provided, Host IPS must be setup on all the Web servers, Web servers must be configured as per the CIS hardening guidelines and baseline security requirements, logging and monitoring should be enabled.
22) Application access between hosted smart city applications shall be segregated, internal infrastructure and external traffic, Role based access must be defined, hardening of database instances as per the CIS baselines configuration guidelines in the cloud setup must be ensured, Logging and monitoring must be enabled.
23) For SLAs to be used to steer the behavior of a cloud services provider, imposition of financial penalties is to be incorporated.
24) Monitor Vendor Service level agreement for annual end-to-end service availability of 99.999 percent. The end to end service agreement should be in place for minimum period of six years form the date of operations of the systems.

18 Annexure VI – Smart City Guidelines

Universal Access IT Systems to empower differently-abled citizens to access ICT systems with ease

Sl.	Parameters No.	Minimum Requirements
1	Text Alternatives	Provide text alternatives for any non-text content so that it can be changed into other forms people need, such as large print, braille, speech, symbols or simpler language.
2	Non-text Content	All images, form image buttons, and image map hot spots have appropriate, equivalent alternative text. Images that do not convey content, are decorative, or contain content that is already conveyed in text are given null alt text (alt="") or implemented as CSS backgrounds. All linked images have descriptive alternative text. Equivalent alternatives to complex images are provided in context or on a separate (linked and/or referenced via longdesc) page.
3	Time-based Media	Provide alternatives for time-based media.
4	Audio Description or Media Alternative (Prerecorded)	A descriptive text transcript OR audio description audio track is provided for non-live, web-based video
5	Adaptable	Create content that can be presented in different ways (for example simpler layout) without losing information or structure.

6	Info and Relationships	Semantic markup is used to designate headings (<h1>), lists (, , and <dl>), emphasized or special text (, <code>, <abbr>, <blockquote>, for example), etc. Semantic markup is used appropriately. Tables are used for tabular data. Where necessary, data cells are associated with their headers. Data table captions and summaries are used where appropriate. Text labels are associated with form input elements. Related form elements are grouped with fieldset/legend.
7	Meaningful Sequence	The reading and navigation order (determined by code order) is logical and intuitive.
8	Use of Color	Color is not used as the sole method of conveying content or distinguishing visual elements. Color alone is not used to distinguish links from surrounding text unless the luminance contrast between the link and the surrounding text is at least 3:1 and an additional differentiation (e.g., it becomes underlined) is provided when the link is hovered over or receives focus.
9	Audio Control	A mechanism is provided to stop, pause, mute, or adjust volume for audio that automatically plays on a page for more than 3 seconds.
10	Resize text	The page is readable and functional when the text size is doubled.
11	Images of Text	If the same visual presentation can be made using text alone, an image is not used to present that text.
12	Keyboard Accessible	Make all functionality available from a keyboard.
13	Keyboard	All page functionality is available using the keyboard, unless the functionality cannot be accomplished in any known way using a keyboard (e.g., free hand drawing). Page-specified shortcut keys and accesskeys (accesskey should typically be avoided) do not conflict with existing browser and screen reader shortcuts.
14	No Keyboard Trap	Keyboard focus is never locked or trapped at one particular page element. The user can navigate to and from all navigable page elements using only a keyboard.

15	Pause, Stop, Hide	Automatically moving, blinking, or scrolling content that lasts longer than 5 seconds can be paused, stopped, or hidden by the user. Moving, blinking, or scrolling can be used to draw attention to or highlight content as long as it lasts less than 5 seconds. Automatically updating content (e.g., automatically redirecting or refreshing a page, a news ticker, AJAX updated field, a notification alert, etc.) can be paused, stopped, or hidden by the user or the user can manually control the timing of the updates.
16	Seizures	Do not design content in a way that is known to cause seizures.
17	Three Flashes or Below Threshold	No page content flashes more than 3 times per second.
18	Navigable	Provide ways to help users navigate, find content, and determine where they are
19	Bypass Blocks	A link is provided to skip navigation and other page elements that are repeated across web pages. If a page has a proper heading structure, this may be considered a sufficient technique instead of a "Skip to main content" link. Note that navigating by headings is not yet supported in all browsers. If a page uses frames and the frames are appropriately titled, this is a sufficient technique for bypassing individual frames.
20	Page Titled	The web page has a descriptive and informative page title.
21	Focus Order	The navigation order of links, form elements, etc. is logical and intuitive.
22	Headings and Labels	Page headings and labels for form and interactive controls are informative. Avoid duplicating heading (e.g., "More Details") or label text (e.g., "First Name") unless the structure provides adequate differentiation between them.
23	Focus Visible	It is visually apparent which page element has the current keyboard focus (i.e., as you tab through the page, you can see where you are).
24	Readable	Make text content readable and understandable
25	Language of Page	The language of the page is identified using the HTML lang attribute
26	Language of Parts	The language of page content that is in a different language is identified using the lang attribute.
27	Predictable	Make Web pages appear and operate in predictable ways.
28	On Input	When a user inputs information or interacts with a control, it does not result in a substantial change to the page, the spawning of a pop-up window, an

		additional change of keyboard focus, or any other change that could confuse or disorient the user unless the user is informed of the change ahead of time.
29	Compatible	Maximize compatibility with current and future user agents, including assistive technologies.
30	Parsing	Significant HTML/XHTML validation/parsing errors are avoided. In content implemented using markup languages, elements have complete start and end tags, elements are nested according to their specifications, elements do not contain duplicate attributes, and any IDs are unique, except where the specifications allow these features.
31	Name, Role, Value	Markup is used in a way that facilitates accessibility. This includes following the HTML/XHTML specifications and using forms, form labels, frame titles, etc. appropriately. For all user interface components, the name and role can be programmatically determined; states, properties, and values that can be set by the user can be programmatically set; and notification of changes to these items is available to user agents, including assistive technologies.
32	Audio-only and Videoonly (Pre-recorded)	A descriptive text transcript (including all relevant visual and auditory clues and indicators) is provided for non-live, web-based audio (audio podcasts, MP3 files, etc.) A text or audio description is provided for non-live, web-based video-only (e.g., video that has no audio track).
33	Captions (Prerecorded)	Synchronized captions are provided for non-live, web-based video (YouTube videos, etc.)
34	Captions (Live)	Synchronized captions are provided for all live multimedia that contains audio (audio-only broadcasts, web casts, video conferences, Flash animations, etc.)
35	Audio Description (Prerecorded)	Audio descriptions are provided for all video content NOTE: Only required if the video conveys content visually that is not available in the default audio track.
36	Sensory Characteristics	Instructions do not rely upon shape, size, or visual location (e.g., "Click the square icon to continue" or "Instructions are in the right-hand column"). Instructions do not rely upon sound (e.g., "A beeping sound indicates you may continue.").
37	Distinguishable	Make it easier for users to see and hear content including separating foreground from background.
38	Contrast (Minimum)	Text and images of text have a contrast ratio of at least 4.5:1. Large text - at least 18 point (typically 24px) or 14 point (typically 18.66px) bold has a contrast ratio of at least 3:1.
39	Enough Time	Provide users enough time to read and use content.

40	Timing Adjustable	If a page or application has a time limit, the user is given options to turn off, adjust, or extend that time limit. This is not a requirement for real-time events (e.g., an auction), where the time limit is absolutely required, or if the time limit is longer than 20 hours.
41	Link Purpose (In Context)	The purpose of each link (or form image button or image map hotspot) can be determined from the link text alone, or from the link text and its context (e.g., surrounding paragraph, list item, table cell, or table headers). Links (or form image buttons) with the same text that go to different locations are readily distinguishable.
42	Multiple Ways	Multiple ways are available to find other web pages on the site - at least two of: a list of related pages, table of contents, site map, site search, or list of all available web pages.
43	On Focus	When a page element receives focus, it does not result in a substantial change to the page, the spawning of a pop-up window, an additional change of keyboard focus, or any other change that could confuse or disorient the user.
44	Consistent Navigation	Navigation links that are repeated on web pages do not change order when navigating through the site.
45	Consistent Identification	Elements that have the same functionality across multiple web pages are consistently identified. For example, a search box at the top of the site should always be labeled the same way.
46	Input Assistance	Help users avoid and correct mistakes.
47	Error Identification	Required form elements or form elements that require a specific format, value, or length provide this information within the element's label. If utilized, form validation errors are presented in an efficient, intuitive, and accessible manner. The error is clearly identified, quick access to the problematic element is provided, and user is allowed to easily fix the error and resubmit the form.
48	Labels or Instructions	Sufficient labels, cues, and instructions for required interactive elements are provided via instructions, examples, properly positioned form labels, and/or fieldsets/legends.
49	Error Suggestion	If an input error is detected (via client-side or server-side validation), provide suggestions for fixing the input in a timely and accessible manner.
50	Error Prevention (Legal, Financial, Data)	If the user can change or delete legal, financial, or test data, the changes/deletions can be reversed, verified, or confirmed.
51	Visual Captcha	Alternative mode of authentication should be offered to in order to be authenticated

52	Mandatory use of Unicode for regional language	Unicode facilitates assistive technology to access content.