



Request for Proposal

For

Selection of Master System Integrator (MSI) for Implementation,
Operation & Maintenance of Surveillance System under

Safe City Project of Delhi Police



RFP No.: CDACP/Safe City/MSI/2020/313,
Dated: 18 December 2020



Centre for Development of Advanced Computing

A Scientific Society of Ministry of Electronics & Information Technology, Government of India
Innovation Park, Panchavati, Pashan Road, PUNE- 411008.

Tel: +91-20-25503673

delhisafecitybid@cdac.in



This Page is Left Bank Intentionally



Disclaimer

The information contained in this Request for Proposal document ("RFP") or subsequently provided to Bidders/prospective MSI, whether verbally or in documentary or any other form by or on behalf of C-DAC or any of its Directors, employees or advisers, is provided to Bidders/prospective MSI on the terms and conditions set out in this RFP and such other terms and conditions subject to which such information is provided.

This RFP is neither an offer nor agreement by C-DAC to the Bidders/prospective MSI or any other person. The purpose of this RFP is to provide interested parties with information that may be useful to them in the preparation of their Proposals (Bids) pursuant to this RFP. This RFP includes statements, which reflect various assumptions and assessments arrived at by C-DAC. Such assumptions, assessments and statements do not purport to contain all the information that each Bidder/prospective MSI may require. This RFP may not be appropriate for all persons, and it is not possible for C-DAC, its Directors, employees or advisers to consider the objectives, technical expertise and needs of each party who reads or uses this RFP. The assumptions, assessments, statements and information contained in this RFP, may not be complete, accurate, adequate or correct. Each Bidder/prospective MSI should, therefore, conduct own investigations and analysis and should check the accuracy, adequacy, correctness, reliability and completeness of the assumptions, assessments and information contained in this RFP and obtain independent advice from appropriate sources at their own cost.

The information given is not an exhaustive account of statutory requirements and should not be regarded as a complete or authoritative statement of requirements. C-DAC accepts no responsibility for the accuracy or otherwise for any interpretation or opinion on the facts, requirements and legal provisions expressed herein.

C-DAC, its Directors, employees and advisers make no representation or warranty and shall have no liability to any person including any Bidder/prospective MSI under any law, statute, rules or regulations or tort, principles of equity or unjust enrichment or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this RFP or otherwise, including the accuracy, adequacy, correctness, reliability or completeness of the RFP and any assessment, assumption, statement or information contained therein or deemed to form part of this RFP or arising in any way in this Selection Process.

C-DAC shall not be liable for any loss, damage, costs etc. of any nature whether resulting from negligence or otherwise, howsoever caused, arising from reliance of any Bidder/prospective MSI upon the statements contained in this RFP.

C-DAC may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information, assessment or assumption contained in this RFP.

Issuance of this RFP does not imply that C-DAC is bound to select a MSI or to appoint the selected MSI. C-DAC reserves the right to reject all or any of the Proposals (Bids) without assigning any reasons whatsoever.



Bidder/prospective MSI shall bear all the costs associated with or relating to preparation and submission of proposal including but not limited to preparation, copying, postage, delivery fees, expenses associated with any demonstrations or presentations which may be required by C-DAC or any other costs incurred in connection with or relating to its Proposal. All such costs and expenses shall remain with the Bidder/prospective MSI and C-DAC shall not be liable in any manner whatsoever for the same or for any other costs or expenses incurred by Bidder/prospective MSI in preparation or submission of the Proposal, presentation/demonstration/proof of Concept etc. regardless of the conduct or outcome of the selection process.

---0--0--0---



Table of Contents

Chapter 1. : Instructions For Bidders (IFB)	11
1.1. Required Assistance to Bidders.....	11
1.2. On-Line Bid Submission.....	11
1.2.1. Registration on e-procurement Portal	11
1.2.2. Preparation of Bids & adequate attention to NIT, corrigendum, uploading formats, others	11
1.2.3. Successful Submission of bids.....	12
1.3. Fact Sheet & Calendar of Events	12
1.4. Acronyms- list of abbreviations.....	14
1.5. Purpose.....	20
1.6. Definitions	20
1.6.1. Interpretation.....	22
1.7. Introduction to the Project- Delhi Safe City	23
1.7.1. Safe City Need in the National Capital Territory, Delhi.....	23
1.7.2. Important Stakeholders for important guidance and contributions.....	23
1.7.3. Delhi Police Functioning Structure and administration	24
1.7.4. Governance Structure for Safe City Project of Delhi Police.....	24
1.8. General	24
1.9. Eligible Bidders.....	25
1.9.1. Compliant Bids/Completeness of Response	25
1.9.2. Bidder to Inform (clarification)	25
1.9.3. Bid Preparation Costs	26
1.9.4. Pre-Bid Meeting & Clarification	26
1.9.5. Responses to Pre-Bid Queries and Issue of Corrigendum	26
1.9.6. RFP Document Fee.....	27
1.9.7. Contents of Bid	27
1.9.8. Validity of Bids.....	30
1.9.9. Language of Bids	30
1.9.10. Authentication of Bids.....	30
1.9.11. Amendment of Request for Proposal.....	31
1.9.12. Bid Price	31
1.9.13. Deviations and Exclusions	31
1.9.14. Total Responsibility.....	31
1.9.15. Late Bids.....	32
1.9.16. Right to Terminate the Process.....	32



1.9.17. Non-Conforming bids.....	32
1.9.18. Acceptance/ Rejection of Bids	32
1.9.19. Confidentiality	33
1.9.20. Bid Disqualification.....	33
1.9.21. Fraud and Corrupt Practices	33
1.9.22. Conflict of Interest.....	34
1.9.23. Sub-Contracting.....	35
1.9.24. Right to vary quantity	35
1.9.25. Withdrawal, Substitution, and Modification of Bids.....	35
1.9.26. Site Visit for preparation of the bid	35
Chapter 2. Conditions of Contract.....	37
2.1. Special Conditions of Contract (SCC).....	37
2.1.1. Signing of Agreement and Release of Payments	37
2.1.2. Bid Security/ Earnest Money Deposit (EMD)	37
2.1.3. Pre-Qualification / Eligibility Criteria	37
2.1.4. Exemptions	41
2.1.5. Opening of Bids	41
2.1.6. Clarification on Bids	41
2.1.7. Tender Evaluation Committee (TEC).....	41
2.1.8. Evaluation Process	42
2.1.9. PoC Evaluation Guidelines	46
2.1.9.1. Approach to be undertaken for the Demonstration of Proof of Concept (PoC)	47
2.1.9.2. Field Components Setup.....	47
2.1.9.3. Network Setup	47
2.1.9.4. Software and Server Setup	48
2.1.9.5. Team setup for PoC by bidder.....	48
2.1.9.6. Flow for the PoC	49
2.1.9.7. PoC Setup Document	49
2.1.9.8. PoC setup Requirement	50
2.1.10. PoC Demonstration – salient points	50
2.1.10.1. PoC Scope and Technical Evaluation Parameters.....	53
2.1.11. Award of Contract /Order.....	85
2.1.12. Notification of Award.....	85
2.1.13. Locations for Delivery and Project Implementation	85
2.1.14. Prices	85



2.1.15. Performance Security	86
2.1.16. Timelines linked with Payment Schedule	87
2.1.17. Warranty	94
2.1.18. Operations and Maintenance	95
2.1.19. Liquidated Damages	104
2.1.20. Penalties for Non/Under Performance	104
2.1.21. Termination	105
2.1.22. Consequence of Termination	105
2.1.23. Limitation of Liability:	106
2.1.24. Indemnity	107
2.1.25. Security and Safety	107
2.1.27. Confidentiality	107
2.1.28. Events of Default by MSI	108
2.1.29. Severability and renegotiation	109
2.1.30. Non-Waiver:	109
2.1.31. Fall Clause:	109
2.1.32. Jurisdiction	109
2.2. General Conditions of Contract (GCC)	109
2.2.1. Term and Extension of the Contract	109
2.2.2. Dispute Resolution	111
2.2.3. Time is of the essence	111
2.2.4. Conflict of interest	111
2.2.5. Publicity	112
2.2.6. Insurance	112
2.2.7. Project Audits and Testing	112
2.2.8. Final Acceptance at Site Test Procedure (FAT Procedure):	114
2.2.9. Transfer of Ownership	115
2.2.10. Exit Management Plan	115
2.2.11. Intellectual Property Rights	116
2.2.12. Failure to agree with the Terms & Conditions of the RFP	117
Chapter 3. Schedule of Requirements	118
3.1. SoR Format	118
3.1.1. Hardware and Software and Networking Components	118
3.1.2. Civil Works and interiors of C4i	139
3.1.3. Civil Works and interiors of C3i	154



3.1.4. Civil Works and interiors of C2i.....	158
3.1.5. Civil Works and interiors of Data Centre	163
Chapter 4. : Specifications and allied Technical Details.....	186
4.1. Executive Summary	186
4.1.1. At a Glance- summarized scope for implementation.....	186
4.2. Aim, Objectives and Benefits of Delhi Safe City to be realized through MSI	186
4.2.1. Aim	186
4.2.2. Objective	187
4.2.3. Intended Benefits	189
4.3. Delhi Safe City- Targeted Impact & Outcome on Delhi Police and Citizens through successful Project Implementation by MSI.....	190
4.4. Key components- Project Requirement & understanding for MSI.....	191
4.5. Implementation Approach- Essential & Planned approach by MSI.....	195
4.6. Physical Layouts of Civil Infrastructure Areas with essential components as envisaged	206
4.7. System Functional Requirements and Key Performance Indicators.....	211
4.8. Component-wise Functional Requirements (with KPIs) and Technical Requirements.....	215
4.14 CHANGE Management- Training, Capacity Building.....	582
4.15 DC & C4i drawings	586
4.16 Layout drawings of C3i	586
4.17 Certifications for Project components.....	587
4.18 Coordinates of all Police Stations (C2i locations)- district wise and the status of civil infrastructure	590
4.19 Location details of 3351 field sites and the respective number of deployable cameras	590
4.20 Details of the poles to be erected/ installed (5361 no.)	590
4.21 Important Instructions for Application Software	590
Chapter 5. : Price Bid Format.....	592
Chapter 6. Contract Form (Draft).....	613
6.1. Scope of work.....	615
6.2. Key Performance Measurements.....	615
6.3. Commencement and Progress.....	615
6.4. Standards of performance.....	615
6.5. Approvals and Required Consents	616
6.6. MSI's Obligations.....	616
6.7. C-DAC's Obligations	623
6.8. Payment Terms.....	624
6.9. Ownership and Retention of Documents	626



6.10.	Information Security	626
6.11.	Records of contract documents	627
Chapter 7. : Standard Formats.....		628
7.1.	Annexure – 1: Covering Letter	628
7.2.	Annexure – 2: Format for Power of Attorney to Authorized Signatory	630
7.3.	Annexure – 3: Undertaking towards EMD.....	631
7.4.	Annexure – 4: Documents Check-List.....	632
7.5.	Annexure – 5: Undertaking for Non-Malicious Code	635
7.6.	Annexure – 6: Manpower Plan.....	636
7.7.	Annexure – 7 : Manufacturers' Authorization Form	640
7.8.	Annexure – 8: Total Responsibility Certificate.....	642
7.9.	Annexure - 9: Unconditional and Irrevocable Performance Bank Guarantee Format.....	642
7.10.	Annexure – 10: Non-Blacklisting Declaration by JV Members.....	644
7.11.	Annexure – 11: Brief company profile (required for both bidder and JV member)	645
7.12.	Annexure - 12: Change Control Note	646
7.13.	Annexure – 13: JV Agreement.....	648
7.14.	Annexure – 14: Pre-Qualification Criteria Document Index List	650
7.15.	Annexure – 15: Integrity Pact.....	651



This Page is Left Bank Intentionally



Chapter 1. : Instructions For Bidders (IFB)

1.1. Required Assistance to Bidders

Any query relating to the process of online bid submission or queries relating to CPP Portal in general may be directed to the 24x7 CPP Portal Helpdesk on :- 0120-4200 462, 0120-4001 002, 0120-4001 005, 0120-6277 787, e-mail for Technical - support-eproc@nic.in

From C-DAC, the following credentials may be referred for assistance on RFP document:
delhisafecitybid@cdac.in .

1.2. On-Line Bid Submission

The bidders are required to submit soft copies of their techno-commercial bids electronically through the CPP Portal, using valid Digital Signature Certificates.

1.2.1. Registration on e-procurement Portal

- a. Bidders are required to enroll on the e-Procurement module of the Central Public Procurement Portal (url: <https://eprocure.gov.in/eprocure/app>).
- b. As part of the enrolment process, the bidders will be required to choose a unique username and assign a password for their accounts.
- c. Bidders are advised to register their valid email address and mobile numbers as part of the registration process. These would be used for any communication from the CPP Portal.
- d. Upon enrolment, the bidders will be required to register their valid Digital Signature Certificate (Class II or Class III Certificates with signing key usage) issued by any Certifying Authority recognized by CCA India with their profile.
- e. Only one valid DSC should be registered by a bidder. Please note that the bidders are responsible to ensure that they do not lend their DSCs to others, which may lead to misuse.
- f. Bidder then can log into the site through the secured login by entering their user ID / password and the password of the DSC / e-Token.

1.2.2. Preparation of Bids & adequate attention to NIT, corrigendum, uploading formats, others

- a. Bidders should take into account any corrigendum published on the Tender Document before submitting their bids.
- b. Bidders should go through the tender advertisement and the Tender Document carefully to understand the documents required to be submitted as part of the bid. Please note the number of covers in which the bid documents have to be submitted, the number of documents – including the names and contents of each of the documents that need to be submitted. Any deviations from these may lead to rejection of the bid.
- c. Bidders, in advance, should get the bid documents ready to be submitted as indicated in the Tender Document / schedule and generally, they can be in PDF / XLS / RAR / DWF formats. Bid documents may be scanned with 100dpi with black and white option and should be readable.
- d. To avoid the time and effort required in uploading the same set of standard documents which are required to be submitted as a part of every bid, a provision of



uploading such standard documents (e.g. PAN card copy, annual reports, auditor certificates etc.) has been provided to the bidders. Bidders can use 'My Space' area available to them to upload such documents. These documents may be directly submitted from the 'My Space' area while submitting a bid, and need not be uploaded repeatedly. This will lead to a reduction in the time required for bid submission process.

1.2.3. Successful Submission of bids

- a. Bidder should log into the site well in advance for bid submission so that the bid could be uploaded in time i.e. on or before the bid submission time. Bidder will be responsible for any delay due to other issues.
- b. The bidder has to digitally sign and upload the required bid documents one by one as indicated in the Tender Document.
- c. The server time (which is displayed on the bidders' dashboard) will be considered as the standard time for referencing the deadlines for submission of the bids by the bidders, opening of bids etc. The bidders should follow this time during bid submission.
- d. The uploaded Bid documents become readable only after the tender opening by the authorized bid openers.
- e. The hard copy of the Tender Fee document should be posted/couriered/given in person to the Tender Inviting Authority, within, on or before bid submission due date and time as indicated in the tender.
- f. Upon the successful and timely submission of bids, the portal will give a successful bid submission message and a bid summary will be displayed with the bid no. and the date & time of submission of the bid with all other relevant details.

1.3. Fact Sheet & Calendar of Events

Sr. No.	Item	Description
1	RFP- in 7 Chapters	Chapter 1: Instructions to Bidders Chapter 1 details the instructions with respect to the bid process management, Pre-qualification, technical evaluation framework, technical & financial forms along with the bid submission guidelines. Chapter 2: Conditions of Contract Chapter 2 includes Prequalification criteria, opening of Bids, Timelines and Payment Schedule etc., General conditions of the contract, Special conditions of the contract, SLA, Penalties, POC Evaluation formats etc. Chapter 3: Schedule of Requirement (SoR) Chapter 3 details about the type and number components required at Data Center, and Command and Control Centers as well as at field locations. This Chapter will also include information about POC Evaluation formats, Testing and Audits etc.



		Chapter 4: Scope of work Chapter 4 includes the Project Scope including Functional Requirement Specifications & Technical Requirement Specifications, Key Performance Indicators, Approach of the solution, Design & Standards, Planning & Execution, Testing, Approvals, Operation & Maintenance Phase, Technical Details of Data Center, Near DR, C4i, C3i, C2i, SLAs for the project etc. Physical Layouts of Data Center, C4i, C3i, C2i, SLAs for the project etc. Chapter 5: Price Bid Format Chapter 5 contain financial bid (.xls file) as per the format given on CPP portal. Chapter 6: Contract Form Chapter 6 contains the Master Service Agreement (MSA), which covers the contractual, legal terms & conditions applicable for the proposed engagement. Chapter 7: Standard Formats Chapter 7 contains formats of required documents referred in the FRP document.
2	Method of Selection	QCBS (Quality cum Cost-Based Selection): The weightage given to the technical and financial score will be 70% and 30% respectively. Each Technical Bid will be assigned a Technical score out of a maximum 100 marks. Only the Bidders who secure minimum 15 marks for parameter G of QCBS and an overall Technical score of 70% or more in the Technical Evaluation Framework (Parameter A-H) as given in the RFP will qualify for Financial Evaluation stage. Failing to secure minimum marks shall lead to technical rejection of the Bid. The Contract will be awarded to the Bidder who will gain maximum marks through QCBS terms and conditions (Technical-cum-Commercial scores) laid down in the RFP.
3	Availability of RFP Documents	Download from https://eprocure.gov.in/eprocure/app
4	RFP Document Fee/ Tender document fee (Non-refundable and Not exempted)	INR 5,000/- (INR Five Thousand Only)- inclusive of taxes



5	Bid Security/ Earnest Money Deposit (EMD)	Declaration as per format given at Annexure - 3
6	Bid validity	Bid must remain valid up to 180 (One Hundred & Eighty) days from the actual date of submission of the Bid.
7	Currency	Currency in which the Bidders may quote the price and will receive payment is INR only.
8	Bank Details for depositing Tender fee/ EMD	Name of Account: Centre for Development of Advanced Computing Name of Bank: IDBI Bank, Gokhale Road, Pune - 411016, Account No: 600104000083030 IFSC / NEFT Code: IBKL0000600
9	Release of RFP	18th December, 2020
10	Last date of sending pre-bid queries on RFP	28th December, 2020, 1700 Hrs.
11	Pre-bid Meeting date	30th December, 2020, 1200 Hrs. (maximum 2 member representation for prospective MSI bidders with Authorization Letter)
12	Venue for pre-bid meeting	Centre for Development of Advanced Computing, S. No 34, Innovation Park, Panchavati, Pashan Road, Pune - 411 008.
14	Last date for submission of Bids	23rd January, 2021, 1500 Hrs.
15	Opening of Technical Bids	25th January, 2021 1500 Hrs
16	Opening of Commercial Bids	Will be notified later.

1.4. Acronyms- list of abbreviations

Sr. No	Term/Acronyms	Description
1.	AAA	Authorization, Authentication and Accounting
2.	AFIS	Automatic Fingerprint Identification System
3.	AI	Artificial Intelligence
4.	ANPR	Automatic Number Plate Recognition
5.	API	Application Programming Interface
6.	APT	Advanced Persistent Threats
7.	AVLS	Automatic Vehicle Location System
8.	BOQ	Bill of Quantities
9.	BDCR	Big Data and Correlation Tool



Sr. No	Term/Acronyms	Description
10.	C2i	Command & Control
11.	C3i	Command, Control & Communication
12.	C4i	Integrated Command, Control, Communication & Compute
13.	CAD	Computer Aided Dispatch
14.	CAPEX	Capital Expenditure
15.	CCIS	Crime Criminal Information System
16.	CCTNS	Crime and Criminal Tracking Network and Systems
17.	CCTV	Closed Circuit Television
18.	CDR	Call Detail Record
19.	CERT-IN	Computer Emergency Responses Team – India
20.	CMMI	Capability Maturity Model Integration
21.	CMOS	Complementary metal–oxide–semiconductor chip
22.	CoAP	Constrained Application Protocol
23.	COTS	Commercial Off-The-Shelf
24.	CPPP	Central Public Procurement Portal
25.	CPU	Central Processing Unit
26.	CRUD Operations	Create, Read, Update and Delete operations
27.	CSV	Comma-Separated Values
28.	CTFS	The Combined Technical and Financial Score
29.	DAS	Digital Address System
30.	DC	Data Center
31.	DCP	Deputy Commissioner of Police
32.	DDos	Denial of Service Attack
33.	DG Set	Diesel generator
34.	DHQs	District Headquarters
35.	DPIP	Detailed Project Implementation Plan
36.	DRC	Disaster Recovery Center
37.	DSC	Digital Signature Certificate
38.	DVI	Digital Video Interface
39.	DVM	Digital Video Manager
40.	EMD	Earnest Money Deposit
41.	EMS	Enterprise Management System
42.	EOC	Emergency Operation Center
43.	ERP	Enterprise Resource Planning
44.	ERSS	Emergency Response Support System



Sr. No	Term/Acronyms	Description
45.	FIR	First Information Report
46.	FPS	Frames Per Second
47.	FRS	Facial Recognition System
48.	GCC	General Conditions of Contract
49.	GI	Galvanized Iron
50.	GIS	Geographical Information System
51.	GOI	Government Of India
52.	GPS	Global Positioning System
53.	GPU	Graphics processing unit
54.	GSM	Global System for Mobile
55.	GST	Goods and Services Tax
56.	GUI	Graphical User Interface
57.	HA	High Availability
58.	HDMI	High-Definition Multimedia Interface
59.	HTTP	Hypertext Transfer Protocol
60.	HTTPS	Hypertext Transfer Protocol Secure
61.	HVAC system	Heating, ventilation, and air conditioning
62.	IAM	Identity and Access Management
63.	ICCC	Integrated Command & Control Center
64.	ICCP	Integrated Command & Control Platform
65.	ICJS	Integrated Criminal Justice System
66.	ICT	Information & Communications Technology
67.	IFB	Instructions For Bidders
68.	IoT	Internet of Things
69.	IP	Internet Protocol
70.	IPPBX	Internet Protocol Private Branch Exchange
71.	IPS	Intrusion Prevention System
72.	ISDN	Integrated Services Digital Network
73.	ISMS	Information Security Management System
74.	ITIL	Information Technology Infrastructure Library
75.	ITMS	Integrated Transportation Management System
76.	JV	Joint Venture
77.	LAN	Local Area Network
78.	LDAP	Lightweight Directory Access Protocol
79.	LOI/LOA	Letter of Intent/Letter of Award



Sr. No	Term/Acronyms	Description
80.	MAC	Media Access Control
81.	MAF	Manufacturers'/Producers' Authorization Form
82.	MCC	Mobile Command Centers
83.	MCCV	Mobile Command Control Vehicles
84.	MeitY	Ministry of Electronics and Information Technology
85.	MFA	Multi-Factor Authentication
86.	MHA	Ministry of Home Affairs
87.	ML	Machine Learning
88.	MoU/MoA	Memorandum of Understanding/ Memorandum of Agreement
89.	MoWCD	Ministry of Women and Child Development
90.	MPLS	Multi-Protocol Label Switching
91.	MQTT	Message Queue Telemetry Transport
92.	MSA	Master Service Agreement
93.	MSI	Master System Integrator
94.	MUX	Multiplexer
95.	NAC	Network Access Control
96.	NAS	Network Attached Storage
97.	NCR	National Capital Region
98.	NCRB	National Crime Record Bureau
99.	NCT	National Capital Territory
100.	NDA	Non-Disclosure Agreement (NDA)
101.	nDRC	Near Data Recovery Center
102.	NIC	National Informatics Centre
103.	NIT	Notice Inviting Tender
104.	NMS	Network Management System
105.	NOC	Network Operations Center
106.	O&M	Operation & Maintenance
107.	OCR	Optical Character Recognition
108.	OEM	Original Equipment Manufacturer
109.	OFC	Optical Fiber Cable
110.	OGC	Open Geospatial Consortium
111.	ONVIF	Open Network Video Interface Forum
112.	OPEX	Operation Expense
113.	OSPF	Open Shortest Path First
114.	PA System	Public Address System



Sr. No	Term/Acronyms	Description
115.	PB	Petabyte
116.	PBG	Performance Bank Guarantee
117.	PCC	Police Clearance Certificate
118.	PCR	Police Control Room
119.	PCR Vans	Police Control Room Vans
120.	PDU	Power Distribution Unit
121.	PHQ	Police Headquarters
122.	PiB	Pebibyte
123.	P-IRIS	Picture Intelligence Recording and Investigation System
124.	PIU	Picture Intelligence Unit
125.	PKI	Public Key Infrastructure
126.	PoC	Proof of Concept
127.	PoE	Power Over Ethernet
128.	PoP	Point of Presence
129.	PSTN	Public Switched Telephone Network
130.	PTZ	Pan-Tilt-Zoom
131.	QCBS	Quality and Cost Based Evaluation
132.	QoS	Quality of Services
133.	RFP	Request for Proposal
134.	RoW	Right of Way
135.	RPO	Recovery Point Objective
136.	RTO	Recovery Time Objective
137.	RTS	Real Time Streaming
138.	RTSP	Real Time Streaming Protocol
139.	SAN	Storage Area Network
140.	SCC	Special Conditions of Contract
141.	SDK	Software Development Kit
142.	SDK/APIs	Software Development Kit/Application programming interface
143.	SD-WAN	Software-Defined Wide-Area Network
144.	Server Room	Sever room and data centre shall mean the same.
145.	SFTP	Screened Fully Shielded Twisted Pair
146.	SIEM	Security Information and Event Management
147.	SJB	Surveillance Junction Box
148.	SLA	Service Level Agreement; Performance and Maintenance SLA executed as part of this Master Service Agreement;



Sr. No	Term/Acronyms	Description
149.	SME	Subject matter experts
150.	SMPS	Switched-Mode Power Supply
151.	SOA	Service-Oriented Architecture
152.	SOP	Standard Operating Procedure
153.	SoR	Schedule of Requirement
154.	SSL	Secure Sockets Layer
155.	SSO	Single Sign-On
156.	STP	Shielded Twisted Pair
157.	STQC	Standardization Testing and Quality Certification
158.	SYSLOG	System Logging Protocol
159.	TCP/IP	Transmission Control Protocol/Internet Protocol
160.	TEC	Tender Evaluation Committee
161.	TLS	Transport Layer Security
162.	TSP	Total Service Provider (C-DAC)
163.	UAT	User Acceptance Testing
164.	UDP	User Datagram Protocol
165.	UHD	Ultra High Definition
166.	UHF	Ultra High Frequency
167.	UI	User Interface
168.	UPS	Uninterruptible Power Supply
169.	URL	Uniform Resource Locator
170.	USB	Universal Serial Bus
171.	UTM	Unified Threat Management
172.	VA	Video Analytics
173.	VMS	Video Management Software/System
174.	VNMS	Virtual Network Management System
175.	VOIP	Voice Over Internet Protocol
176.	VPN	Virtual Private Network
177.	WAF	Web Application Firewall
178.	WAN	Wide Area Network
179.	Web PIS	Web-Based Personnel Information System
180.	WMS	Web Map Service
181.	XLS	Excel Spreadsheet
182.	ZIPNET	Zonal Integrated Police Network



1.5. Purpose

This document introduces the bidders with essential parameters that will help in understanding the requirement of C-DAC/ Delhi Police so the intended bidder can participate in the competitive bid process and thereby formulate a time bound implementation approach.

This Chapter of the RFP will clearly define the foundation of the envisioned project with clear set of instructions to bid as per standard norms, project terms and conditions (GCC & SCC), evaluation and selection criterion, timelines, associated payment terms, roles and responsibilities of stakeholders, etc.

The aim of this system is to capture all activities at the places under surveillance, generate alarms, warnings in case of any potential threat to women's safety, especially physical / sexual harassment targeting women, followed by real-time technology aided assistance to women in distress.

The broad aims to achieve through this envisaged project are:

- a. Enhanced surveillance and demonstrative presence / visibility in public places by installing CCTV cameras and deploying dedicated women's mobile police vans (Prakhar Vans) and Mobile Command Control Vehicle [MCCV].
- b. A fast and efficient emergency response program, for assisting women in distress
- c. Focus on ensuring rapid availability of professionally trained police personnel to address the needs of women in distress through the use of technology.

The broad objectives include: Women, Children and Elderly People' Security and Safety- Quick and effective emergency response system, Improved responsiveness, Effective Policing, Improved Management, Reduction in crime, Integrations and scalability, Process Commissioning through ICT (Information and communication Technology), Skill enhancement.

The objectives and intended benefits of this envisaged projects are detailed out with the Scope of Work in Chapter 4 so as to enable the prospective bidders to understand and relate the project fundamentals with the project requirements in a better meaningful way.

1.6. Definitions

- a. **"Acceptance of System"**: The system shall be deemed to have been accepted by C-DAC & Delhi Police, subsequent to its installation, rollout and deployment of trained manpower, when all the activities as defined in Scope of Work detailed in Chapter 4 of the RFP have been successfully executed and completed to the satisfaction of C-DAC & Delhi Police.
- b. **"Applicable Law(s)"**: Any statute, law, ordinance, notification, rule, regulation, Judgment, order, decree, bye-law, approval, directive, guideline, policy, requirement or other governmental restriction or any similar form of decision applicable to the relevant party and as may be in effect on the date of the execution of this contract and during the subsistence thereof, applicable to the Project.
- c. **"Bid"**: Offer by the Bidder to fulfil the requirement of the Authority for an agreed price. It shall be a comprehensive technical and financial response to the RFP.
- d. **"Bidder"** shall mean the Sole Bidder or the JV organization submitting the proposal in response to this RFP



- e. **“C-DAC”** means the Centre for Development of Advance Computing, a key stakeholder for Delhi Safe City Project has been appointed as the Nodal Agency and Total Service Provider for Delhi Police towards the selection of Implementation Agency, conduction of implementation approach of Delhi Safe City Project. C-DAC will be acting as an interim employer for the MSI till the contractual association with the Implementation agency.
- f. **“MSI”** means the Successful Bidder who is selected by C-DAC through this RFP process. The Successful Bidder shall carry out all the services mentioned in the scope of work of this RFP.
- g. **“Contract/Agreement”** means the Contract/Agreement entered into by and between the two parties viz. C-DAC and MSI, Sole or Joint Venture, as the case maybe, with the entire documentation specified in the RFP.
- h. **“Contract Value”** means the price payable to MSI under this Contract for the complete and proper performance of its contractual obligations.
- i. **“Commercial Off-The-Shelf (COTS)”** refers to software products that are ready-made and available for sale, lease, or license to the general public.
- j. **“JV”**: A JV consists of multiple members (not more than three parties) entering into a JV Agreement for a common objective of satisfying the project requirements & represented by a legal entity, designated as a “MSI” post declaration of the L1 bidder. At the stage of Bid Process, the JV can be a non-incorporated entity in the form of mutual agreement among the parties involved with the purpose of participation only.
- k. **“Data Centre Site”** means the Data Centre sites including their respective Data Centre space, wherein the delivery, installation, integration, management and maintenance services as specified under the Scope of Work are to be carried out for the purpose of this Contract.
- l. **“Document”** means any embodiment of any text or image however recorded that includes any data, text, images, sound, voice, codes, databases or any other electronic documents as per IT Act 2000.
- m. **“Deliverables”** means Products, infrastructure and services agreed to be delivered by the Bidder in pursuance of the agreement as defined more elaborately in the RFP, Implementation and the Maintenance phases and includes all documents related to the user manual, technical manual, design, process and operating manuals, service mechanisms, policies and guidelines (such as security related, data migration related), inter alia payment and/or process related etc., source code and all its modifications.
- n. **“Effective Date”** means the date on which C-DAC issues the Letter of Intent/ Work Order to proceed subsequent to the Contract is signed, and executed by the Parties hereto.
- o. **“GCC”** means General Conditions of Contract
- p. **“Goods”** means all of the equipment, sub-systems, hardware, software, products accessories, software and/or other material / items which MSI is required to supply, install and maintain under the contract.
- q. **“Intellectual Property Rights”** means any patent, copyright, trademark, trade name, service marks, brands, proprietary information whether arising before or after the execution of this Contract and the right to ownership and registration of these rights.
- r. **“Go-Live”** means commissioning of Project after installation and commencement of all safe city components, including training as per scope of work mentioned in this RFP. MSI should have the approval from C-DAC for user acceptance testing.
- s. **“Non-Compliance”** means failure/refusal to comply with the terms and conditions of the tender
- t. **“Non-Responsive”** means failure to furnish complete information in a given format and manner required as per the tender documents or non-submission of tender offer in given forms/ pro forma or not following procedure(s) mentioned in this tender or any of required



- details or documents is missing or not clear or not submitted in the prescribed format or non-submission of RFP Document/ tender fee and/ or EMD
- u. **"Notice"** means: a notice; or consent, approval or other communication required to be in writing under this Contract.
 - v. **"OEM"** means the Original Equipment Manufacturer of any equipment / system / software / product which are providing such goods to C-DAC under the scope of this RFP.
 - w. **"MSI's Team"** means MSI who has to provide goods & services to C-DAC under the scope of this Contract. This definition shall also include any and/or all of the employees of MSI, authorized service providers/ partners and representatives or other personnel employed or engaged either directly or indirectly by MSI for the purposes of this Contract.
 - x. **"NoC"** A Network Operations Center (NoC) is defined as the place from which the networks are supervised, monitored and maintained. It typically has a network operations center, a room containing visualizations of the network or networks that are being monitored, workstations at which the detailed status of the network can be seen, and the necessary software to manage the networks.
 - y. **"Replacement Service Provider"** means the organization replacing MSI in case of contract termination for any reasons
 - z. **"Required Consents"** The consents, waivers, clearances and licenses to use Authority Intellectual Property Rights, rights and other authorizations as may be required to be obtained for the software and other items that MeitY, GoI & their nominated agencies are required to make available to Bidder pursuant to this Agreement
 - aa. **"Service Level"** The level of service and other performance criteria which will apply to the Services delivered by the Bidder;
 - bb. **"Sub-Contractor"** shall mean the entity named in the contract for any part of the work or any person to whom any part of the contract has been sublet with the consent in writing of C-DAC and the heirs, legal representatives, successors and assignees of such person.
 - cc. **"SCC"** means Special Conditions of Contract.
 - dd. **"Services"** means the work to be performed by the MSI pursuant to this Contract, RFP and to the contract to be signed by the parties in pursuance of any specific assignment awarded by C-DAC.
 - ee. **"Server Room"** or **"Data Center"** shall have the same meaning.
 - ff. **"Successful Bidder"**: The Bidder who is qualified & successful in the bidding process and is awarded the work.

1.6.1. Interpretation

- i. In this Contract/Agreement unless specified otherwise:
 - a. The clause headings are for convenience of reference only and do not form part of this Contract/Agreement;
 - b. A reference to a clause number is a reference to all of its sub-clauses;
 - c. The word "include" or "including" shall be deemed to be followed by "without limitation" or "but not limited to" whether or not they are followed by such phrases;
 - d. Unless otherwise specified a reference to a clause, sub-clause or section is a reference to a clause, sub-clause or section of this Contract including any amendments or modifications to the same from time to time;
 - e. A word in the singular includes the plural and a word in the plural includes the singular;
 - f. A word importing a gender includes any other gender;



- ii. A reference to a person includes a partnership and a body corporate, its successors and assignees or a reference to legislation includes legislation repealing, replacing or amending that legislation;
 - a. Where a word or phrase is given a particular meaning, it includes the appropriate grammatical forms of that word or phrase which have corresponding meanings.
 - b. In the event of an inconsistency between the terms of this Contract and the RFP and the Bid, the terms hereof shall prevail.

1.7. Introduction to the Project- Delhi Safe City

1.7.1. Safe City Need in the National Capital Territory, Delhi

Delhi Police is the law enforcement agency of the National Capital Territory, Delhi, providing policing services to the citizens of Delhi through 16 districts. Despite the best efforts of law enforcement agencies, such as dedicated Women helpline Number, Women PCR Vans, special police unit for women and children, anti-stalking helpline and mobile applications such as Himmat Plus designed for women safety, women in the national capital of Delhi tend to feel unsafe in many public spaces.

While safe city is a concept, which is evolving, the Ministry of Home Affairs has issued advisories, where effective measure to be taken to curb crime against women. Some of the important features prescribed for increasing security for women in rural and urban places, inter-alia, include (in terms of Safe City):

- a. Surveillance through CCTV and technology-based interventions;
- b. Safety in Public Transportation systems

As part of its endeavors to enhance women safety in Delhi with use of all possible means and resources with utmost efficiency, Delhi Police intends to undertake a Safe City Project with various analytical and Artificial Intelligence tools for safety in public places in Delhi.

The use of state-of-the-art CCTV monitoring, helps to ensure a cityscape that is safe and secure for women, is a technology model that has been widely demonstrated across the globe. To ensure safety and security in places frequently visited by women, such as market places, highways, bus terminals, metro stations, recreational areas, areas around women schools/ colleges/ institutions, etc., the need for such a technology enabled surveillance is more imperative, therefore, Delhi Police has recommended to introduce a 24x7 real-time Safe City Project in Delhi to ensure women's safety and protection.

1.7.2. Important Stakeholders for important guidance and contributions

The project requires collaboration between multiple stakeholders for its successful execution. It is therefore important to understand the various stakeholders envisioned to be part of this project and the role that they are expected to play. Following are the critical stakeholders whose involvement will drive the project and enable the establishment of strong project governance:

- i. Ministry of Home Affairs (MHA)
- ii. Ministry of Women and Child Development (MoWCD)
- iii. Delhi Police
- iv. C-DAC (Total Service Provider)- Nodal Agency
- v. Master System Integrator (Implementation Agency)



- vi. Internet Service Provider (Network Bandwidth Provider Agency)
- vii. Civic agencies of Government of National Capital Territory, Delhi (GNCT)
- viii. Power Distribution Companies of Delhi

1.7.3. Delhi Police Functioning Structure and administration

Delhi Police is headed by the Commissioner of Police. The entire portfolio of functions is divided into 16 districts of Delhi NCT. There are 7 Range Offices which regulates the respective groups of District Offices.

The key decision taking entities regarding Delhi Safe City includes the Spl. Commissioner of Police at PHQ and Deputy Commissioner of Police (DCP) at the District level.

Henceforth, the following propositions of Command and Control have been envisaged to empower PHQ, Districts Offices, and Police Stations for effective facilitation of Decision Support System:

Sr. No.	Office	Envisaged Facility
1.	PHQ	Integrated Command, Control, communication and Compute (C4i) center
2.	Districts	Command, Control and Communication (C3i) center
3.	Police Station	Command and Control (C2i) center

1.7.4. Governance Structure for Safe City Project of Delhi Police

- a. National Level Committee (Home Secretary, GoI)
- b. State Level Apex Committee under the chairmanship of CP, Delhi
- c. Steering Committee chaired by Spl. CP
- d. Technical Committee chaired by Spl. CP
- e. Purchase Committee chaired by Spl. CP
- f. TSP (Total Service Provider/C-DAC) for Project monitoring

1.8. General

- a. While every effort has been made to provide comprehensive and accurate background information, requirements and envisaged solution(s) specifications, Bidders must conduct their own due diligence and form their own conclusions about the solution(s) needed to meet C-DAC/ Delhi Police requirements. Bidders and recipients of this RFP may wish to consult their own legal advisers in relation to this RFP.
- b. All information supplied by Bidders as part of their Bids in response to this RFP, may be treated as contractually binding on the Bidders, on successful award of the assignment by C-DAC on the basis of this RFP.
- c. No commitment of any kind, contractual or otherwise shall exist unless and until a formal written Agreement has been executed by or on behalf of C-DAC. Any notification of preferred bidder status by C-DAC shall not give rise to any enforceable rights to the Bidder. C-DAC may cancel this public procurement at any time prior to a formal written Agreement being executed by or on behalf of C-DAC.
- d. Telex, cable or facsimile Bids will be rejected.



- e. For any assistance, the Bidders can contact the following officer as per their convenience on the address given below:
Department: MMG Group of C-DAC
Email Id: delhisafecitybid@cdac.in

1.9. Eligible Bidders

Bids may be submitted by either of the following categories of Bidders only:

The Bidder can be either a Sole Bidder i.e. Single Master System Integrator (MSI) or a JV of companies as described below.

A JV should not consist of more than three parties. The JV would have the sole responsibility of ensuring the delivery of products and services mentioned in all chapters of this RFP. The Sole Bidder/ JV would also be responsible for ensuring the successful execution of integrated solution including meeting the SLAs. The list of JV Members needs to be declared in the Bid which cannot be changed by the Bidder later on.

The Member of the JV holding highest stake shall be the Principal Partner.

A JV agreement must be submitted along with the Bid and shall specify the roles & responsibilities of the JV members.

The Sole Bidder or Joint Venture must comply the Eligibility/Pre-Qualification criteria as stipulated at Para 2.1.3 Chapter 2 of this document. In case of Joint Venture, the Lead/Principal Partner shall be liable for all acts and omissions. The Principal Partner shall be responsible for the successful completion of the Contract/Agreement and C-DAC shall be communicating with the Principal Partner for all necessary actions. The Principal Partner shall be held liable and responsible for any breach of any of the terms and conditions of the Contract / Agreement.

The Sole Bidder or a Joint Venture as the bidder, shall hereafter be referred as 'bidder' in this document.

1.9.1. Compliant Bids/Completeness of Response

- a. Bidders are advised to carefully study all instructions, forms, terms, requirements and other information in the RFP document. Submission of the Bid shall be deemed to have been done after careful study and examination of the RFP document with full understanding of its implications.
- b. Failure to comply with the requirements of this Clause No. 8 may render the Bid non-compliant and the Bid may be rejected. Bidders must:
 - i. Include all documents specified in this RFP, in the Bid
 - ii. Follow the format of this RFP while developing the Bid and respond to each element in the order as set out in this RFP
 - iii. Comply with all requirements as set out within this RFP

1.9.2. Bidder to Inform (clarification)

The Bidder shall be deemed to have carefully examined the Terms & Conditions, Scope, Service Levels, Specifications, and Schedules of this RFP. If Bidder has any doubts/clarifications as to the meaning of any portion of the conditions or the specifications, he shall get them clarified before the last date for Submission of Pre-Bid



Queries, set forth the particulars thereof and submit them to C-DAC in writing in order that such doubt may be removed or clarifications are provided in the manner set out in the RFP.

1.9.3. Bid Preparation Costs

The Bidder shall bear all costs associated with the preparation, submission, clarification of its Bid, attending pre-bid meetings etc., if any.

1.9.4. Pre-Bid Meeting & Clarification

Bidders Queries: In case of any doubts and/ or queries pertaining to technical solution, specifications terms and conditions of the tender, prospective bidder may send their queries in writing through e-mail (delhisafecitybid@cdac.in). The queries, requests for clarifications etc. must be sent on or before the date given in Fact Sheet and Calendar of Events on Para 1.3 of Chapter 1. The bidders are requested to go through the entire Tender Document thoroughly, before raising any query. C-DAC, Pune shall address the queries raised by the bidders in the pre-bid meeting. The replies to queries would be made available on CPP Portal and C-DAC's web site in due course of time.

The pre-bid queries should be submitted in MS excel sheet format given below, along with name and details of the organization submitting the queries.

Name of Bidder:					
Sr. No.	Chapter No	Para No	Page No	Clause/ Content in the RFP	Suggestive input/ clarification for the Content in the RFP
1					
2					
.					

C-DAC shall not be responsible for ensuring that the Bidders' queries have been received by them. Any requests for clarifications post the indicated date and time shall not be entertained by C-DAC.

Pre-bid meeting will be held as per details given in Fact Sheet and Calendar of Events, given para 1.3 of Chapter 1. Maximum of 02 members per Bidder will be allowed to participate in the Pre-Bid Conference. The representatives attending the pre-bid meeting should carry appropriate authority letter with them.

1.9.5. Responses to Pre-Bid Queries and Issue of Corrigendum

The responses/replies to pre-bid queries will be uploaded on CPP Portal after the pre-bid conference. No further clarifications shall be entertained after the date and time of submission of queries.



C-DAC shall endeavor to provide timely response to all queries. However, C-DAC makes no representation or warranty as to the completeness or accuracy of any response made in good faith. C-DAC does not undertake to answer all the queries that have been posed by the bidders.

Any modifications of the RFP Documents, which may become necessary as a result of the Pre-Bid Conference, shall be made by C-DAC exclusively through a corrigendum and in writing and any such corrigendum shall be deemed to be incorporated into this RFP. However, in case of any such amendment, the bid submission date may be extended at the discretion of C-DAC.

Any corrigendum/notification/ responses/replies issued by C-DAC, subsequent to issue of RFP, shall only be available/hosted on CPP Portal and on C-DAC web site.

1.9.6. RFP Document Fee

RFP can be downloaded from the website URL mentioned in the fact sheet.

RFP Document Fee/ Tender Fee of (As mentioned in the facts sheet) shall be paid at the time of submission of bid through online mode only. The tender fee shall be non-refundable and/or non-adjustable.

Without the payment of tender fee, the Bid shall be deemed as incomplete and non-responsive and shall not be considered. There would be a processing fess which should be paid through online mode only.

1.9.7. Contents of Bid

The 'Two e-bid' system will be followed for this RFP where the Technical Bid and Financial Bid are required to be uploaded in separate e-packets, as described below.

I: The "Technical e-Bid" documents should be uploaded in e-Packet 1.

II: The "Financial e-Bid" should be uploaded in e-Packet 2.

A. e-Packet No. 1 will contain:

1. Covering Letter as per format given in 'Annexure 1'
2. A written undertaking from each of the JV members, in case of a JV, duly signed by the authorized signatory, holding a written power of attorney for this bid on a stamp paper, authorizing the JV and the authorized signatory to incur liabilities and receive instructions for and on behalf of any and all JV members, and the entire execution of the Agreement/Contract, including but not limited to the payments 'Annexure 11'
3. DD for RFP Document Fee or on-line payment receipt
4. Bid Security/Earnest Money Deposit (EMD) receipt or Declaration as per Annexure 3.
5. GST registration certificate/s and copy of PAN
6. Copy of certificate of Incorporation/Registration of bidder firm under applicable Indian law. In case of JV the copy of duly executed JV agreement along with, the certificates of registration for all members are required. Global companies to



- provide equivalent proof of incorporation/ registration in India as per applicable Law
7. The copy of registration certificate or a declaration in compliance with the provisions stipulated in office memorandum F/No/6/18/2019-PPD dated 23 July 2020 issued by public procurement Division, Dept. of Expenditure, Ministry of Finance, GoI.
 8. MoA among the JV Partners showing the area of business their legal arrangement inter se.
 9. Copies of audited balance sheets for the financial years 2019-20, 2018-19 and 2017-18 pertaining to sole bidder/ members of JV (In case of JV)
 10. Certificate from the Statutory Auditor/CA on net worth and Profitability for financial years 2019-20, 2018-19 and 2017-18 pertaining to sole bidder / each member of JV (In case of JV)
 11. Certificate from the Statutory Auditor/CA certifying the annual turnover of sole bidder/lead partner (In case of JV) in the areas of Supply, Implementation and Integration of City Surveillance System and/or, Data Centre infrastructure in years 2019-20, 2018-19 and 2017-18.
 12. Certificate from the Statutory Auditor/CA on net worth and Profitability for the FY 2019-20, 2018-19 and 2017-18 pertaining to OEM of cameras, ICCC and VMS, FRS, Video Analytics.
 13. Copies of audited balance sheets OR Certificate from the Statutory Auditor/CA certifying the annual turnover of OEM of cameras, Servers, Storage, Networking & Security components, ICCC and VMS, FRS, Video Analytics for the FY 2019-20, 2018-19 and 2017-18.
 14. Document Check list as Per format given in '**Annexure 4**'
 15. List and address of bidder's office in Delhi or, undertaking from authorized signatory of bidder to open office with GST registration in Delhi within 60 days from Contract signing.
 16. The details of TAC centre/s in India with toll free number, pertaining to OEMs of camera, ICCC and VMS, FRS, Video Analytics.
 17. Copies of the CMMI level certificates in the name of the sole bidder/JV members and valid ISO certifications- if applicable.
 18. The copies of supply orders, contracts, and agreements or completion / installation certificates in the name of bidder/s in support of eligibility criteria/ pre-qualification criteria stipulated at para no. 2.2.3 of chapter 2 of this document.
 19. The copies of supply orders, contracts, and agreements or completion / installation certificates in the name/s of respective OEMs of components/subsystems, in support of eligibility criteria/ pre-qualification criteria stipulated at para no 2.2.3 of chapter 2 of this document
 20. Non-Malicious Code undertaking from OEMs of Camera and Video Analytic software, as per **Annexure – 5**.
 21. Certificate from Statutory Auditor/Company Secretary/ Board of Directors or Cost Accountant to the effect that for the purpose of this RFP, the bidding firm complies with the Order No P-45021/2/2017-PP (BE-II). Dated 4th June, 2020 issued by Public Procurement Division, Department of Investment and Internal Trade, Ministry of Commerce, GoI.
 22. Certificate from the statutory auditor of the bidding firm towards compliance with the pre-qualification criteria stipulated at 2.1.3, A.



23. Certificates of Origin and certificate of country of manufacture pertaining to Cameras, Servers, VMS, ICCV, UPS, Batteries, IP Phones, and Hand held devices, Video walls, Laptops, Workstations, Television, Printers, Storage, Power Meters, DG set, HVAC equipments and networking components offered.
24. Certificate from OEM of cameras in their letterhead confirming that any component/ hardware / parts / assembly / software including firmware used in the offered solution (hardware / software) **DO NOT COMPLY** to - GB28181, GB/T 28181-2011; GB/T28181-2011; GBT 28181- 2011; GBT28181-2011 standards.
25. Address and other details of RMA set up of OEM of camera in India.
26. Certificate from OEM of Cameras stating that OEM is not banned or suspended by ONVIF in last 5 years from the date of publishing this RFP.
27. Certification from OEM of ICCV towards compliance of eligibility /Pre-qualification criteria as mentioned in para 2.1.3 of Chapter 2
28. Certification from OEM of VMS towards compliance of eligibility /Pre-qualification criteria as mentioned in para 2.1.3 of Chapter 2
29. Details of service centre/Lab in India pertaining to OEM's of Cameras, servers, Storage, Display Monitors, Video Wall.
30. The details explaining level of understanding of the scope of work and all aspects of this project.
31. Details pertaining to overall project implementation approach, Phase wise scope and overlapping of activities, how time lines could be met, availability of qualified manpower, deployment plan, etc.
32. Availability and utilization of funds, contingency plan
33. Vendor management and plans for procurement of material in time
34. Risk Mitigation Plan/ Strategy/ SLA
35. Technical specifications of major components of the solution.
36. The line diagrams, drawings, GA Layouts, network diagrams, maps etc. as required for implementation of project.
37. Detailed technical compliance statement as given in Chapter 4.
38. Scalability, Safety, Reliability and Security features of the offered solutions
39. Manpower to be deployed on the project as per the format given at **Annexure – 6**.
40. Bill of quantities being offered as per format given in Chapter 3 (SoR)
41. Un-priced commercial bid (with prices blocked) actually uploaded on CPP portal, along with the commercial terms and conditions.
42. Product Certifications pertaining to components, Sub-systems offered as a part of solution.
43. Manufacturers'/Producers' Authorization Form (MAF) for Cameras, Servers, Storage, Networking switches, DG Set, HVAC system, UPS, ICCV, and VMS, as per format given at **Annexure – 7**.
44. Total responsibility undertaking, as per format given in **Annexure - 8**.
45. The bidder shall give undertaking towards compliance with eligibility criteria as para no. 2.1.3.A(i, j, k & l) of chapter 2.

Note: In view of large size of Bid to be submitted the bidders are requested to submit the above listed documents in the same sequence along with the list of contents.



B. e-Packet No. 2 will contain:

The Financial bid (.xls file) should be uploaded in e-packet 2. The Financial bid must be as per format given on CPP Portal.

Notes:

- i. The prices should NOT be indicated in the Technical Bid but should only be indicated in the Financial Bid.
- ii. All the documents submitted towards eligibility of pre-qualification/ eligibility criteria should be arranged as per the Annexure -14.
- iii. All the pages of the Bid must be sequentially numbered. The Bid documents must contain in the beginning of the document, a list of contents with page numbers.
- iv. The original Bid shall be prepared in indelible ink. It shall contain no interlineations or overwriting, except as necessary to correct errors made by the Bidder itself. Any such corrections must be initiated by the person (or persons) who sign(s) the Bids.
- v. All pages of the Bid shall be initialed and stamped by the person (or persons) who signs the Bid.

The bid documents should be addressed to:

Executive Director

Centre for Development of Advanced Computing(C-DAC)
Innovation Park, Panchavati,
Pashan Road, Pune – 411 008.

The Bid shall be uploaded/submitted on CPP Portal by the date and time mentioned in the Fact sheet.

1.9.8. Validity of Bids

The Bid submitted shall remain valid for a period of 120 days from date of submission. C-DAC may request for extending the validity without change in the financial Bid. A bid valid for a shorter period shall stand rejected.

C-DAC may ask for the bidder's consent to extend the period of validity. Such request and the response shall be made in writing only. A bidder agreeing to the request for extension will not be permitted to modify his bid.

1.9.9. Language of Bids

The Bid should be prepared and submitted by the Bidders in English language only. If any submitted supporting documents are in any language other than English, translation of the same in English language is to be provided (duly attested) by the Bidders. For purposes of interpretation of the documents, the English translation shall prevail.

1.9.10. Authentication of Bids

An authorized representative (or representatives) of the Bidder shall initial all pages of the Pre-Qualification, Technical and Financial Bids.



Bid should be accompanied by an authorization in the name of the signatory (or signatories) of the Bid. The authorization shall be in the form of a written power of attorney accompanying the Bid or in any other form demonstrating that the representative has been duly authorized to sign.

1.9.11. Amendment of Request for Proposal

At any time prior to the due date for submission of Bid, C-DAC may, for any reason, whether at its own initiative or in response to a clarification requested by prospective Bidder(s), modify the terms & conditions, quantities, specifications or other requirements stipulated in RFP document by amendments. Such amendments shall be uploaded on CPP Portal, through corrigendum and shall form an integral part of RFP document. The relevant clauses of the RFP document shall be treated as amended accordingly.

It shall be the responsibility of the prospective Bidder(s) to check C-DAC's website from time to time for any amendment in the RFP document. In case of failure to get the amendments, if any, C-DAC shall not be responsible.

In order to allow prospective Bidders a reasonable time to take the amendment into account in preparing their Bids, C-DAC, at its discretion, may extend the deadline for submission of Bids. Such extensions shall be uploaded on C-DAC's website.

1.9.12. Bid Price

Financial Bid shall be as per the format provided in the RFP. Bidders shall give the required details of all applicable taxes, duties, other levies and charges etc. in respect of direct transaction between C-DAC and the Bidder.

Bidders shall quote for the entire scope of contract on an "overall responsibility" basis such that the total Bid Price covers Bidder's all obligations mentioned in or to be reasonably inferred from the bidding documents in respect of providing the product/services.

Prices quoted by the Bidder shall remain firm during the entire contract period and not subject to variation on any account. A Bid submitted with an adjustable price quotation shall be treated as non-responsive and rejected. The applicable rates of GST for each line item must be mentioned separately.

1.9.13. Deviations and Exclusions

Bids shall be submitted strictly in accordance with the requirements and terms & conditions of the RFP. The Bids with deviation(s) to the clauses and/or outlined scope mentioned in the RFP and/or non-submission of required documentations are liable for rejection.

1.9.14. Total Responsibility

Bidder should issue an undertaking for taking total responsibility for the defect free operation with effective SLAs of the proposed solution as per the format mentioned in **Annexure 8**.



1.9.15. Late Bids

- a. Bids received beyond the submission date and time mentioned in this RFP shall summarily be rejected and not considered for evaluation.
- b. The Bids submitted by telex/telegram/fax/e-mail etc. shall not be considered. No correspondence shall be entertained in this regard. Bids submitted only in accordance with the procedures and guidelines laid down in this RFP shall be considered valid and due for evaluations.
- c. C-DAC shall not be responsible for any non-receipt/non-delivery or delay in delivery of the documents due to technical snag whatsoever at Bidder's end, No correspondence regarding such non-submissions shall be entertained.
- d. C-DAC reserves the right to modify and amend any of the above-stipulated condition/criterion.

1.9.16. Right to Terminate the Process

C-DAC may terminate the RFP process at any stage during the bidding process and without assigning any reason whatsoever. C-DAC makes no commitments, express or implied, that this process guarantees any Bidder the allotment of this project in question. This RFP does not constitute an offer by C-DAC.

1.9.17. Non-Conforming bids

A Bid may be construed as a non-conforming bids and ineligible for consideration:

- a. Non-Compliance of any clause(s) of this RFP.
- b. If a Bid does not follow the format requested in this RFP or does not appear to address the particular requirements of the solution.

1.9.18. Acceptance/ Rejection of Bids

- a. C-DAC reserves the right to reject in full or part, any or all Bids without assigning any reason thereof. C-DAC reserves the right to assess the Bidder's capabilities and capacity. The decision of C-DAC shall be final and binding.
- b. Bid should be free of over writing. All erasures, correction and/or addition must be clearly written and duly attested.

In the event of any assumptions, presumptions, key points of discussion, recommendation or any points of similar nature submitted along with the Bid, C-DAC reserves the right to reject the Bid and forfeit the EMD.

If there are any discrepancies in the Financial Bid, it shall be subjected to the following:

- a. If, in the Price Bid structure quoted for the required goods/services/works, there is any discrepancy between the unit price and total price (which is obtained by multiplying the unit price by the quantity), the unit price shall prevail and the total price corrected accordingly.
- b. If there is an error in a total corresponding to the addition or subtraction of subtotals, the subtotals shall prevail and the total shall be corrected.
- c. If there is a discrepancy between words and figures, the amount in words shall prevail.
- d. Any discrepancies found in the offer may be intimated to the Bidder and C-DAC may request the Bidder requesting clarification for the same within a stipulated



timeframe. C-DAC reserves all the rights to take appropriate decisions as it may deem fit upon receiving the clarifications for such discrepancies. The decision taken by C-DAC on such matter(s) or otherwise shall be final and binding.

1.9.19. Confidentiality

All the material/information shared with the Bidder during the course of this procurement process as well as the subsequent resulting engagement following this process with the successful bidder, shall be treated as confidential and should not be disclosed in any manner to any unauthorized person under any circumstances. The employees of the successful Bidder and JV Members who are proposed to be deployed on the Project need to furnish a Non-Disclosure Agreement (NDA).

1.9.20. Bid Disqualification

The Bid is liable to be disqualified/ a proper explanation may be called in the following cases or in case Bidder fails to meet the bidding requirements as indicated in this RFP:

- a. During validity of the Bid, or its extended period, if any, the Bidder increases its quoted prices;
- b. The Bidder's Bid is conditional and has deviations from the terms and conditions of RFP;
- c. Bid is received in incomplete form;
- d. Bid is not accompanied by all the requisite documents;
- e. Information submitted in Technical Bid is found to be misrepresented, incorrect or false, accidentally, unwittingly or otherwise, at any time during the processing of the contract (no matter at what stage) or during the tenure of the contract including the extension period if any;
- f. Financial Bid is enclosed with the same document as Technical Bid;
- g. Bidder tries to influence the Bid evaluation process by unlawful/corrupt/fraudulent means at any point of time during the Bid process;
- h. In case any one of the parties of the JV [Lead and/or the JV member(s)] submits multiple Bid(s) or if common interests are found in two or more Bidders, the Bidders are likely to be disqualified, unless additional Bids/Bidders are withdrawn upon notice immediately;
- i. If any of the Member Bidder of any JV is also a member in any other Bid, then all the affected Bids shall be disqualified.

1.9.21. Fraud and Corrupt Practices

- a. The Bidders and their respective officers, employees, agents and advisers shall observe the highest standard of ethics during the Selection Process. Notwithstanding anything to the contrary contained in this RFP, C-DAC shall reject a Bid without being liable in any manner whatsoever to the Bidder, if it determines that the Bidder has, directly or indirectly or through an agent, engaged in corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice (collectively the "Prohibited Practices") in the Selection Process. In such an event, C-DAC shall, without prejudice to its any other rights or remedies, forfeit and appropriate the EMD, as mutually agreed genuine pre-estimated compensation and damages payable to C-DAC for, inter alia, time, cost and effort of C-DAC, in regard to the RFP, including consideration and evaluation of such Bid.



- b. Without prejudice to the rights of C-DAC under Clause above and the rights and remedies which C-DAC may have under the LOI or the Agreement, if a Bidder is found by C-DAC to have directly or indirectly or through an agent, engaged or indulged in any corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice during the Selection Process, or after the issue of the LOI or the execution of the Contract such Bidder shall not be eligible to participate in any tender or RFP issued by C-DAC during a period of 3 years from the date such Bidder is found by C-DAC to have directly or through an agent, engaged or indulged in any Prohibited Practices.
- c. For the purposes of this Section, the following terms shall have the meaning herein after respectively assigned to them:
- “corrupt practice” means (i) the offering, giving, receiving, or soliciting, directly or indirectly, of anything of value to influence the action of any person connected with the Selection Process (for avoidance of doubt, offering of employment to or employing or engaging in any manner whatsoever, directly or indirectly, any official of C-DAC/ Delhi Police who is or has been associated in any manner, directly or indirectly with the Selection Process or the LOI or has dealt with matters concerning the Agreement or arising there from, before or after the execution thereof, at any time prior to the expiry of one year from the date such official resigns or retires from or otherwise ceases to be in the service of C-DAC/ Delhi Police, shall be deemed to constitute influencing the actions of a person connected with the Selection Process); or (ii) save as provided herein, engaging in any manner whatsoever, whether during the Selection Process or after the issue of the LOA or after the execution of the Agreement, as the case may be, any person in respect of any matter relating to the Project or the Award or the Agreement, who at any time has been or is a legal, financial or technical consultant/adviser of C-DAC/ Delhi Police in relation to any matter concerning the Project;
 - “fraudulent practice” means a misrepresentation or omission of facts or disclosure of incomplete facts, in order to influence the Selection Process;
 - “coercive practice” means impairing or harming or threatening to impair or harm, directly or indirectly, any persons or property to influence any person’s participation or action in the Selection Process;
 - “undesirable practice” means (i) establishing contact with any person connected with or employed or engaged by C-DAC/ Delhi Police with the objective of canvassing, lobbying or in any manner influencing or attempting to influence the Selection Process; or (ii) having a Conflict of Interest; and
 - “restrictive practice” means forming a cartel or arriving at any understanding or arrangement among Bidders with the objective of restricting or manipulating a full and fair competition in the Selection Process.

1.9.22. Conflict of Interest

- a. A Bidder shall not have a conflict of interest that may affect the Selection Process or the Solution delivery (the “Conflict of Interest”). Any Bidder found to have a Conflict of Interest shall be disqualified. In the event of disqualification, C-DAC reserves the right to take action as per applicable rules.



- b. C-DAC requires that the Bidder provides solutions which at all times hold C-DAC's/ Delhi Police' interests paramount, avoid conflicts with other assignments or its own interests, and act without any consideration for future work. The bidder shall not accept or engage in any assignment that would be in conflict with its prior or current obligations to other clients, or that may place it in a position of not being able to carry out the assignment in the best interests of C-DAC/ Delhi Police.

1.9.23. Sub-Contracting

The Bidder would not be allowed to sub-contract work, except for the following:

- a. Facility Management Staff at Ground maintenance, Cleaning, Catering, Vending Space management, Utilities management, Site Preparation etc. and associated manpower and site preparation.
- b. Sub-contracting shall be allowed only with prior written approval of C-DAC. However, even if the work is sub-contracted, the sole responsibility of the work shall lie with the Successful Sole Bidder/ JV Bidder. The Successful Bidder shall be held responsible for any delay/error/non-compliance etc. of its sub-contracted vendor.

1.9.24. Right to vary quantity

- a. At the time of award of contract or during the implementation of project, the quantity of goods, works or services originally specified in the bidding documents may be increased/ decreased upto (+/-) 25%. It shall be without any change in the unit prices or other terms and conditions of the Bid and the bidding documents.
- b. If C-DAC/ Delhi Police does not procure any subject matter of procurement or procures less than the quantity specified in the bidding documents due to change in circumstances, the Bidder shall not be entitled for any claim or compensation except otherwise provided in the bidding document.
- c. Repeat orders for extra items or additional quantities may be placed, if it is provided in the bidding document, on the rates and conditions given in the contract if the original order was given after inviting open competitive bids. Delivery or completion period may also be proportionally increased.

1.9.25. Withdrawal, Substitution, and Modification of Bids

- a. No Bid may be withdrawn, substituted, or modified in the interval between the Bid submission deadline and the expiration of the Bid validity period specified by the Bidder in the Bid Submission Form, or any extension thereof agreed to by the Bidder.
- b. Any alteration/ modification in the Bid or additional information supplied subsequent to the Application Due Date, unless the same has been expressly sought for by the Authority, shall be disregarded.
- c. Bids withdrawn shall not be opened and processed further.

1.9.26. Site Visit for preparation of the bid

- The Bidder may wish to visit and examine the site or sites and obtain for itself, at its own responsibility and risk, all information that may be necessary for preparing the bid and entering into the Contract. The costs of visiting the site or sites shall be at the Bidder's own expense.
- It is strongly recommended that bidders may conduct their own studies and surveys as per the requirement of RFP wherever necessary, prior to the proposal submission at their own costs.



- No site visits shall be arranged or scheduled after the deadline for the submission of the Bids and prior to the award of Contract.

(End of Chapter – 1)



Chapter 2. Conditions of Contract

2.1. Special Conditions of Contract (SCC)

2.1.1. Signing of Agreement and Release of Payments

The Agreement for project implementation will be signed between selected bidder (Lead Partner in case of JV) and C-DAC, Pune.

The draft of the Agreement is given in Chapter 6 of this document. However, all the terms and conditions stipulated in this tender shall also be the part of the Agreement to be signed.

All the invoices should be raised in the name of C-DAC Pune. The payments as stipulated in the Contract will be released by C-DAC, Pune on approval of competent authority from C-DAC.

2.1.2. Bid Security/ Earnest Money Deposit (EMD)

The bidder must submit declaration towards EMD / bid security, as given in 'Annexure - 3' subject to the conditions stipulated therein.

2.1.3. Pre-Qualification / Eligibility Criteria

The bidder must comply with the Pre-qualification/Eligibility criteria stipulated below. C-DAC reserves the right to disqualify the bidder in case the bidder does not meet any one or more of the following criteria.

A. Bidder Pre-Qualification Criteria

- a. The Sole Bidder/Each Member of JV must be an entity registered in India under applicable law.
- b. The Sole Bidder / Each Member of JV shall be in operations for a period of at least five (05) years as on published date of RFP.
- c. The annual turnover of sole bidder or the turnover of all JV members put together in each of the last 03 financial year shall be Rs. 300/- Crores.
- d. In case of JV, at least 51% of the turnover criteria shall be met by the Lead Partner (with Management Control in India) and the remaining can be satisfied by the other JV partners.
- e. Sole Bidder or Lead Partner of JV shall have minimum 30% average annual turnover into in the areas of Supply, Implementation and Integration of City Surveillance System and/or, Data Centre infrastructure in last three (03) financial years.
- f. The Sole Bidder or JV Lead partner shall have positive net-worth in the last 03 Financial Year.
- g. All the JV members should have positive net worth as per the audited consolidated financial statements in each of the last 03 financial years.
- h. The sole bidder and all the JV members should be profitable entities at the time of bidding.
- i. The bidder shall not propose any freeware software/community edition as part of ICCS project and thus minimize the chances of severe security risks.



- j. The Bidder shall quote only one specific make and model from only one specific OEM, for each of the goods. Providing more than one option shall not be allowed. All goods quoted by the Bidder must be associated with item code and names and with printed literature describing configuration and functionality. Any deviation from the printed specifications should be clearly mentioned in the offer document by the Bidder.
- k. The MAC address/ Serial Number of the surveillance cameras and other necessary components must be registered in the name of the OEM supplying the equipment's.
- l. Bidder's solution shall adhere to the model framework of cyber security guidelines issued by MeitY (Ministry of IT) from time to time
- m. The Sole bidder or any member of the JV or OEM(s) or its parent company or allied business subsidiary companies should not have been blacklisted/banned/debarred/Non-Performance by GOI/State Govt./PSU/by prominent foreign nations due to security concerns during the last 05 years from the date of publishing the bid. A blacklisted /debarred entity in India or in Prominent Countries shall not be allowed to bid through either any of its Indian subsidiaries/Channels-Partners/Off-shore or Overseas Establishments.
- n. The Sole Bidder or the JV (in case of a JV), should have office in the Delhi/NCR or should furnish an undertaking that the same would be established within one month of signing the contract, if project is awarded.
- o. The Sole Bidder / Each member of JV shall have any one of the following ISO Certifications valid at the time of Bidding:
 - ISO 9001:2008/ 2015
 - ISO 20000:2015 for IT Service Management or equivalent certification
 - ISO 27001:2015 for Information Security Management System or equivalent certification.
- p. The Sole bidder / any JV members should have CMMI level 3 or better certification
- q. The Sole Bidder / Any member in case of JV shall have successfully executed below mentioned projects in last seven years (excluding civil work):
 - At least one order covering Data Center with designed IT load of minimum 30KW excluding redundancy.
 - At least one order/project covering Surveillance projects minimum camera installation base of 500 IP cameras in outdoor environment for a surveillance project with a single Town/City.
 - At least one order covering Surveillance project including surveillance cameras, ICCV, VMS, and Video Analytics Software etc.
 - At least one order of minimum Rs. 05 Cr covering Command and control center/ City Control Room/ Communication Center
 - Orders covering Video analytics/Face Recognition (The cumulative amount of successfully executed orders/projects should be minimum Rs. 02 Crores)
- r. The sole bidder (the Lead bidder and members – in case of JV) must comply with the requirements stipulated in Office Memorandum: F/No/6/18/2019-PPD dated 23rd July, 2020, issued by Public Procurement Division, Department of Expenditure, Ministry of Finance and GoI.
- s. The solution offered must comply with the provisions of Order No P-45021/2/2017-PP (BE-II). Dated 4th June, 2020 issued by Public Procurement Division, Department of Investment and Internal Trade, Ministry of Commerce, GoI read with order number W-43/4/2019-IPHW- MeitY, dated 7th September, 2020 issued by IPWH division of MeitY, GoI



B. Pre-Qualification Criteria for OEMs

- I. OEMs of Camera, VMS, ICCC, AI based Video Analytics Platform, FRS, ANPR should have Presence in India for last five years as on the bid issuance date.
- II. The OEM(s) of Camera, VMS, ICCC should be a profit-making company and should have a positive net worth for last 03 years.
- III. OEM of Server, Storage and networking components should have TAC support centre In India and with Toll Free TAC helpdesk Number.

a. Camera OEMs

- i. OEM should have a minimum cumulative turnover of Rs. 200 Crores in last 02 financial years from the date of opening of tender.
- ii. OEM of IP CCTV cameras should have supplied at least 30,000 IP CCTV cameras in India or globally during the last 05 years
- iii. OEM of IP CCTV camera should have successfully completed at least one order for supply and installation of 1,000 IP CCTV cameras during the last 05 years.
- iv. OEM should have authorized service centre in India
- v. OEM should have ISO certifications: ISO 9001; ISO 14000 & OHSAS 18001;2007/ISO 45001
- vi. Cameras; Camera Firmware; SDK; APIs etc. shall not contain any embedded malicious code which may: -
 - Inhibit the desired and designed functions of the equipment's and Solution.
 - Tap information regarding network
 - There are / will no Trojans, Viruses, worms, Spy wares
 - OEM shall be liable under Information Technology Act, 2000 and Indian Penal Code 1860 in case any Such malicious code in offered / developed software
- vii. Any component/ hardware / parts / assembly / software including firmware used in the offered solution (hardware / software) MUST NOT comply to - GB28181, GB/T 28181-2011; GB/T28181-2011; GBT 28181-2011; GBT28181-2011 standards. Also, the IP CCTV System MUST NOT have CCC.
- viii. OEM should have its own Repair/Service-Support center in the country and must own its RMA set up in India for a minimum of 05 years from the date of submission of bid (not as joint venture, partnership firms or through any other association). In case of product failure OEM should replace malfunction product with equivalent working product immediately till the repaired or alternate product received.
- ix. IP CCTV System OEM for Cameras & VMS must be a member &/or listed in the ONVIF website. The quoted products must be ONVIF compliant not conformant. Online verification of OEM in ONVIF website must be available. No OEM should be banned or suspended by ONVIF within the last five years from the date of publishing the bid.

b. OEM of ICCC

- i. OEM of C4I should have Installation base of at least 05 Safe City Projects / Smart Cities in India or globally during the last 05 years, at least with one project with Bigdata Correlation engine/platform.



- ii. OEM of C4I should have supplied at least 3 + Sub System Integration in single order during the last 05 years in India or globally.
- iii. ICCC should have cyber Security certifications from UL or equivalent from any Indian certifying laboratory
- c. OEM of VMS**
 - i. OEM of VMS should have supplied at least 50,000 cameras Licenses in India or globally in qualifying orders during the last 05 years
 - ii. OEM certifications
 - VMS Should be ONVIF Profile S & G.
 - Should also roadmap of ONVIF Profile T/Q. Declaration for the same to be provided.
- d. AI Based Video Analytics Platform**
 - i. OEM must have supplied AI based Video Analytics platform in minimum 02 Safe Cities/Smart Cities with at least 03 AI based Video Analytics use- cases projects in India and presence from last 05 Years.
- e. OEM of Server**
 - i. OEM must have supplied servers in minimum 02 Safe Cities/Smart Cities projects in India
 - ii. OEM of server should be validated with offered ICCC and VMS software with minimum one year of existence
- f. OEM of Storage**
 - i. OEM should have successfully completed at least one order for supply and installation of minimum 08 PiB scale out NAS Storage in India.
- g. OEM of UPS**
 - i. Offered Product should be OEM own Designed, Developed & Manufactured, OEM should have certificate of incorporation in INDIA for >10 Years
 - ii. At least one order covering minimum installation base of 1000 outdoor UPS for a project.
 - iii. OEM Should have ISO 9001 or ISO 14001 certificate for Manufacturing facility from reputed Agency.
 - iv. OEM Should have annual turnover of > 100 CR for consecutive 03 Years and same should be authorize from Reputed Agency.
 - v. OEM should have its own Repair/Service-Support center in India from the date of submission of bid (not as joint venture, partnership firms or through any other association). In case of product failure OEM should replace malfunction product with equivalent working product immediately till the repaired or alternate product received.

Notes:

- i. Bidders are advised to submit necessary and sufficient documents in support of eligibility criteria stipulated above.
- ii. C-DAC reserves the right to contact the concerned authority of the client/ end user for verification of the Orders/ Contracts referred by the bidder.



- iii. C-DAC reserves the right to award the Contract in compliance with the Make in India Initiative /directives issued by GoI and polices towards MSME.

2.1.4. Exemptions

If in the view of bidder, any exemption/relaxation is/are applicable to them from any of the eligibility/pre-qualification requirements, under any Rules, process, Guidelines, Directives of Government of India, bidder may submit their claim for the applicable exemption/relaxation, quoting the valid Rule, process, Guidelines or Directives. In this case the bidder should submit their request for claiming concession/exemption from any particular criteria enclosing the necessary and sufficient valid documents along with the technical bid, in support of their claim.

2.1.5. Opening of Bids

There will be Two Bid-opening events as follows:

Event 1: Opening of Technical Bids (e-packets 1)

The venue, date and time for opening the technical bids shall be as mentioned in the Fact Sheet.

Event 2: Opening of Financial Bids (e-packet 2)

- a. The Financial Bids of only those Bidders will be opened who clear the Pre-Qualification Bid stage AND who score equal to or more than qualifying marks in the Technical Bid stage, as explained in para 2.1.8 given below.
- b. The date and time for opening of Financial Bid would be communicated to eligible Bidders only.

2.1.6. Clarification on Bids

During the Bid evaluation, C-DAC may, at its own discretion, ask the Bidder for any clarification(s) of its Bid. The request for clarification and the response shall be in writing, and no change in the price or substance of the Bid shall be sought, offered, or permitted. C-DAC's decision on the clarification(s) received shall be final and binding.

2.1.7. Tender Evaluation Committee (TEC)

C-DAC shall constitute a Tender Evaluation Committee (TEC) to evaluate the responses of the Bidders. The Tender Evaluation Committee shall evaluate the responses to the RFP and all supporting documents/documentary evidence. Inability to submit requisite supporting documents/documentary evidence by bidders may lead to rejection of their bids.

The decision of the Tender Evaluation Committee in the evaluation of Bids shall be final and binding. No correspondence will be entertained outside the process of evaluation with the Committee. The Tender Evaluation Committee may ask for meetings with or presentation from the Bidders to seek clarifications or confirmations on their Bids.

The Tender Evaluation Committee reserves the right to reject any or all Bids. Each of the responses shall be evaluated as per the criteria and requirements specified in this RFP.



2.1.8. Evaluation Process

The steps for evaluation are as follows:

a. Stage 1: Pre-Qualification

- i. C-DAC shall carry out the preliminary examination of the technical bid documents submitted in e-packet 1 to check the compliance with pre-qualification requirements/ Eligibility Criteria stipulated at para 2.1.3 of Chapter 2 of this document.
- ii. **Each of the Pre-Qualification Criteria mentioned in the RFP is MANDATORY.** In case, the Bidder does not meet any one or more of the criteria, the bid shall be disqualified.
- iii. The detailed technical evaluation of the bids shall be carried out only for the bidders who comply with the pre-qualification Requirements/Eligibility Criteria.

b. Stage 2: Technical Evaluation

- i. "Technical Bid" of only the Bidders who succeed in Stage 1 will be evaluated.
- ii. C-DAC will further evaluate the Technical Bids of the short-listed Bidders to determine whether the Technical Bids are substantially responsive. This evaluation will be based on Quality and Cost Based System (QCBS).
- iii. The QCBS evaluation includes 08(Eight) technical parameters (Parameters A to H) and one Financial parameter (Parameter I). The technical parameters shall carry maximum marks of 100, as detailed below.
- iv. The TEC constituted by C-DAC will be empowered to determine an appropriate marking system for evaluation of bids. The Technical Score (TS) secured by all eligible bidders will be a part of technical evaluation report and will be displayed on CPP Portal, before opening of Financial Bids.

c. Stage 3: Financial Evaluation and QCBS

The Financial bids of only those bidders who secure minimum 15 marks for parameter G of QCBS table AND overall Technical Score of 70% or more will be opened.

The total prices (All- inclusive) quoted by the bidders (as per price bid format) for all the four phases including the warranty charges for 05 years, the O & M charges for three years along with the applicable GST, as per the price bid format will be considered for the purpose of evaluation and comparison of bids.

The Combined Technical and Financial Score (CTFS) will be calculated by assigning the weightage in proportion of 70:30 (70 % weightage for Technical parameters and 30 % weightage for price).

The Combined Technical and Financial Score (CTFS) will be calculated by using following formula:

$$CTFS = 0.7*TS + (0.3)*(Cmin/Cb * 100)$$

Where,

- i. CTFS = Combined Technical and Financial Score (calculated up to two decimal points).



- ii. TS = Technical score for the bidder under consideration.
- iii. Cb = Actual price quoted by the bidder.
- iv. Cmin = Lowest price among the financial proposals under consideration.

d. Technical Parameters for QCBS:

A. Data center Design & successful installation by Bidder

The size of Data Center in a single order in the name of the bidder/any JV member and successfully installed in India, in last 07 years.

Sr. No	Size of Data Centre in KW of IT Load	Marks
1	DC with designed IT load excluding redundancy: up to - 30KW	06
2	DC with designed IT load excluding redundancy: up to - 40KW	07
3	DC with designed IT load excluding redundancy : up to - 50KW	08
4	DC with designed IT load excluding redundancy: up to - 60KW	09
5	DC with designed IT load excluding redundancy: above - 60KW	10

B. Cumulative Number of IP Cameras successfully installed by the bidder/any JV member in outdoor environment in maximum 05 orders.

Sr. No	Cumulative Number	Marks
1	From 500 to 1000	06
2	From 1001 to 1500	07
3	From 1501 to 2000	08
4	From 2001 to 2500	09
5	Above 2500	10

C. Number of orders/projects, each with a min. value of Rs. 05 Cr, successfully completed by the bidder/any JV member for building integrated command and control center (ICCC) in India, in last 07 years.

Sr. No	Number of orders	Marks
1	1	06
2	2	08
3	More than 2	10

D. Previous experience of the bidder/JV Member in implementing the projects using following software's in last 07 Years:

- i. FRS Software
- ii. ANPR Software
- iii. Video Analytics Software

Sr. No	No. of Applications	Marks
1	Any one of the above-mentioned software applications	04
2	Any Two of the above-mentioned software applications	06
3	All of the above-mentioned software application	08



4	Any Two of the above-mentioned software applications using Unified Integrated Platform	10

E. Previous Experience (Orders successfully completed) of the OEM's, ISV's in using following components:

Sr. No	OEM's of	Parameter	Max Marks
1.	Cameras	Deployment of cameras in a City wide / Outdoor Environment project – If Single PO comprises of camera Nos From 1000 up to 2000 cameras – 01 Mark If Single PO of more than 2000 cameras – 02 Mark	02
2.	Field switches	If One project of min. 50 switches – 0.5 Mark If One project of min. 100 switches - 01 Marks	01
3.	Servers	OEM should have supplied at least 20 servers in minimum 01 Safe City/Smart city Projects in Last 05 Years - 01 Mark	01
4.	Storage	OEM should have supplied the Storage for at least 1 Safe /Smart City surveillance projects of at least 10 PB - 01 Mark Storage should be validated with offered ICCC and VMS software with minimum one year of existence -01 Mark	02
5.	ICCC Software	Deployment of ICCC software in a Safe /Smart City surveillance projects of cumulative 1,000 cameras -01 Mark	02
6.		Single user interface for C4i, VMS, Big Data Correlation engine and Video synopsis application – 01 Mark	
7.	VMS Software	Deployment of VMS software in Safe /Smart City surveillance projects of min 2000 to 5000 cameras – 01 Mark	02
8.		Deployment of VMS software in Safe /Smart City surveillance projects of min 5000 above cameras– 01 Mark	
9.	SDK Capabilities offered /ICCC application	Well documented SDK for further developments and integration with 3rd party systems along with online support portal outlining all the 3rd party integrations and 24/7 support on SDK Package to be submitted in 'Undertaking proforma' without any cost implications for 05 Years of project duration and O&M phase – 01 Marks	01
10.	FRS Software	Deployment of FRS software in a Safe /Smart City surveillance projects city wide / Outdoor project of min 50 FRS channels – 01 Mark	01



11.	ANPR Software	Deployment of ANPR software in a Safe /Smart City surveillance projects city wide / Outdoor project of min 100 channels – 01 Mark	01
12.	Video Analytics Software	Deployment of VA software in a Safe /Smart City surveillance projects city wide / Outdoor project of min 100 channels – 01 Marks	01
13.	Unified Platform	Unified platform 02 project deployed and running – 01 marks	01
Total			15

F. Evaluation of the Bid Submitted/ Solution offered

Sr. No	Description	Marks
1	The TEC will evaluate the bidder on the basis of following aspects evident from the bid submitted/ Solution offered: • Level of understanding of the scope of work and all aspects of this project. • Overall project implementation approach, Phase wise scope and overlapping of activities, How time lines could be met, availability of qualified manpower, deployment plan • Availability and utilization of funds, contingency plan • Vendor management and plans for procurement of material, Service & Resource within stipulated timeline • Risk Mitigation Plan/ Strategy/ SLA • Technical specifications of major components of the solution • Whether the solution offered by the bidder meets the mandatory features and functionalities as stipulated in RFP. Whether solution offers something extra? • scalability of proposed solution • Safety and security measures, Reliability of proposed solution • Innovative approaches – towards minimization of B/W requirement, OPEX, time of implementation, additional features of the softwares, any additional suggestion to scale up the objective of the solution without any financial implication • Innovative approaches – towards minimization of B/W requirement, OPEX, time of implementation • Availability of relevant manpower on the role of bidder, capability of bidder to deploy adequate manpower for the project and time schedule for same • Any specific flaw or weakness in the offered solution • Co-ordination with MPLS Service Provider (ISP) to meet the timeline of the project • Plan to Integrate Community Surveillance & Existing Cameras in other projects • SMS Gateway Integration & other Mobile app Integration	20



G. Proof of Concept (POC):

Sr. No	Description	Marks
	Demonstration and outcome of Proof of Concept activity, as mentioned in the Para 2.1.9 of Chapter 2 of this document.	20

H. Credentials of the Bidder:

Sr. No	Description	Marks
1.	The TEC shall also assess the bidder's capability based on following aspects: • Previous experience (own experience & that of JV members) of bidder in the area of - CCTV surveillance system, DC Infrastructure, Use of various surveillance software applications, projects of similar nature and capacity. • Whether offering own applications or bought-out • Awards/ prizes won, success story, noteworthy achievements • The Expertise and size of the team, the bidder has planned to deploy for this projects • Implementation of Large complex network project • Overall assessment of the Technical Committee	05

Note: The bidder should submit the relevant documents in e-packet 1, in support of the criteria stipulated above.

I. Total Price Quoted:

The total price quoted for all the components, equipment's, sub-systems, hardware, software, services, allied/incidental charges, warranty charges, O & M charges, applicable GST, as per scope stipulated in this document shall be considered for computing Combined Technical and Financial Score (CTFS).

2.1.9. PoC Evaluation Guidelines

As a part of bid evaluation process, the bidder must demonstrate the Proof of Concept (PoC) towards the solution offered.

The bidder shall be required to demonstrate the parameters and features as stipulated at para 2.1.10.1 mentioned below. Technical committee will provide technical marks for each component according to the full compliance and successful demonstration of the given parameter and features.

C-DAC reserves the right to summarily reject the bids of the bidders' whose documents found missing or not submitted along with the bid being required for Technical evaluation without giving any prior notice. All Equipment technical and functional specification mentioned should be available in the technical bid and same will be verified during PoC.



2.1.9.1. Approach to be undertaken for the Demonstration of Proof of Concept (PoC)

- PoC site will be allotted to the Bidder by the C-DAC. PoC site as allotted to the bidder should be visited and surveyed. Information about PoC Site will be communicated to Bidder after Opening of Technical Bid.
- All field systems/components/Software installations shall be done post approval from the C-DAC. The field systems/components should be fixed as per PoC requirements and submitted in the Bid.
- Power for the field equipment will be provided by the Bidder.
- Bidder will submit wiring diagram so that in case of any power-supply related issue during the demo, it can be resolved. However, connectivity from the field devices to PoC site is to be arranged by the Bidder.
- Total power capacity for demo equipment including compute infrastructure must be calculated in advance. Feasibility of sourcing utility power from allotted site/room must be checked in advance.
- Power backup via UPS must be provisioned by the Bidder as per site conditions.
- Google Map can be used as GIS map, and field systems/components (or any other asset) locations should be clearly marked on it with live video streaming.
- Bidder shall provide all the documents required for the Acceptance Test Procedure (ATP) as per the PoC details mentioned in here under. C-DAC reserves the right to modify the ATP for PoC as required.

2.1.9.2. Field Components Setup

- PoC must use the same make and model of the field components offered in the Bid.
- The quantity of the field components should be determined based on the site and PoC requirement as mentioned in this document.
- Before installing field components at the allotted field location, the Bidder is required to show each field component to PoC Evaluation team members/Delhi Police, along with BoQ (Make, Model, Serial number and photo of Equipment/OEM label on the respective field components body) at the time of technical presentation.
- All installation of field equipment in PoC (like cameras, JBs, UPS etc.) must be placed on poles, as per actual deployment scenario and Bidder shall arrange the required accessories.
- Cameras must be tested for all lighting conditions.

2.1.9.3. Network Setup

- PoC must use the same make and model of the edge switch offered by bidders in their solution.
- Other than Edge switch, it can use any other L2/L3 switches to connect to Server setup required for PoC setup.
- The network setup must allow exact bandwidth to be provided / measured to each field systems/components.
- Bidder shall take out real-time bandwidth/network utilization reports from the setup.
- The bidders should use quoted NAC Tool for the demonstration purposes only.



2.1.9.4. Software and Server Setup

A complete setup of following software components but not limited to, is mandatory during the PoC demo:

- a. ICCV Software
 - b. Video Management System
 - c. Under Unified Platform
 - o Video Analytics Platform using use-cases (all mentioned in RFP)
 - o ANPR Application
 - o Facial Recognition System
 - d. Surveillance Cameras
 - e. Mobile Application
 - f. Video Summarization and Analysis
 - g. Edge gateway
 - h. L2 Field Switch
 - i. L3 Switch (10Gb)
 - j. NAC
 - k. EMS
 - l. Servers
- A set of servers (sized appropriately for PoC setup), which are required to install the server-side components of the above-mentioned applications must be made available and installed by the bidder.
 - These details should be provided by Bidder or their OEM partners in the bid.
 - Entire setup should be integrated, configured & tested at before the PoC demonstration as per RFP and PoC requirements as mentioned above in PoC document.

2.1.9.5. Team setup for PoC by bidder

A competent team must be selected and briefed in advance for the PoC demonstration. The team must have the following members:

- i. **PoC Lead and SPOC:** Should be the PoC Manager/Project Manager/Solution Architect as proposed by bidder in their technical bid and responsible to function as chief narrator/demonstrator as well as Single Point of Contact (SPOC). He/she will carry out the complete PoC demo/tour. He/she must have complete control over the PoC and must know the RFP requirements well.
- ii. **Subject Experts:** For each of the components, there can be subject matter experts (SME). These members should be the technical manpower as proposed in the technical bid. These SME may be from OEM partners (if in-house knowledge for that OEM equipment is not sufficient). The respective SMEs of each component is allowed to focus only on their components. Ideally, the following SMEs are required:
 - a. Command and Control Expert
 - b. Security & Surveillance Expert
 - c. Network & Infrastructure Expert
 - d. Server Storage/Database Expert
 - e. MPLS Network Expert (Optical fiber)
 - f. AI based Video Analytics Platform Expert



- iii. **Key Account Manager/Bid Lead:** To answer any query related to the exact offering in the bid (viz-a-viz items offered in PoC)

The PoC Lead should front-end the entire PoC and walk through the entire demonstration. At appropriate points, he/she should hand over the control to the respective SME, to enable demonstration of a particular component (if required).

2.1.9.6. Flow for the PoC

There should be a well-defined flow for the PoC. The flow of the PoC must be briefed through presentation at the start of the PoC, so as to explain about the components and the features that are going to be demonstrated during the PoC.

The aim of the PoC should be functional compliance as well as operational explanation of the system. The focus should be on demonstrating the features of the field systems/components along with their associated software applications that are to be used in actual work-flow of the city monitoring as per RFP. Hence the flow of PoC must be drafted accordingly and PoC must be conducted as per the defined flow and demonstration of field systems/components along with their associated software applications.

2.1.9.7. PoC Setup Document

A document for the PoC setup and presentation must be prepared and presented prior to embarking the PoC. The document must include the following:

- i. **Objective** - To define the objective of the PoC, which are intended to be demonstrated
- ii. **Site planning:** Indicating the location, make, model and quantity of the devices on the field – including GIS Map showing the field systems/components along with their field of view (wherever applicable).
- iii. **Schematic Network Diagram:** How the devices, equipment are connected in the demo area.
- iv. **Bill of Material** (major items) installed for the PoC should be in line with solution components as mentioned above for PoC Technical evaluation. This document should be provided with exact quantity of the hardware, software and networking equipment's etc. as demonstrated.
- v. **List of software** to be used in PoC demonstration.
- vi. **Application Screenshots** - Photographs/screen capture of the various software applications
- vii. **List of Video Recordings supplied** - Camera recordings from all CCTV cameras of PoC should be labelled properly and copied in USB media. The content sheet of the USB media with Demo/PoC/Presentation Proceeding Location, Camera name, Location, Resolution, Start Time, Duration, End-Time, Size of File, Name of File, Status/Remarks.
- viii. **List of Video Analytics/Alarms** -The alarm event logs should be labelled properly and copied in USB media. The content sheet of the USB media to have Camera name, Location, Time, Alarm type, Alarm Result/flag, Status/Remarks.
- ix. **Network Bandwidth observations** -Network bandwidth consumed as observed for the equipment and solutions at various times (e.g. day time, night-time, less



movement in FoV, more movement in FoV, etc.) for different resolution settings at cameras.

- x. **Technical Parameters / Observations** - Technical parameters/Datasheets/ brochures/ literatures of equipment used for PoC for software and hardware demonstrated.
- xi. **Contact Info** - Name, Email and Mobile number of PoC Lead and SME in case any further clarification is required about the PoC.
- xii. Any additional measure to meet the solution requirement and performance by the MSI must be indicated clearly.

2.1.9.8. PoC setup Requirement

The Bidder must consider the hardware and software listed below for PoC and it should be of same make and model as proposed in the bid.

Sr. No.	Component/ Application software	Min. Quantity
1.	Fixed Camera	6
2.	PTZ Camera	2
3.	ANPR Camera	4
4.	L2 Field Switch	4
5.	55"/70" 4K Video Wall	1
6.	L3 Switch (10G)	1
7.	Field UPS	As required
8.	Junction Box / Enclosure	As required
9.	ICCC software	As required
10.	VMS Software	As required
11.	Video Summarization	As required
12.	EMS & Help Desk Dashboard	As required
13.	AI based Video Analytics Platform with Use- Cases	As required
14.	Facial Recognition System	As required
15.	ANPR Software	As required
16.	NAC Tool	As required
17.	EMS Software	As required
18.	Servers (Min. 128GB, 40 cores GPU, CPU)	As required
19.	NAS storage	As required
20.	Any other component/ accessories required for successful PoC Demonstration	As required

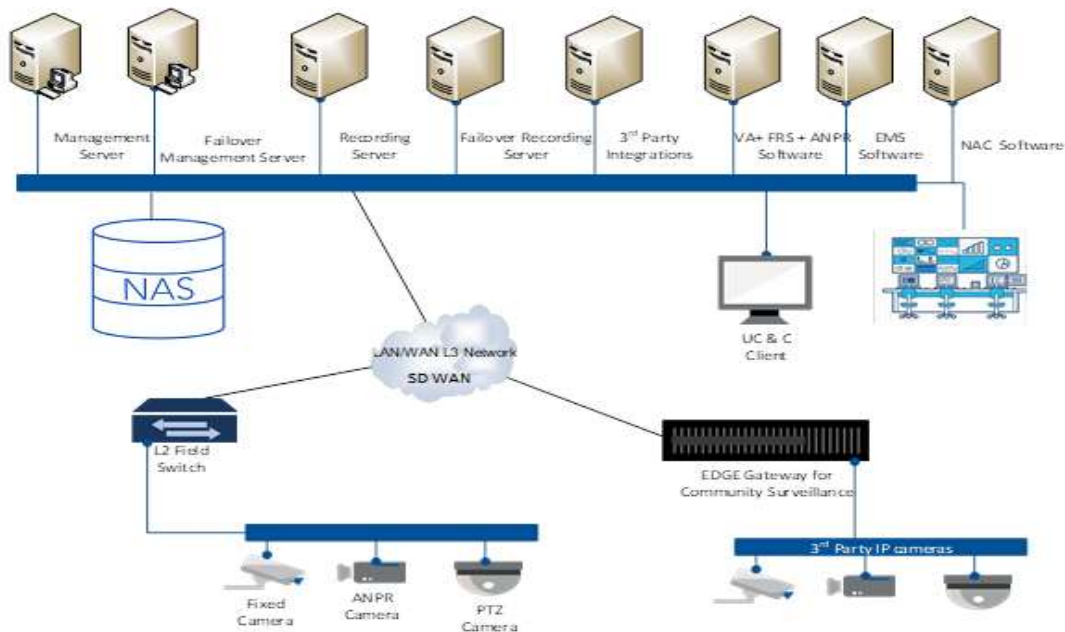
2.1.10. PoC Demonstration – salient points

The PoC demonstration must mandatorily cater to the following salient points:

- i. Major components covered during PoC
- ii. Proficiency of Setting up of the system for PoC
- iii. Proper deployment & integration of System like VMS & ICCC along with Video Analytics Platform and the associated use cases.
- iv. Demonstration of alert cycle management using all associated hardware and software
- v. Demonstration of Incident management and its lifecycle using all associated hardware and software

- vi. Floating of Analytics licenses on multiple cameras using unified platform GUI. Dynamic Deployment and association of Video analytics use cases including FRS and ANPR to various cameras using the AI based Video Analytics platform
- vii. Technical Compliance of the system demonstrated (viz-a-viz RFP specifications)
- viii. Completeness of the PoC document
- ix. Capability of the bidder to respond to the queries raised during the PoC
- x. Additional Systems demonstrated (if any) – bidder can propose any other system/solution in line to the RFP requirement for project benefit.
- xi. Bandwidth Provisioning and verification
- xii. A minimum of 48 streams or better from the cameras and other means available (Min 12 physical cameras) for POC shall be brought on VMS / C4i platform and the same should be routed to analytics software for checking the overall performance of the system in the areas of robustness, availability, analytics accuracy and error handling capacity of the software along with the performance of the overall HW parameters like CPU / GPU, Network etc.
- xiii. Adequacy of the PoC recordings given in CD/DVD/USB Pen-Drive.

Indicative Network Architecture:



The PoC demonstration should primarily cover the following steps at the minimum along with the evaluation framework as mentioned below PoC scope and Technical evaluation parameters.

- i. Introduction of the PoC Team.
- ii. Brief objectives of PoC and flow/steps in which the PoC will progress.
- iii. Summary explanation for the Bill of Material for PoC.
- iv. Inspection of all PoC equipment by the evaluation committee and comparison with Bid proposal.



- v. Actual walk-through of the system covering all components:
 - a. Camera Equipment
 - b. Edge Networking
 - c. Networking and Server information
 - d. Demonstration of location of equipment on GIS map.
 - e. Video Management System & Video Recording
 - f. Storing mechanism of the data / Replication
 - g. Advanced Video Analytics with supportive Artificial Intelligence System software using unified platform, FRS, ANPR
 - h. ICCCC Platform & Big Data mining and Co-Relation engine
 - i. Workflow and Use cases
 - j. NAC Deployment and integration
 - k. Any other features as per RFP, related to PoC items
 - l. Video Summarization and Analysis
 - m. Integration of all subsystems mentioned in the PoC
- vi. Command & Control Centre: The data feeds of the various systems/components configured under the scope of PoC should be displayed at the workstation of Operator (Operator 1) along with the ability to view the camera's live and recorded video feed on Video Wall. The feeds shall be made available for recording and storing at the PoC control centre (software, hardware).
- vii. Dashboard: The operator (Operator 1) shall be able to present the Alert on the geospatially enabled maps in the form of visual & audio. Auto pop-up of alert manager window shall be demonstrated.
- viii. Alerts: Below information to be demonstrated by the Alert Manager:
 - a. Show the target alert
 - b. Time the alert was created
 - c. Description of the alert
 - d. Field Cameras/Systems/Components which created the alert
 - e. It will have provision to facilitate the operator to locate the sensor on GIS map
 - f. Provision to acknowledge the alert
 - g. Provision to close the alert
 - h. Provision to see detailed view which should include
 - o Alert description with timestamps
 - o Live & Recorded video of the camera/data feeds of the other field sensors/systems/components
 - o Map section by displaying the sensors and resources
 - o Standard Operating Procedure (SOP) as mentioned above
- ix. Acknowledgement of the alert by operator (Operator 1) in alert manager
- x. Demonstration of predefined and relevant SOP in the SOP section by operator (Operator 1)
- xi. Demonstration of specifying the custom comments in the appropriate field by operator (Operator 1)
- xii. Demonstration of performing all the tasks specified in the SOP by operator (Operator 1)
- xiii. Reports: Demonstration of generation and receipt of analysed reports from the ICCCC of the system by the operator (Operator).



- xiv. Integration capabilities (VMS + GIS/Maps + ICCV Software + Field Devices + Analytics+ FRS + ANPR)
- xv. Further Steps: Provide response/ clarifications to Technical evaluation committee against their queries as per terms of RFP.
- xvi. Demonstration of ICCV Mobile Application
- xvii. Demonstration of PIU/P-IRIS software features
- xviii. Any Additional component/ software/ product required for successful PoC by MSI
- xix. Photographs and related documents of furniture to be proposed in all Command and Control Centers

NOTE: On completion of POC, the Bidder should dismantle the equipment and remove them from the Location of POC, only when asked by the C-DAC/Technical Evaluation Committee, and not before that.

2.1.10.1. PoC Scope and Technical Evaluation Parameters

A. Camera: ATP Procedure for POC of FIXED camera; PTZ camera & ANPR camera Important Instructions to bidders for POC:

- Quoted models/items/part references must be in operation. No item should be end of life for a minimum period of 8 years from the date of quoting or submitting the bid. An undertaking cum declaration shall be submitted.
- 'Original Certificates' copies duly signed by Power of Attorney (POA) of the respective Bidder/OEM or Managing Director or Company Secretary or Board of Directors. The Original POA copy shall have to be attached/ enclosed or showcased during POC /Technical Bid Evaluation.
- All original Certificates shall have to be furnished during the time of evaluation. All Certificates shall be allowed which are published on or before the publishing of the bid. All Certificates specific to quoted product model / product part reference or product item no. must be submitted (No Series Reference Certificates shall be allowed.).
- UL Certificate must mention the specific model no quoted and shall be available for online for verification. No OEM model series' number or OEM Product Series or Product category specific Certificates shall be accepted.
- Online ONVIF S; G/ Profile S, G, T must be available for checking & confirmation. Hard copies shall also be submitted
- Third Party Test certificates of IP67; IK -10; NEMA -4X must be provided. No Self Declaration shall be admissible.
- CE, FCC, UL/cUL, BIS Certificate must be submitted along with the Bid Document.

B.1. Outdoor Fixed Camera - 4MP

Sr. No	Parameters	Specifications	Method for Testing during POC	Demonstrated / Submitted & Verified
A 1	OFFLINE PARAMETERS' POC - TEC/ATP			
	Image Sensor	1/3" Progressive Scan CMOS Sensor or better	Technical sheet/Product Manual/OEM Declaration of Compliance on Letter	Data of



2			Head or all duly signed by POA as required. POA copy to be enclosed with Bids	
	Lens	2.8mm – 12mm Lens, Auto / DC / P-Iris or better, Varifocal	Technical Data sheet/Product Manual/OEM Declaration of Compliance on Letter Head or all duly signed by POA as required. POA copy to be enclosed with Bids	
	3	Wide Dynamic Range	True WDR of 120dB or better	
	4	Minimum Illumination	Color: 0.01Lux @f/1.6 or better	
	5	IR Filter	Automatic Built-in IR Cut Filter	
	6	ONVIF Profile	S & G/ S,G,T	
	7	Operating Temperature	-30 °C ~ 60 °C, Up to Humidity 90%	
	8	Housing	IP67 and IK10 rated for Outdoor Housing	



B 1	9	Certification	CE, FCC, UL/cUL, BIS, NEMA 4X	duly signed by POA as required. POA copy to be enclosed with Bids. Original reports shall also be showcased.	
	10	EMI EMC	Surge test (Level 4) as per IEC:61000- 4-5(Level 4)	Third Party Test certificates/Reports being duly signed by POA as required. POA copy to be enclosed with Bids. Original reports shall also be showcased.	
	11	MTBF	Min 100000 Hours or better	Third Party Test certificates/Reports being duly signed by POA as required. POA copy to be enclosed with Bids. Detailed Lab Test report and certified original report must be showcased and submitted.	
	12	Misc.	The Camera to be provided by the OEM/bidder should not be complying to GB28181, GB/T28181-2011 standards and there should be no option to activate or deactivate GB/T 28181 standards in the camera web page/settings.	Technical Data sheet/Product Manual/OEM Declaration of Compliance on Letter Head or all duly signed by POA as required. Factory Test Certificate shall be submitted. POA copy to be enclosed with Bids	
		Maximum Image Resolution	2688 X 1520 or better	Technical Data sheet/Product Manual/OEM Declaration of Compliance on Letter Head or all duly signed by POA as required. Factory Test Certificate shall be submitted. POA copy to be enclosed with Bids.	
				In the Camera browsing window, the variable resolution should get reflected and able to define	



2			the viewing resolution as per requirement up to 4MP or better	
	IR	50mtrs or better to be considered internal or external	Able to detect & identify a human / object / vehicle from 50mtrs away from the Camera location during night time	
	3	Shutter Speed	Auto / Manual, 1/3s ~ 1/30000s or better	
	4	Image Quality	Support Object Distance at the end of 50mtr during day and as well as night	
	5	Video Streaming	Triple Streaming Supported or Individually configurable minimum 03 video streams	
	6	Video Compression	H.265, H.264 (Dynamic group of pictures) or better	
	7	Local Storage	SD Card slot with 128GB or better support with provided 128 GB card	
	8	Image Settings	Color, Brightness, Sharpness, Contrast, White balance, Backlight compensation, Image Mirroring, Text and image overlay, BLC/HLC/AGC required	
	9	Supported Protocol	HTTP, HTTPS/SSL/TLS, TCP, ICMP/RTSP, RTP, UDP, IGMP, RTCP, SMTP, FTP, DHCP, UPnP/ARP/DNS,	



10		SMTP, Ipv4/Ipv6, ONVIF		
	Security	SSL & TLS; SSH; HTTPS; 802.1x NAC; Multiple EAP methods; AES/DES	Shall be tested in conjunction with proposed VMS by installing SSL Certificate for triggering the TLS to figure out the data security.	
	11	Manufacturer Authenticity	MAC ID & Firmware Authenticity; non-compliance to GB28181, GB/T28181-2011	
			An online inspection shall be done through in conjunction with necessary offline documents by using third party tools to determine the Duplicate MAC Address Detection, if any. So also, the online authenticity of Firmware shall be checked to determine if it's a malicious or modified or duplicate coded. A live investigation shall be conducted with specific tools to verify the non-compliance of GB28181, GB/T28181-2011.	
	12	SD Card recording	Offline Recording	The POC must establish the SD recording proof in-conjunction with quoted VMS by Bidder.
13	Seamless Server Based Analytics Integration	Video Analytics' POC Integration	The POC must establish the various type of video analytics as per RFP integration for live & recording proof in-conjunction with quoted VMS & Video Analytics System by Bidder.	



B.2. Outdoor PTZ Camera - 4MP, 30x Optical Zoom and Joystick control operations

Sr. No	Parameters	Specifications	Method for Testing during POC	Demonstrated / Submitted & Verified
A	OFFLINE PARAMETERS' POC - TEC/ATP			
	1	Image Sensor	1/3" CMOS Sensor min 4MP or better	Technical Data sheet/Product Manual/OEM Declaration of Compliance on Letter Head or all duly signed by POA as required. POA copy to be enclosed with Bids
	2	Focal Length	4.5 mm - 135 mm or 4.3 mm - 129 mm or 4.8 mm - 144 mm or 6mm -180 mm	Technical Data sheet/Product Manual/OEM Declaration of Compliance on Letter Head or all duly signed by POA as required. POA copy to be enclosed with Bids
	3	Wide Dynamic Range	True WDR 120dB or better	Technical Data sheet/Product Manual/OEM Declaration of Compliance on Letter Head or all duly signed by POA as required. POA copy to be enclosed with Bids
	4	Minimum Illumination	Color: 0.01Lux @f1.6 or better	Technical Data sheet/Product Manual/OEM Declaration of Compliance on Letter Head or all duly signed by POA as required. POA copy to be enclosed with Bids
	5	Zooming Capacity	Optical: 30X or better Digital: 16X or better	Technical Data sheet/Product Manual/OEM Declaration of Compliance on Letter Head or all duly signed by POA as required. POA copy to be enclosed with Bids
	6	PAN & TILT Speed	Manual: 180°/s Preset: 240°/s & Manual: 120°/s Preset: 200°/s	Technical Data sheet/Product Manual/OEM Declaration of Compliance on Letter Head or all duly signed by POA as



7			required. POA copy to be enclosed with Bids	
	MTBF	Min 80000 Hours or better	Technical Data sheet/Product Manual/OEM Declaration of Compliance on Letter Head or all duly signed by POA as required. Factory Test Certificate shall be submitted. POA copy to be enclosed with Bids	
	ONVIF Profile	S & G/S,G,T	Online ONVIF S; G/ Profile S, G, T must be available for checking & confirmation. Hard copies shall also be submitted duly signed by POA as required. POA copy to be enclosed with Bids	
	Operating Temperature	-30 °C ~ 60 °C, Up to Humidity 90%	Technical Data sheet/Product Manual/OEM Declaration of Compliance on Letter Head or all duly signed by POA as required. POA copy to be enclosed with Bids	
	Housing	IP67 and IK10 rated Outdoor Housing	Third Party Test certificates/Reports being duly signed by POA as required. POA copy to be enclosed with Bids. Original reports shall also be showcased.	
	Certification	CE, FCC, UL/cUL, BIS, NEMA 4X	Third Party Test certificates/Reports being duly signed by POA as required. POA copy to be enclosed with Bids. Original reports shall also be showcased.	
12	EMI EMC	Surge test (Level 4) as per IEC:61000- 4-5(Level 4)	Third Party Test certificates/Reports being duly signed by POA as required. POA copy to be enclosed with Bids. Detailed Lab Test report and certified original report must be showcased and submitted.	



13	Misc.	The Camera to be provided by the OEM/bidder should not be complying to GB28181, GB/T28181-2011 standards and there should be no option to activate or deactivate GB/T 28181 standards in the camera web page/settings.	Technical Data sheet/Product Manual/OEM Declaration of Compliance on Letter Head or all duly signed by POA as required. Factory Test Certificate shall be submitted. POA copy to be enclosed with Bids.	
B	ONLINE PARAMETERS' POC - TEC/ATP			
1	Maximum Image Resolution	2592 × 1520 (4MP) or better	In the Camera browsing window, the variable resolution should get reflected and able to define the viewing resolution as per requirement up to 4MP or better	
2	IR Distance	150mtrs or better	Able to detect & identify a human / object / vehicle from 150mtrs away from the Camera location during night time	
3	Image Quality		Support Object Distance at the end of 150mtr during day and as well as night	
4	Video Streaming	Triple Streaming Supported or Individually configurable minimum 03 video streams (Multicasting)	Able to view multiple streaming configurations via Camera web browsing window	
5	Video Compression	H.265, H.264, or better	Able to view multiple streaming configurations via Camera web browsing window	
6	Preset	256 or better	Able to view multiple streaming configurations via Camera web browsing window	
7	Local Storage	SD Card slot with 128GB or better support with	Able to view the local storage capacity via web browsing of Camera	



8		provided 128 GB card		
	Defog	Digital defogger/defogger	Able to view and configure variable image settings via we browsing of Camera	
9	Supported Protocol	IPv4/IPV6, HTTP, HTTPS, FTP, SMTP, UPnP, SNMP, DNS, DDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, ICMP, DHCP, ONVIF	Compliance for major protocol during live POC shall be tested – ONVIF; RTSP; RTP; DHCP; ARP/DNS; etc.	
10	Security	SSL & TLS; SSH; HTTPS; 802.1x NAC; Multiple EAP methods; AES/DES	Shall be tested in conjunction with proposed VMS by installing SSL Certificate for triggering the TLS to figure out the data security.	
11	Manufacturer Authenticity	MAC ID & Firmware Authenticity; non-compliance to GB28181, GB/T28181-2011	An online inspection shall be done through in conjunction with necessary offline documents by using third party tools to determine the Duplicate MAC Address Detection, if any. So also, the online authenticity of Firmware shall be checked to determine if it's a malicious or modified or duplicate coded. A live investigation shall be conducted with specific tools to verify the non-compliance of GB28181, GB/T28181-2011.	
12	SD Card recording	Offline Recording	The POC must establish the SD recording proof in-conjunction with quoted VMS by Bidder.	
13	Seamless Server Based Analytics Integration	Video Analytics' POC Integration	The POC must establish the various type of video analytics as per RFP integration for live & recording proof in-conjunction with quoted	



			VMS & Video Analytics System by Bidder.	

B.3. Outdoor Fixed ANPR Camera with IR Illuminator- 2MP

Sl. No	Parameters	Specifications	Method for Testing during POC	Demonstrated / Submitted & Verified
A	OFFLINE PARAMETERS' POC - TEC/ATP			
1	Shutter Type	Global shutter sensor or rolling shutter sensor with Image stabilization	Technical Data sheet/Product Manual/OEM Declaration of Compliance on Letter Head or all duly signed by POA as required. Factory Test Certificate shall be submitted. POA copy to be enclosed with Bids	
2	OCR Accuracy	Camera resolutions as needed by the solution to achieve highly reliable results of min 90% + capture and OCR accuracy min 90% in both day and night.	Technical Data sheet/Product Manual/OEM Declaration of Compliance on Letter Head or all duly signed by POA as required. Factory Test Certificate shall be submitted. POA copy to be enclosed with Bids	
3	Image Sensor	1/2" Progressive Scan CMOS Sensor 2.0 megapixel or better CMOS.	Technical Data sheet/Product Manual/OEM Declaration of Compliance on Letter Head or all duly signed by POA as required. Factory Test Certificate shall be submitted. POA copy to be enclosed with Bids	
4	Lens	C/CS or inbuilt with 5- 50 mm; Automatic Built in IR Cut filter	Technical Data sheet/Product Manual/OEM Declaration of Compliance on Letter Head or all duly signed by POA as required. Factory Test Certificate shall be submitted. POA copy to be enclosed with Bids	
5	Wide Dynamic Range	True WDR 120dB or better	Technical Data sheet/Product Manual/OEM Declaration of Compliance on Letter Head or all duly signed by POA as	



6			required. Factory Test Certificate shall be submitted. POA copy to be enclosed with Bids	
	Minimum Illumination	Color: 0.001Lux @f/1.6 B/W: 0.001Lux @f/1.6 Or better	Technical Data sheet/Product Manual/OEM Declaration of Compliance on Letter Head or all duly signed by POA as required. Factory Test Certificate shall be submitted. POA copy to be enclosed with Bids	
7	Maximum Image Resolution	1920 X 1080	Technical Data sheet/Product Manual / OEM Declaration of Compliance on Letter Head or all duly signed by POA as required. Factory Test Certificate shall be submitted. POA copy to be enclosed with Bids	
8	MTBF	Min 100000 Hours or better	Technical Data sheet/Product Manual/OEM Declaration of Compliance on Letter Head or all duly signed by POA as required. Factory Test Certificate shall be submitted. POA copy to be enclosed with Bids	
9	ONVIF Profile	S & G/S,G.T	Online ONVIF S; G/ Profile S, G, T must be available for checking & confirmation. Hard copies shall also be submitted duly signed by POA as required. POA copy to be enclosed with Bids	
10	Operating Temperature	-30 °C ~ 60 °C, Up to Humidity 90%	Technical Data sheet/Product Manual/OEM Declaration of Compliance on Letter Head or all duly signed by POA as required. POA copy to be enclosed with Bids	
11	Housing	IP67 and IK10 rated Outdoor Housing	Third Party Test certificates/Reports being duly signed by POA as required. POA copy to be enclosed with Bids. Original reports shall also be showcased.	



12	Certification	CE, FCC, UL/cUL, BIS, NEMA 4X	Third Party Test certificates/Reports being duly signed by POA as required. POA copy to be enclosed with Bids. Original reports shall also be showcased.	
13	EMI EMC	Surge test (Level 4) as per IEC:61000- 4-5(Level 4)	Third Party Test certificates/Reports being duly signed by POA as required. POA copy to be enclosed with Bids. Detailed Lab Test report and certified original report must be showcased and submitted.	
14	Misc.	The Camera to be provided by the OEM/bidder should not be complying to GB28181, GB/T28181-2011 standards and there should be no option to activate or deactivate GB/T 28181 standards in the camera web page/settings.	Technical Data sheet/Product Manual/OEM Declaration of Compliance on Letter Head or all duly signed by POA as required. Factory Test Certificate shall be submitted. POA copy to be enclosed with Bids.	
B	ONLINE PARAMETERS' POC - TEC/ATP			
1	Maximum Image Resolution	1920 X 1080	In the Camera browsing window, the variable resolution should get reflected and able to define the viewing resolution as per requirement up to 2MP or better	
2	IR Distance	80mtrs, with internal or external IR	Able to detect a human / object / vehicle from 80mtrs away from the Camera location during night time	
3	Shutter Speed	Auto / Manual, 1s ~ 1/30000s or better	Able to define the Shutter Speed from Camera Web Browsing Window	
4	Image Quality		Support Object Distance at the end of 80mtr during day and as well as night	
5	Video Streaming	Unicast, Multicast, Broadcast support along with multi stream support	Able to view multiple streaming configurations via Camera web browsing window	

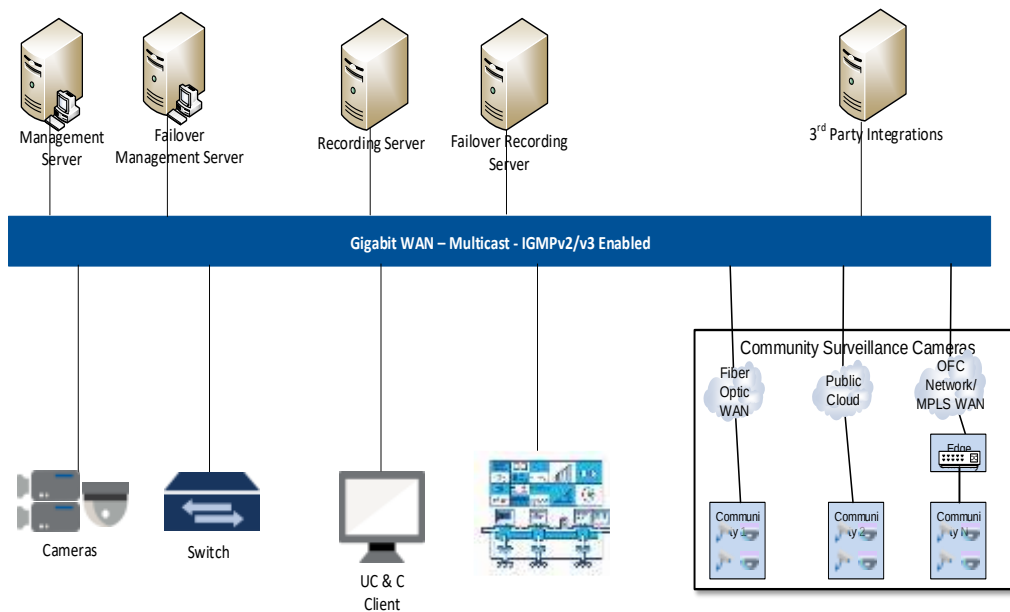


6	Video Compression	H.265, H.264, or better	Able to view multiple streaming configurations via Camera web browsing window	
7	Local Storage	SD Card slot with 128GB or better support with provided 128 GB card	Able to view the local storage capacity via web browsing of Camera	
8	Image Settings	Colour, Anti-glare Brightness, Sharpness, Contrast, White balance, Backlight compensation, Image Mirroring, Text and image overlay, HLC, 3D DNR, Defog, EIS, ROI, AGC, bmp format	Able to view and configure variable image settings via web browsing of Camera	
9	Supported Protocol	HTTP, HTTPS/SSL/TLS, TCP, ICMP/RTSP, EAP-TLS, EAP-MD5, RTP, UDP, IGMP, RTCP, SMTP, FTP, DHCP, UPnP/ARP/DNS/DynDNS, SMTP, Ipv4/Ipv6, ONVIF	Compliance for major protocol during live POC shall be tested – ONVIF; RTSP; RTP; DHCP; ARP/DNS; etc.	
10	Security	SSL & TLS; SSH; HTTPS; 802.1x NAC; Multiple EAP methods; AES/DES	Shall be tested in conjunction with proposed VMS by installing SSL Certificate for triggering the TLS to figure out the data security.	
11	Manufacturer Authenticity	MAC ID & Firmware Authenticity; non-compliance to GB28181, GB/T28181-2011	An online inspection shall be done through in conjunction with necessary offline documents by using third party tools to determine the Duplicate MAC Address Detection, if any. So also, the online authenticity of Firmware shall be checked to determine if it's a malicious or modified or duplicate coded. A live investigation shall be conducted with specific tools	

12	SD Card recording	Offline Recording	to verify the non-compliance of GB28181, GB/T28181-2011.	
			The POC must establish the SD recording proof in-conjunction with quoted VMS by Bidder.	
13	Seamless Server Based Analytics Integration	Video Analytics' POC Integration	The POC must establish the various type of video analytics as per RFP integration for live & recording proof in-conjunction with quoted VMS & Video Analytics System by Bidder.	

B. Compliance of the software solutions to the Tender Specifications

Indicative Reference Design:



- MSI has to demonstrate all the features of ICCC and VMS as per specification.
- Demonstrate the ICCC Software solution for multi-monitor displays (2*2 Displays).
- Integration SOP for other software.



B.1. ICC

Sr. No	Parameters	Method for Testing during POC	Demonstrated / Submitted & Verified
1.	User Interface and operator Simplicity	Demonstrate the UC & C operator interface covering the below aspects of the specification a. Overall C4I interface for configurations of the overall system, Privilege management, Configurations for ingesting 3rd party systems like Video analytics, Synopsis etc. b. Interface for Live, Recording, playback and Video related alarms and events interface from UC&C module. c. Troubleshooting tools for various sub systems in the areas of VMS, Analytics, Video Synopsis, Network layer, Cameras, Cyber security etc. connected with the UC & C module. d. Flexibility to configure, manage and monitor operator screens and functionalities based on the operator type. For ex, configuring the system for PTZ access or certain camera access only to certain type of operators / analysts. More use cases must be demonstrated around the flexibility of the configurations and how those configurations would impact the operator interface in real time Command Center	
2.	Reliability and Failover	Demonstrate the Native failover capabilities of the UC & C Platform, Clients connection and its impact during the failure, Impact on the Database and re connection, Switch over time between the primary and secondary servers and impact and Automatic recovery of the system with no manual intervention when the Primary DC is up and operational	
3.	Single User Interface	Demonstrate the UC & C interface capabilities for all the other sub systems including the VMS, Incident management, Alarm management, 3rd party meta data, Video synopsis from UC & C interface etc.	
4.	3rd party device support	Demonstrate the user interface to support configure, manage, and monitor 3rd party devices like Cameras, communication devices,	



		operator to operator voice communication interface etc.	
5.	3rd party software integrations and architecture	a. Explain / Demonstrate the architecture adopted for 3rd party systems integrated via the SDK and Cyber security methods adopted to keep the integration secure using the methods of TLS / Digital certificates as outlined in the RFP specification. b. Explain how the life cycle management is maintained the system reliability is maintained between the systems when any future software upgrade is made in the UC & C module or its sub systems including the 3rd party applications like VMS, Big data core relation engine, Analytics, Video synopsis SW etc.	
6.	Situational Awareness module (Maps)	a. Demonstrate the online GIS and Offline map capabilities of the UC & C module, configuration capabilities and how simple the interface is to configure the Maps, plotting of edge devices like cameras etc. both on GIS and offline Maps link to GIS in the format PDF or JPEG. b. Drill down capabilities of the maps from GIS to offline maps all the way to floor level. c. Alarm management capabilities from maps and ease of operator navigation. d. Automatic map locations being pointed and highlighted for specific alarms. e. Live and Playback of CCTV cameras from Map interface both online and offline. f. Pinning capabilities for cameras of interest specific for investigations. g. PTZ controls of cameras from MAP interface. h. Camera Field of View capabilities from UC & C Map interface	
7.	UC & C Alarm and Events management capabilities	a. Demonstrate the capabilities of alarm management with in UC & C interface both native and from 3rd party systems like Video Analytics, FR, Video synopsis etc. b. Demonstrate the capabilities for configuring various types of alarms / events both for automatic and manually created alarms. c. Demonstrate the priority settings for each alarm type, Recipients of all alarms of specific alarm type, Automatic associated / nearest camera pop up for both Live and	



		playback specific to the alarm, alarm thresholds, and Assign a time schedule or a coverage period to an alarm, auto acknowledgment of certain type of alarms. d. Demonstrate automation capabilities like auto video recording from UC & C interface upon specific type of alarms being triggered for ex Potential suspect face detected, accident, crowd gathering etc. e. Demonstrate the native tools available to protect critical alarms stored beyond the default configured storage period for longer retention time for Judicial and investigation purposes. f. Demonstrate the Notification capabilities of alarms which provides controls that operator can use to sort and filter the messages that it displays along with custom colors and sounds configured for specific alarm type. g. Demonstrate export functionalities of Alarms / critical events and all other associated data to that specific alarm through email or messaging. h. Demonstrate the PTZ patters / zoom capabilities from UC & C interface for specific alarms For Ex, Analytics alarm for Chain snatching triggered from VA provider, SOS calls, PTZ camera pattern auto focused on the alarm / situation.	
8.	Incident management Capabilities	a. Demonstrate the map-centric (Both online and offline maps) approach and detailed overview of incident data, combining incident history, operator comments, workflow and operator action logs, standard operating procedures, relevant live and playback video, and an aggregated events sequence of the incident. b. Demonstrate the Criticality of the Incident qualified from an Alarm / Event natively or from 3rd party systems like VA, FR etc. c. Demonstrate the Automatic and Manual incident triggers using both MAP and Non-Map interface with in UC & C. d. Demonstrate the native Rule engine configuration and simplicity for configuring the IF / Then / ELSE / OR/ BOOLEAN logics for qualifying alarms and incidents for	



		operators. Demonstrate using a use case like Missing object or Camera tempering etc. to show the rule engine effectiveness and its impact on the false alarms. e. Demonstrate the ownership capabilities of the Alarms / Events and qualified for an incident within UC & C interface, request or release the ownership of an incident. f. Demonstrate guidance for operators in the form of a standard operating procedure (SOP) for the response to an incident type. g. Demonstrate the following as outlined in the specification – - Change the incident state. - Forward the incident. - Transfer the incident to different stake holder or operator. - Edit the incident - Attach additional supporting data like Camera footage etc. related to specific to the incident. - Link other similar related incidents. - Attach a document as a URL link to the incident for postmortem - Link / protect the flagged incident data from deletion for post investigation and judicial purposes. - Min 2 end to end use cases demonstrating the overall alarm management / Incident management capabilities of the platform. - Demonstrate the overall Incident reporting, storing and retrieval of the reports on need basis. - Demonstrate the overall incident export capabilities for the 2 Use cases showcased under Point i, with all the associated information related to the incident from cameras, recorded footage, PDF documents, location of the incident etc. as a part of Incident report along with encryption capabilities. - All the other features as outlined in the RFP specification	



9.	BDCR Use cases	a. Demonstrate the ease of configuration for the BDCR tool from UC & C interface. b. Integrated / interface with Min 4 - 5 data sources can be simulated for Crime related data sources and live for CCTV data source and demonstrate the Co Relation / Data Mining capabilities from UC & C platform. c. Demonstrate an end to end use case situation on how the Co Relation tool functions to specific incident like CAD Call and how the data being presented from different sources relevant to the specific incident type. d. Demonstrate the Co Relation tool capabilities based on Geo location / Distance and time of incident in mining the data from various data sources and presenting in a single pane of glass for investigation purposes. e. Demonstrate all the reporting / dashboarding capabilities within the UC & C interface. f. Demonstrate all the other features as outlined in the RFP related to BDCR tools.	
10.	Reporting Capabilities	Demonstrate all the reporting capabilities as sought in the RFP in dashboard formats covering the Health status of the devices, Operators connected, 3rd party devices connected, Real time alarms, Live incidents, Cyber Security parameters etc. from the UC & C interface	
11.	Proactive Intelligence tools	a. Demonstrate the ease of configuration and management of proactive threat activation tools within UC & C interface. b. Activate a specific Alarm / threat from UC & C or Mobile interface and demonstrate the proactive action system can take for specific action related to the threat activated. For Ex, Bomb alert, Suspicious package / object detection etc.	
12.	Mobile App	a. Demonstrate the secure link / Cyber Security hardening capabilities between the Mobile app and Central UC & C servers. b. Demonstrate the ability to navigate the Mobile app using the GIS map interface c. Demonstrate the live and playback of recorded video footages of nearest cameras	



		from Mobile app through the tile or GIS view from the UC & C interface d. Demonstrate the Alarm management capabilities from the app e. Demonstrate the collaboration / tracking capabilities with in Mobile app. f. Demonstrate the threat level activation and de activation capabilities from the mobile app. g. Stream live video using Mobile app from UC & C interface to Command center, activate the workflow / SOP procedure upon detection of such activity for further investigation / incident management. h. Demonstrate all the other Mobile app capabilities.	
13.	External integration capabilities	a. Explain the 3rd party systems integrated, methodology. b. SDK documentations, Support structure and Methodology.	
14.	Cyber Security Use cases.	a. Demonstrate the end to end communication protocols methodology between the servers, Clients, Mobile app, and 3rd party systems. b. Demonstrate possible encryption methods for Data storages and export. c. Demonstrate the Recorded footage and Live monitoring watermarking Capabilities. d. Demonstrate the dashboard capabilities to track the Cyber Security status of the system deployed. e. Demonstrate the tools available for Automatic / Schedule patch / SW upgradation for the UC & C platform. f. Demonstrate the online / offline Cyber Security response capabilities	



B.2. VMS

Sr. No	Parameters	Method for Testing during POC	Demonstrated / Submitted & Verified
1.	Openness	Demonstrate the openness of the system by connecting different make of cameras. Auto discovery of cameras attached to the network, assign multiple schedules to a single / group of cameras.	
2.	Monitoring	Demonstrate the following monitoring functionalities: - Single Camera View - Various Tile Grid View – 1x1 to 8x8 - Camera Sequence view - Change / set specific tile patters for operators based on their user privileges. - Verify the live monitoring on Video Wall. - Live, Playback and pinning of critical cameras from Map Interface for both GIS and Offline maps. - Tile and Map view in single user interface. - Tree view of all cameras connected with in operator interface and easy drag and drop with live and playback view of respective cameras. - Demonstrate camera from Community feeds for all 3 possible design as outlined in the RFP in single plane of view in the operator interface. - Native tools with live data to trouble shoot camera streams, network traces, packet loss, layers of packet loss, bandwidth consumed etc. all with in the operator interface. - Native tools to bookmark important events / events for later retrieval on any recorded camera and to uniquely name each bookmark in order to facilitate future searches for easy investigation from operator interface.	
3.	PTZ Functionalities	Demonstrate the overall PTZ functionalities. - PTZ Coordinates Set Zero Position and obtained from camera. - PTZ Specific Commands - PTZ Free Look Mode Zooms with Mouse wheel	



		d. PTZ pan, tilt, zooms with the PTZ Widget e. PTZ - on tile - Arrow icon, Iris Close/Open, Focus Near/far f. Edit PTZ presets g. Verify PTZ tour / patterns h. PTZ - Calibration tool	
4.	Recording	Demonstration of the following features. a. Display playback video from different reports from recording servers, bookmark data, motion-based alarms etc. b. Digital Zoom functionality for both PTZ and Fixed cameras. c. Slow motion (forward and reverse) d. Fast forward (all speeds) e. Rewind (includes smooth reverse playback) f. Previous and next frames navigation g. While in playback mode, seek two different places within the timeline h. Synchronize more than one tile in playback i. Demonstrate the edge recording within camera and automatic recording being filled when there is a network disconnect between the cameras and Central recording servers. j. Native tools to protect video data from deletion based on policies defined, applicable mainly for the flagged data and critical incident data use cases. k. Native tool to take snapshots of live video and be able to save or print the snapshots, associate the same to specific alarm or incident from Operator interface. l. Native tool to browse through a list of all bookmarks created on the system and select any bookmarked event for viewing/ investigation	
5.	Multicast Support	Demonstrate the end to end multicast capabilities for following: a. Camera configured with Multicast and demonstrate the camera access from multiple client stations the same stream over Multicast with no dependency on the recording server 's.	
6.	Reliability and Native Failover	Demonstrate the Native failover capabilities without using any third-party application or windows cluster for the following applications: a. Demonstrate the Recording server failover and its impact on the Video footages	



		recorded. Playback to check for any video loss during such failover and fall back in recording servers.	
7.	Camera Authentication Scheme	Demonstrate the following use cases for Camera Authentication configured based on the rules configured - a. Operator Interface not being allowed to add video units if basic authentication is enabled in the camera. b. Operator interface can define password policy for cameras and user interface providing insights if the same policy is not followed during the configuration of the cameras. c. Operator Interface Validate that cameras password can be changed directly from the VMS client all at once or individually. d. Operator interface having the ability to notify for new camera Firmware and upgrading the camera firmware directly from the same operator interface. e. Native tools / system capabilities to handle Brute force attacks for failed logins. f. Native tools to lockdown the operator client after specific time of inactivity g. Native tools to raise alarms / events in the C4i interface if specific or Operator user login being failed and capture as part of Audit trials with in system.	
8.	Forensic search tools	Demonstrate the following Investigation / Forensic tools - a. Demonstrate the capability of video search based on area of interest or object for easy investigation and large recorded video data condensed into small time frame video related to the area of interest or object selected for play back. b. Demonstrate camera to camera tracking tools without manually switching between cameras to track area of interest or possible suspects / people. c. Demonstrate the Video synopsis capabilities within the operator interface. d. Demonstrate the FR capabilities with Metadata overlay for hotlist alarms etc.	
9.	Community Surveillance	Demonstrate the capability of viewing the streams from community surveillance cameras	



		in a single view of Operator interface using the following medium: - a. LAN / WAN b. Edge based IOT Gateway	
10.	General Features	a. Demonstrate the IPv6 capabilities of the VMS platform. b. No dependency on camera MAC address for licensing. c. Demonstrate native tools to real time and scheduled backup of video/ Flagged and critical data to Near DR Servers/Storage. d. Interface customization capabilities like PTZ, tool bars, menu controls etc. based on specific operator user privileges. e. Tools for exporting video and a self-contained video player on various media such as USB keys, CD/DVD-ROM for evidence in encrypted and encrypted format. f. Native tools to build sequences of video to create a storyboard and allow the export of synchronous cameras from operator interface.	

B.3. L2 Field Switch

Sr. No	Parameters	Method for Testing during POC	Demonstrated / Submitted & Verified
Compliance to the Network as specified in the Tender Specifications			
1.	Edge Switches (L2 8 Port Field Switch)	a. To ensure LAN ports being disrupted by flooding the switch should be configurable to control (Bcast/Ucast/Mcast) storms b. To ensure flexible, reliable applications delivery and prioritize traffic, switch should be configured for QoS Shaping with 8 queues c. To ensure flexible delivery and power savings, switch should be configured for POE power scheduling daily and weekly per time interval d. Device should be configured for 802.1x radius with NAC integration e. IP and MAC binding should be configured to ensure all requests from particular IP address are served only by the endpoint	



		having that particular MAC address. This is to ensure security at edge f. To reject invalid and malicious traffic, Arp Inspection to be configured g. To restrict IP traffic on untrusted Layer 2 ports, Source Guard should be configured h. Switch should be configured with cable diagnostics to verify cable length. This is to ensure optimal distance for connectivity of camera from PoE switch port i. Integration with camera vendor to ensure seamless connectivity j. Switch should be configurable via CLI or GUI to test device performance for throughput, latency k. PIM protocol-based multicast functionality if provided will be added advantage. l. Vendor should configure G.8032 protocol for ring protection and recovery of traffic in <50 ms. Vendor should configure at least 4 switches in the ring for this test	
2.	Bandwidth validation	a. Bandwidth Consumed by Fix Box Camera at 25 FPS (normal time) b. Bandwidth consumed by Fix Box Camera at 25 FPS (no movement/night period) c. Bandwidth Consumed by PTZ Camera at 25 FPS (normal time) d. Bandwidth consumed by PTZ Camera at 25 FPS (no movement/night period) e. Bandwidth Consumed by ANPR Camera at 25 FPS (normal time) f. Bandwidth consumed by ANPR Camera at 25 FPS (no movement/night period)	



C. Compliance to the integration requirements as specified in the Tender Specifications

Sr. No	Parameters	Functionality Test in Demonstration	Demonstrated / Submitted & Verified
1.	ICCC + VMS+ Video Analytics + GIS + ANPR + FRS + Mobile Devices	Integration of offered subsystems.	
2.	Edge Gateway	Edge gateway Integration with third party VMS/NVR along with quoted VMS/ICCC has to be demonstrated for viewing existing camera feeds.	
3.	EMS Software	• Network Fault Management • Network Performance Management • Server Performance Monitoring • Centralized Log Management • Centralized and Unified Dashboard • Centralized and Customizable • Service Level Reporting • Help Desk for Incident Management	
4.	NAC	• Should be able to integrate with all makes of manageable network devices which are capable of supporting open standards-based protocols required for NAC operation. • Must enable diagnosis of network issues and performance through real-time NetFlow analysis. • Must provide port level analysis capability • Should be able to perform posture check for compute end points (Windows & MAC) for OS health for parameters like Registry Keys, allowed process, AV or Firewall Enabled etc.	



D. AI Based Video Intelligence Platform & Video Analytics Use Case Parameters for Proof of Concept –

Sr. No.	Parameters	Functionality Test in Demonstration	Demonstrated / Submitted & Verified
1.	Innovation	Any new and out of the box showcase which can help CDAC and Delhi Police.	
2.	High Availability and Virtualization Support	Bidder to showcase High Availability and Virtualization capability of Video Analytics Platform in case of failure of any one node. The POC documentation should include a benchmarking reports / case studies to support the capabilities.	
3.	New Application Development Capabilities of the Platform	Bidder to showcase the following capabilities of the AI based Video Analytics Platform in detail during the POC – • The AI system shall also support native or third-party developed algorithms and use-cases that can provide the user with a large base of use-cases to choose from. • For new application development, the system shall provide a developer Software Development Kit (SDK) for this purpose. The SDK shall be provided along with detailed documentation for building end-to-end use-cases on the system. • The system shall also allow the user to plug different AI models in the individual running of the video analytics use-case.	
4.	Annotation tool with Project Management capabilities	Bidder to showcase the following capabilities of the AI based Video Analytics Platform in detail during the POC – • The system shall have an inbuilt annotation tool that allows a user to label the images with relevant information using both rectangle and polygon drawing facilities. • The annotation should allow labelling of images or drawn objects with different class names. In case of persons, it should also support labelling of various attributes such as color of clothing, type of clothing, age, gender etc. as well. • The annotation tool should have a comprehensive project management feature, including assigning annotation jobs on a set of images to individual users. The system should also have support for higher privileged users who can	



		approve/disapprove the annotations done by the annotators. • The user should be able to train new deep-learning models from the annotated data using the Annotation UI itself. The user-interface should allow to plug-in the trained model in any of the relevant Video Analytics use-cases dynamically at each camera. • The system should allow the user to plug newly trained AI models at runtime by simply selecting the models in the per-camera configuration page.	
5.	Training	Bidder to showcase the following capabilities of the AI based Video Analytics Platform in detail during the POC - • The system shall allow seamless training by labelling any objects within the images and providing them suitable attributes of multiple types such as class, subclass, colour, type etc. The system shall allow training to happen continuously, on demand or on periodic intervals, which shall be configurable.	
6.	Complete visibility of all the resources	Bidder to showcase the following capabilities of the AI based Video Analytics Platform in detail during the POC - • The System should provide an intuitive interface for complete visibility of all the resources in the system, such as edge-devices, servers, cameras and their live status on a GIS Map View. Utilization of all Analytics Software Licenses including FRS and ANPR for ease of dynamic deployment of applications across cameras. • The system should provide component level view and health parameters of system resources such as CPU, GPU, Memory, Storage.	
7.	User Management	Bidder to showcase the following capabilities of the AI based Video Analytics Platform in detail during the POC - • The system should support user with a hierarchical access level, with different access level for different users demarcated with respect to cameras, use-cases and the data. The user access control system should allow setting of SOP's like CRUD (Create,	



		Read, Update and Delete) operations for each user.	
8.	Deployment of use cases across any camera	Bidder to showcase the following capabilities of the AI based Video Analytics Platform in detail during the POC - - The system should allow deployment of any use case on any camera without any MAC level or IP level locking. Ideally any use case should be deployable and redeploy able on any camera or video source as far as the camera view supports such use cases to be deployed. - All the Analytics including FRS and ANPR applications should be deployed across the cameras using the same Video Analytics Platform	
9.	Key UI Views	Bidder to showcase the following capabilities of the AI based Video Analytics Platform in detail during the POC - Resource Management View: - The User interface should provide a list of all the resources available in the system such as computing servers, edge-computing devices and cameras. - The status of each of the devices, whether they are online/offline should also be available at all times. Camera Use case matrix: - The user interface should have a matrix to assign, start, stop and schedule any use-case on any camera. - The status of active and non-active analytics should be clearly visible with colour coded information	
10.	Common UI for all the analytics / use cases	Bidder to showcase the following capabilities of the AI based Video Analytics Platform in detail during the POC - The user interface should be a unified dashboard that shows events from all the analytics / use cases (Video Analytics use-cases) and all the cameras in a common UI, and which gets populated in real time from event notifications.	
11.	Configuration per- channel	Bidder to showcase the following capabilities of the AI based Video Analytics Platform in detail during the POC - The system should allow each analytics to be uniquely configured for every individual	



		camera stream, with parameters for camera calibration, image quality improvement, night/day settings etc. - The analytics should be able to run on different cameras with different settings (e.g., different Zones for Intrusion, different lines for line crossing detection, etc.) at different hours of the day. - The configuration page should allow a user to choose any of the available AI models to detect and classify objects within the image. The description of the models should clearly specify performance and hardware requirements of each of the model.	
12.	Hardware Sizing and Benchmarking	MSI will be required to showcase load testing of the CPU and GPU per analytics server to confirm that the video analytics application will perform satisfactory under the full load of Video analytics channels and the number of servers quoted in the BOQ. - Example - If MSI has quoted in-total 50 servers for running the total load of 5000 video analytics use cases, then the MSI should demo 1 server load = $5000/50$ i.e. 100 channels in the POC. The system should process the video at the actual camera resolution at the camera frame rate. - Supporting documents like case studies / benchmarking reports with the Server hardware OEM's should be submitted along with the POC documentation.	
13.	ANPR	ANPR Functionality test in demonstration. - The system should detect and capture Standardized Plates. - Detect plates even at night using IR Illuminators. - Accuracy should be Minimum 95% during the day assignment of labels to individual number plates, such as 'VIP', 'offender', etc. - Generate automatic alarms to alert the control room personnel for further action. Evaluation Parameters – - The solution shall demonstrate the detection of number plate in standard format and in different fonts. The solution provider shall create test cases to detect different number plates. (Accuracy >90%)	



		• The solution provider shall demonstrate the detection of Number plat using IR illuminators in the dark during the night. (Accuracy >90%) • The solution shall demonstrate the detection of various vehicles by attributes like color and type. The solution shall be able to identify the vehicle type. The solution shall be demonstrating over a test video data set.	
14.	Facial Recognition System	Functionality test in demonstration. • Recognition of Full-Face from varying angles. • Recognition of Partial Face from varying angles. • Match suspected criminal face from pre-recorded feeds. • Identify multiple persons of interest in a single frame in real-time. • Generate alerts for blacklisted individuals. Evaluation Parameters – • The accuracy should be showcased using surveillance cameras mounted at actual heights. • The OEM shall show the recognition of full face of test case using - ○ Right part or left part of the face. ○ Facial props worn by the case (like turban, thick beard, etc.) ○ The OEM shall show the demo on a test case to recognize the suspect from the ▪ The pre-recorded feeds ▪ Create a test database using dummy images ▪ From the database created, to identify the criminal in real time. • The OEM shall demonstrate identification of multiple persons in a single frame for ○ Blacklisted individuals – The OEM shall create a test dataset of blacklisted individuals and using it the solution shall identify and raise severity alert. The same shall be demonstrated in a single frame of multiple faces.	



		Whitelisted individuals – The OEM shall create a test dataset of whitelisted individuals and using it the solution shall identify and raise severity alert. The same shall be demonstrated in a single frame of multiple faces.	
15.	Crowd Estimation and Management	Functionality test in demonstration. - Showcase estimation of crowd in extremely dense environments like public processions and festivals, rally etc. Evaluation Parameters – - The accuracy of detection should be above 85% on the video provided by the evaluation committee.	
16.	Person Collapsing	Functionality test in demonstration. The app should detect if a person walking upright has collapsed or fallen on the ground. Evaluation Parameters – - This app should raise an alert if any pedestrian is Jay walking. - The app should provide zone wise data of both the pedestrian movements at zebra crossings and jay walking with a minimum of hourly granularity	
17.	Camera Health Monitoring	Functionality test in demonstration. - The Camera Health Monitoring app should be able to monitor the status of the camera and report an alert in case the camera is not functional or tampered with intentionally or unintentionally. Evaluation Parameters – - The accuracy of application be above 90 % on the video provided by the evaluation committee. - Alerts should be raised on following incidences. - Camera view tampered with bright light - Camera scenes gets too dark below a threshold - The app should raise an alert if the camera is turned off or connectivity is lost. - Camera cable pulled. / Connectivity lost.	



***Miscellaneous:** Power Arrangement- With respect to the power requirements at field for PoC, the power arrangements to be ensured by the MSI through adequate Gen-set as an essential part of the PoC exercise. All arrangements required for POC should be arranged by MSI.

2.1.11. Award of Contract /Order

The Contract will be awarded to the bidder securing highest CTFS. However, C-DAC reserves the right to discard the bidder securing highest CTFS. The scope of contract will cover implementation of all phases including warranty for 05 years and O & M for three years. Delhi Police may enter into a contract for CAMC services, after expiry of warranty period. However, the prices quoted by the bidder for CAMC services will be binding on bidder. A contract will be signed on receipt of performance bank guarantee from the selected bidder. The draft contract form is provided in RFP Chapter 6.

2.1.12. Notification of Award

C-DAC will notify the Successful Bidder confirming the selection of the Bidder. The Bidder shall confirm the acceptance of the same in writing within 05 (five) days.

2.1.13. Locations for Delivery and Project Implementation

The selected bidder shall be required to carry out the project implementation activities within the physical boundary of NCT Delhi Police Commissionerate comprising of 16 districts. The locations for DC, near DR, C4i, C3i, C2i, and field locations are indicated in the location map, and same will be shared post the signing of the Non- Disclosure agreement with selected bidder.

2.1.14. Prices

- a. Bidders shall quote for the entire scope of contract on an “overall responsibility” basis such that the total Bid Price covers Bidder’s all obligations mentioned in or to be reasonably inferred from the bidding documents in respect of providing the product/services.
- b. The prices for components/ sub-systems supplied and services to be provided must be quoted in INR only.
- c. Prices must be quoted as per the format uploaded under this RFP on CPP Portal.
- d. The prices quoted must be inclusive of all the costs, charges, freight, insurance, handling charges, packing charges, license fees, labour charges, warranty for three years and incidental charges till successful completion of project deliverables.
- e. The prices towards extended warranty of further two years, Operation and maintenance for three years and comprehensive AMC (CAMC) for three years should be quoted separately as given in price bid format.
- f. The item wise break up of CAMC charges for three years should be submitted as per the format given in price bid.
- g. The prices must include the charges towards testing, Demonstration of PoC, and completing the quality acceptance criteria, training etc.



- h. All prices should be quoted excluding applicable GST. Bidder must indicate rates of current applicable GST separately for each line item.
- i. In case of change in Government statutory taxes/ duties, the taxes and / or duties applicable as on date of supply will prevail.

2.1.15. Performance Security

Within fifteen (15) days from the date of notification of Award, the Successful Bidder shall at his own expense submit unconditional and irrevocable Performance Security in the form of Bank Guarantee (PBG) to C-DAC. The PBG shall be from a Nationalized Bank or a Scheduled Commercial Bank in the format prescribed in the RFP, payable on demand, for the due performance and fulfillment of the contract by the bidder.

This Performance Bank Guarantee shall be for an amount equivalent to 10% of total contract value.

C-DAC reserves the right to forfeit the Performance Bank Guarantee, in an event if the Bidder:

- a. fails to meet the overall penalty condition as mentioned in RFP para 2.1.29 of Chapter 2 or any changes agreed between the parties,
- b. fails to perform the responsibilities and obligations as set out in the Contract/ Order to the complete satisfaction of C-DAC,
- c. Misrepresents facts/information submitted to C-DAC.

The Performance Bank Guarantee shall be valid till satisfactory completion of warranty period (Go-live of Phase-3 + 62 months). The Performance Bank Guarantee may be discharged/returned by C-DAC upon being satisfied that there has been due performance of the obligations by the Successful Bidder under the Contract.

In the event of the Bidder being unable to service the contract for whatever reason(s), C-DAC shall have the right to invoke the Performance Bank Guarantee. Notwithstanding and without prejudice to any rights whatsoever of C-DAC under the contract in the matter, the proceeds of the PBG shall be payable to C-DAC as compensation for any loss resulting from the Successful Bidder's/ MSI's failure to perform/comply its obligations under the contract.

C-DAC shall notify the Bidder in writing of the exercise of its right to receive such compensation within 40 days, indicating the contractual obligation(s) for which the Bidder is in default. C-DAC shall also be entitled to make recoveries from the Bidder's bills, Performance Bank Guarantee, or from any other amount due to it, an equivalent value of any payment made to it due to inadvertence, error, collusion, misconstruction or misstatement.

In case the Project is delayed beyond the Project Schedule as mentioned in para 2.1.25 of Chapter 2, the Performance Bank Guarantee shall be accordingly extended by the Bidder till completion of scope of work as mentioned in Chapter 4 of RFP.



On satisfactory performance and completion of the order in all respects and duly certified to this effect by the Project Coordinator, Contract Completion Certificate shall be issued and the Performance Bank Guarantee would be returned to the Bidder.

2.1.16. Timelines linked with Payment Schedule

The details of complete project is envisaged to be completed in four phases as given below.

Phase 1 includes 06 Districts of Delhi covering 75 Police Stations (C2I) and 1360 Locations. The Go Live of Phase 1 would be in 09 months. This would also involve 'as-is assessment' and the Blueprinting of a Data Centre, Integrated Command, Control, Communication & Compute center (C4I) at Police HQ, Command, Control & Communication (C3I) at District Head Quarter and Command & Control center(C2I) at Police Stations along with respective IT and Non IT Infrastructure including installation and commissioning of the Filed devices. Phase1 includes the procurement of 1 MCCV & also Integration of 32 existing Databases.

Phase 2 shall cover additional 04 districts with 45 Police Stations (C2I) with 836 Locations. The Go Live of Phase 2 would be in 11 months from Kick-Off Date. This would involve commissioning of near Disaster Recovery Center (nDR), Command, Control & Communication (C3I) at District Head Quarter and Command & Control center(C2I) at Police Stations along with respective IT and Non IT Infrastructure including installation and commissioning of the Filed devices. Phase 2 includes the second MCCV procurement.

Phase 3 shall cover additional 06 districts with 62 Police Stations (C2I) and 1155 Locations. The Go Live of Phase 3 would be in 14 months from Kick-Off Date. This would involve commissioning of Command, Control & Communication (C3I) at District Head Quarter and Command & Control center(C2I) at Police Stations along with respective IT and Non IT Infrastructure including installation and commissioning of the Filed devices.

Phase 2 and Phase 3 will be running concurrently, so that the whole project should be completed in the given timeline.

Phase 4 Warranty and Operation and Maintenance Phase: The bidder shall carry out the operation and maintenance services towards the implemented system for the period of 03 years. The Warranty (05 years) and the O & M (03 years) will run in parallel.

The payments to MSI shall be released in phased manner after the successful completion of the target milestones for the respective phase. The detailed Phase wise timelines linked with Payment Schedule for MSI are as under:

S. No.	Phase-wise Activity	Timeline	Payment (%)
A.	Selection of the MSI	T	
B.	Work Order/ Contract between TSP (C-DAC) and MSI	T+1Week	Advance to MSI: 10% of the Contract Value will be given against Submission of ABG (Advance Bank Guarantee) of 10% as per format given in RFP Performance Security :



C.			Submission of Performance Security of 10% of the contract value at the time of Contract signing.
	Project Kick Off & Team Mobilization		
1.	Kick-off Meet (MSI), Project Inception Phase / Team Mobilization from issue of WO (MSI)	T+3Week	
D.	Phase-1(06 Districts) : Project Design, planning and Implementation activity		
2.	Site Survey (Jointly in-between MSI and ISP), GIS Mapping, Project Planning Phase	T +6week	
3.	Addressing of ROW, RI Issues for MSI activities	T+3 week to T+18 week	
4.	Applying for Power Meters	T+3 week to T+ 30 week	
5.	Delivery of Non-IT items at Site (Procurement & Supply of Material at C4I, C3I, C2I)	T+4 week to T+18 week	40% of the Order value of the respective Non-IT items and other material for Phase-1 against delivery of same at site on Pro-rata basis.
6.	Installation of Non IT Equipment at C4I, C3I, C2I	T+ 6 week to T + 22 Weeks	10% of the Order value of the respective Non-IT items and other material for Phase-1 against installation and commissioning of the same at site on Pro-rata basis.
7.	Procurement & Supply of JB, Poles, Passive Components for Phase 1	T+ 6 week to T + 16 Weeks	40% of the Order value of the respective JB, Poles, Passive Components for Phase-1 against delivery of same at site on Pro-rata basis.
8.	Installation of JB & Poles, Cabling (Power + Cat6) of 6 District's police stations	T+ 6 week to T + 24 Weeks	10% of the Order value of the respective JB, Poles, Passive Components for Phase-1 against installation and commissioning of the same at site on Pro-rata basis.
9.	Procurement of Camera & Switches & UPS	T + 16 Weeks	40% of the Order value of the respective Camera & Switches & UPS for Phase-1 against delivery of same at site on Pro-rata basis.
10.	Installation of Power Meters	T+ 20 week to T + 24 Weeks	55% of the Order value of the Power Meters on supply & Installation for Phase-1 at site on Pro-rata basis.
11.	Installation of Camera, Switches & UPS	T+ 20 week to T + 24 Weeks	10% of the Order value of the respective Camera & Switches & UPS for Phase-1 against installation and commissioning of the same at site on Pro-rata basis.



12.	SOPs & Helpdesk Preparation	T+9 week	
13.	Procurement, Supply of IT Equipment & OS, Security Appliance, Security at DC, C4I, C3I, C2I	T+12 week	40% of the Order value of the respective IT Equipment & OS, Security Appliance, Security at DC, C4I, C3I, C2I for Phase-1 against delivery of same at site on Pro-rata basis.
14.	Installation of IT Equipment & OS, Security Appliance, Security at DC, C4I, C3I, C2I	T+20 week	10% of the Order value of the respective IT Equipment & OS, Security Appliance, Security at DC, C4I, C3I, C2I for Phase-1 against installation and commissioning of the same at site on Pro-rata basis.
15.	Procurement, Supply of Software application for VMS, ICCC, FRS, PIU, ANPR & VA etc.	T+18 week	30% of the Order value of the respective Software application for VMS, ICCC, FRS, PIU, ANPR & VA for Phase-1 against delivery of same at site on Pro-rata basis.
16.	Installation integration of VMS, VA, ICCC, FRS, PIU, ANPR etc. Application Software at C4I, C3I, C2I	T+20 week	20% of the Order value of the respective Software application for VMS, ICCC, FRS, PIU, ANPR & VA for Phase-1 against installation and commissioning of the same at site on Pro-rata basis.
17.	Installation and Commissioning: Integration, Configuration & Operationalization of DC, C2I, C3I, C4I-Testing & Integration with MPLS line links, Camera, DC, C4I, C3I, C2I	T+22 week to T+26 weeks	65% of the Installation and Commissioning Charges for the Integration, Configuration & Operationalization of DC, C2I, C3I, C4I-Testing & Integration with MPLS line links, Camera, DC, C4I, C3I, C2I for Phase-1 against delivery of same at site on Pro-rata basis.
18.	Procurement, customization, installation & Finalization of Mobile Command & Control Vehicle- (1st MCCV)	T + 3Weeks to T+20 Weeks	65% of the order value of MCCV after supplying fully furnished / equipped vehicle and on integration and commissioning of same with the system.
19.	External Integration- Database Integration	T+4 weeks Onward	



	(Platform Identification)		
20.	Training	T+30 Week	
21.	Testing & UAT	T+30 Week	
22.	Contingency Period	T+32 Weeks	
23.	Commissioning of Phase 1	T+34Week	10 % of the order amount pertaining to Phase – 1 will be paid within 30 days of Go-Live of Phase – 1. The acceptance certificate issued by C-DAC/DP must be submitted by MSI for claiming this amount.
E.	Phase-2 (04 Districts) : Project Design, planning and Implementation activity		
24.	Site Survey (Jointly in-between MSI and ISP), GIS Mapping, Project Planning Phase	T+18 week to T+22 week	
25.	Addressing of ROW, RI Issues for MSI activities	T+20 week to T+30 week	
26.	Installation of Power Meters	T+ 20 week to T + 31 Weeks	65% of the Order value of the Power Meters on supply & Installation for Phase-2 at site on Pro-rata basis.
27.	Delivery of Non-IT items at Site (Procurement & Supply of Material at C3I, C2I)	T+18 week to T+34 week	50% of the Order value of the respective Non-IT items and other material for Phase-2 against delivery of same at site on Pro-rata basis.
28.	Installation of Non IT Equipment at C3I, C2I	T+18 week to T+34 week	15% of the Order value of the respective Non-IT items and other material for Phase-2 against installation and commissioning of the same at site on Pro-rata basis.
29.	Procurement & Supply of JB, Poles, Passive Components for Phase 2	T+18 week to T+34 week	50% of the Order value of the respective JB, Poles, Passive Components for Phase-2 against delivery of same at site on Pro-rata basis.
30.	Installation of JB & Poles, Cabling (Power + Cat6) of 6 District's police stations	T+ 18 week to T + 40 Weeks	15% of the Order value of the respective JB, Poles, Passive Components for Phase-2 against installation and commissioning of the same at site on Pro-rata basis.
31.	Procurement of Camera & Switches & UPS	T+ 18 week to T + 28 Weeks	50% of the Order value of the respective Camera & Switches & UPS for Phase-2 against delivery of same at site on Pro-rata basis.



32.	Installation of Camera, Switches & UPS	T+ 24 week to T + 40 Weeks	15% of the Order value of the respective Camera & Switches & UPS for Phase-2 against installation and commissioning of the same at site on Pro-rata basis.
33.	Procurement , Supply of IT Equipment & OS, Security Appliance, Security at C3I, C2I	T+38 week	50% of the Order value of the respective IT Equipment & OS, Security Appliance, Security at C3I, C2I for Phase-2 against delivery of same at site on Pro-rata basis.
34.	Installation of IT Equipment & OS, Security Appliance, Security at C3I, C2I	T+40 week	15% of the Order value of the respective IT Equipment & OS, Security Appliance, Security at C3I, C2I for Phase-2 against installation and commissioning of the same at site on Pro-rata basis.
35.	Procurement and Supply of Hardware infrastructure material and software for nDRC	T+30 week to T+35week	50% of the Order value of the respective Hardware infrastructure material and software for nDRC for Phase-2 against delivery of same at site on Pro-rata basis.
36.	Setup of nDRC and integration with Data Center	T+35week to T+40week	15% of the Order value of the respective Hardware infrastructure material and software for nDRC for Phase-2 against installation and commissioning of the same at site on Pro-rata basis.
37.	Procurement, customization, installation & Finalization of Mobile Command & Control Vehicle- (2nd MCCV)	T+20week to T+40week	65% of the order value of 2nd MCCV after supplying fully furnished / equipped vehicle and on integration and commissioning of same with the system.
38.	Integration, Configuration & Operationalization of C2I, C3I with C4I- Testing & Integration of MPLS , Camera , DC, C4I, C3I, C2I , nDRC	T+41 weeks	65% of the Installation and Commissioning Charges for the Integration, Configuration & Operationalization of C2I, C3I with C4I-Testing & Integration of MPLS , Camera , DC, C4I, C3I, C2I for Phase-2 against delivery of same at site on Pro-rata basis.
39.	External Integration- Database Integration (16 Databases)	T+42 weeks	25% after 10 Database Integration
40.	Training	T+41 weeks	
41.	Testing & UAT	T+41 weeks	
42.	Commissioning of Phase 2	T+42 weeks	10 % of the order amount pertaining to Phase – 2 will be paid within 30 days of Go-Live of Phase – 2. The acceptance certificate issued by C-DAC/DP



			must be submitted by MSI for claiming this amount.
F.	Phase-3 (06 Districts) : Project Design, planning and Implementation activity		
43.	Site Survey (Jointly in-between MSI and ISP), GIS Mapping, Project Planning Phase	T+26 week to T+32 week	
44.	Addressing of ROW, RI Issues for MSI activities	T+28 week to T+40 week	
45.	Installation of Power Meters	T+ 28 week to T + 41 Weeks	65% of the Order value of the Power Meters on supply & Installation for Phase-3 at site on Pro-rata basis.
46.	Delivery of Non-IT items at Site (Procurement & Supply of Material at C3I, C2I)	T+26 week to T+42 week	50% of the Order value of the respective Non-IT items and other material for Phase-3 against delivery of same at site on Pro-rata basis.
47.	Installation of Non IT Equipment at C3I, C2I	T+26 week to T+42 week	15% of the Order value of the respective Non-IT items and other material for Phase-3 against installation and commissioning of the same at site on Pro-rata basis.
48.	Procurement & Supply of JB, Poles, Passive Components for Phase 3	T+26 week to T+42 week	50% of the Order value of the respective JB, Poles, Passive Components for Phase-3 against delivery of same at site on Pro-rata basis.
49.	Installation of JB & Poles, Cabling (Power + Cat6) of 6 District's police stations	T+ 28 week to T + 46 Weeks	15% of the Order value of the respective JB, Poles, Passive Components for Phase-3 against installation and commissioning of the same at site on Pro-rata basis.
50.	Procurement of Camera, Switches & UPS	T+ 26 week to T + 42 Weeks	50% of the Order value of the respective Camera, Switches & UPS for Phase-3 against delivery of same at site on Pro-rata basis.
51.	Installation of Camera, Switches & UPS	T+ 24 week to T + 40 Weeks	15% of the Order value of the respective Camera, Switches & UPS for Phase-3 against installation and commissioning of the same at site on Pro-rata basis.
52.	Procurement , Supply of IT Equipment & OS, Security Appliance, Security at C3I, C2I	T+42 week	50% of the Order value of the respective IT Equipment & OS, Security Appliance, Security at C3I, C2I for Phase-3 against delivery of same at site on Pro-rata basis.
53.	Installation of IT Equipment & OS,	T+48 week	15% of the Order value of the respective IT Equipment & OS, Security Appliance, Security at C3I,



54.	Security Appliance, Security at C3I, C2I		C2I for Phase-3 against installation and commissioning of the same at site on Pro-rata basis.
	Integration, Configuration & Operationalization of C2I, C3I with C4I.	T+50 week	10% of the Order value of the respective IT Equipment & OS, Security Appliance, Security at DC, C4I, C3I, C2I for Phase-3 against installation and commissioning of the same at site on Pro-rata basis.
	Testing & Integration with MPLS, Camera, DC, nDRC, C4I, C3I, C2I		
	55. Testing & Integration of MPLS, Camera, DC, C4I, C3I, C2I	T+50 weeks	
	56. External Integration- Database Integration (16 Databases)	T+50 weeks	25% after 10 Database Integration
	57. Training	T+50 weeks	
58.	Testing & UAT	T+50 weeks	
59.	Commissioning of Phase 3	T+52 weeks	10 % of the order amount pertaining to Phase – 3 will be paid within 30 days of Go-Live of Phase – 3. The acceptance certificate issued by C-DAC/DP must be submitted by MSI for claiming this amount. - The balance amount payable towards the work completed till Go-Live of Phase -3 will be paid in two equal installments - one within 30 days of Go-Live of Phase – 3 and second within 60 days of Go-Live of Phase 3, after adjusting the advance amount on pro-rata basis. - The penalties, SLAs or any amount deductible as per Contract terms will be deducted from payable amount of second installment. - The ABG will be released at this stage.
G.	Phase-4: O&M :Providing O & M services as per Para 2.1.27 of Chapter 2 of this document	T+53 weeks onwards till T+209 Weeks or 03 years after phase -3 go-live whichever is later	The equated quarterly payments towards O & M services will be released at the end of each quarter, on submission of quarterly invoice. The deductible amounts – if any, towards SLA will be deducted on quarterly basis from the quarterly payments. The copy of certificate issued by C-DAC towards satisfactory O&M services rendered by MSI must be attached with the invoice.



2.1.17. Warranty

- a. The bidder shall provide comprehensive warranty towards entire implemented system including IT hardware, Non-IT hardware, software and services etc. The warranty shall commence from the date of acceptance of respective system/post Go-Live of the entire project and shall be operational for a period of minimum 05 years' whichever is later.
- b. Technical Support for Software applications shall be provided by the respective OEMs for the period of warranty. The Technical Support should include all upgrades, updates and patches to the respective Software applications.
- c. The MSI warrants that the Goods supplied under the Contract are new, non-refurbished, unused and recently manufactured at the time of delivery; the End of sale / End of support of any product should not prevail before 18 months of the commissioning; and shall be supported by the MSI and respective OEM along with service and spares support to ensure its efficient and effective operation for the entire duration of the contract.
- d. The MSI warrants that the goods supplied under this Contract shall be of the highest grade and quality and consisted with the established and generally accepted standards for materials of this type. The goods shall be in full conformity with the specifications and shall operate properly and safely. All recent design improvements in goods, unless provided otherwise in the Contract, shall also be made available.
- e. The MSI further warrants that the Goods supplied under this Contract shall be free from all encumbrances and defects/faults arising from design, material, manufacture or workmanship (except insofar as the design or material is required by C-DAC's Specifications) or from any act or omission of the MSI, that may develop under normal use of the supplied Goods in the conditions prevailing at the respective Datacenter / Server Room Sites.
- f. The replacement of faulty hard disks of server, storage and workstation will be on on-returnable basis.
- g. C-DAC shall promptly notify the MSI in writing of any claims arising under this warranty.
- h. Upon receipt of such notice, the MSI shall, with all reasonable speed, repair or replace the defective Goods or parts thereof, without prejudice to any other rights which C-DAC may have against the MSI under the Contract.
- i. If the MSI, having been notified, fails to remedy the defect(s) within a reasonable period, C-DAC may proceed to take such remedial action as may be necessary, at the MSI's risk and expense and without prejudice to any other rights which C-DAC may have against the MSI under the Contract.
- j. Any OEM specific warranty terms that do not conform to conditions under this Contract shall not be acceptable
- k. The selected MSI shall provide Guarantee/Warranty for all Stores, Equipment, Services supplied at least for a period of 60 months (05 years i.e. 03 Years warranty+02 Years extended warranty) from the date of commissioning of the Systems at the Sites/Locations and that the said system would continue to conform to the description and quality for all equipment's/system. If any deviation or deterioration in description and quality, design, workmanship and performance as per the agreed specifications is noticed or discovered during the period of warranty (the decision of the BUYER in that behalf shall be final, and binding on the parties),



the BUYER shall be entitled to reject the said item, systems or such portion thereof as may be discovered or noticed.

- l. On such rejection, the concerned equipment, systems or portions thereof will be at the MSI's risk and all the provisions herein contained related to rejection of said equipment etc. shall apply.
- m. MSI shall replace the said equipment, systems or portions thereof within a period of 48 hours. In such event the remaining warranty period shall apply to the equipment, systems or portions thereof so replaced from the date of replacement.
- n. MSI shall provide 24x7 support with 4 hours response time and 48 hours of resolution time from the date and time of reporting of an error, during the warranty and extended warranty period. The defective card/item/equipment should be repaired/replaced within 48 hours at the location of installation of the said item free of cost. In case major defects requiring the defective card/item/equipment to be taken to the MSI workshop, an immediate substitute card/item/equipment will be provided by MSI for smooth operation of the System and the defective card/item/equipment should be returned/installed duly repaired within six weeks. The to and fro transportation charges of the card/item/equipment will be the responsibility of the MSI.
- o. MSI shall replace the defective equipment, systems or portions thereof at the exact location or place of installation of the said item free of cost.
- p. The warranty period will cover the entire Systems deployed at the Sites/Locations including all perishable, non-perishable and consumable items and equipment's.
- q. MSI is required to provide Software patches from time to time, free of cost during the warranty period.
- r. Further, any bugs/shortcomings detected shall be rectified free of cost during the warranty period.
- s. MSI shall ensure to set up a maintenance base in Delhi with dedicated deployment of sufficient numbers of engineers round the clock for all Command & Control Centres (i.e. Data Centre, nDR, C4i, C3i & C2i) having full knowledge of the system to attend to technical and/or operational problems at each site during the warranty period (60 months) from the date of commissioning/acceptance of the system(s).
- t. Sufficient number of Service Engineers should be deputed round the clock at Data Centre & C4i to attend to any fault immediately.
- u. The Quarterly Preventive Maintenance and diagnostics of the system on all the locations should be carried out by the MSI.
- v. No payment will be made to the MSI towards maintenance, repair, and replacement etc. of the entire System during the warranty period.
- w. During the warranty period, in case any field equipment is damaged by a vehicular accident (or due to any other reason outside the control of MSI, ISP, Vendor, etc.) and need repair/replacement, the corresponding equipment will be replaced by MSI. In such cases, damages are to be borne by the MSI through proper comprehensive insurance for all equipment.

2.1.18. Operations and Maintenance

The MSI shall provide complete Operations and Maintenance support for the integrated solution deployed from the date of Go-Live of respective phases and shall be operational for a period of minimum 03 years' post Go-Live of the entire project.



During the Warranty and O&M period, the MSI shall provide all product(s) and documentation updates, patches/fixes, and version upgrades within 15 days of their availability/release and should carry out installation and make operational the same at no additional cost to C-DAC.

In this phase, MSI would be responsible for operations and maintenance of the entire solution.

The following services should be provided by MSI:

- a. O&M phase planning and monitoring
- b. Ongoing Administration and Maintenance requirements
- c. Operation of Monitoring Centre (including Help Desk)
- d. VAPT Execution
- e. Facility Management Services at Command & Control Centre
- f. MIS Reports and Incident Reporting
- g. Assistance in Integration with other integrations as and when required by adding more use-cases
- h. Continuous Learning to the system on new alerts and VA systems
- i. SLA reporting
- j. The MSI is required to ensure that all the required hardware and software proposed should be capable and meet the required performance as per the RFP.
- k. MSI should ensure while execution and operation & maintenance phase, the industry best practices has to be followed. MSI should adhered to industry standard checkpoints while execution and after starting the operation phase while replacement/ re-installing / re-commissioning such as:
 - Ensure Project objectives are met during O&M phase pertaining to maintenance / operation of hardware, field devices, software and related eco-system etc.
 - Ensure to prepare different kind of reports/documents required during O&M such as preparation of SOPs etc. for effective maintenance of hardware, field devices, software and related eco-system etc.
 - Ensure the safety of the field devices for any damages by providing all necessary equipment's/measures (e.g. housing to protect camera, fencing to poll, conduiting for cables etc.)
 - Maintaining all inventory for the items procured in the project during execution and O&M such maintaining records / registers etc.
 - During operation phase, in case any camera is damaged by a vehicular accident (or due to any other reason outside the control of MSI) and needs repair, then the MSI will need to repair / have the new camera installed at the incidence. Damages are to be borne by MSIs in such cases through proper insurance. During this period, a replacement of the camera to be provided immediately to meet the camera uptime requirement.
 - During O& M Phase, The applications will be customized to meet the project objectives and the requirements of Police Department. The MSI will ensure that the best practices for software development and customization are used during the software development/customization and integration exercise. This would



at a minimum include:

- Software development/customization/integration based on the functional requirement specifications, system requirement specifications, software requirement specifications and solution designs as finalised and approved by Delhi Police. Wherever necessary, the MSI shall develop additional functionality/modules on top of products features, in order to meet the Project requirements.
- Delivering the Surveillance System, along with all of the necessary modules and additional functionalities/ integrated products, utilities, system drivers and documentation consistent with proven standards, including product updates, technology upgrades and patches to run on the selected operating system(s) and hardware according to the solution in O&M Phase.
- It is pertinent to mention that application hosted at the Data Center shall be accessible by the intended users as desired under this Project and the SOPs, Rules and configuration will be changed as per the requirement in O&M Phase.

The Cost of Operation & Maintenance shall be deemed to cover all costs for performing the maintenance services including the cost of providing all labour, tools, equipment, facilities, spare parts, replacement of faulty parts, consumables (excluding diesel/oil and batteries) and other related materials, documentation, staff training, test equipment and all other necessary items.

MSI shall ensure that sufficient maintenance staff is deployed to carry out the maintenance works. Only technically competent and qualified staff shall be deployed for the maintenance works.

MSI shall ensure for the proper functioning of communication lines and all its equipment, diagnose communications faults, perform joint testing etc. through Internet Service Provider (ISP).

MSI shall provide a service escalation list of personnel (including management personnel) to contact in the event of unsatisfactory restoration or service rendered.

Preventive Maintenance (PM)

Regularly scheduled PM shall be performed at least once in three months or as recommended in the product support documentation, whichever is earlier. This maintenance includes all cleaning, lubrication, inspection, testing, calibration, focusing of field equipment, checking of cable insulation, checking for corrosion of steel support, painting works to remove rusts, repairing of concrete base of field equipment and structure, checking of cable clamps and replacement when necessary as well as all alignment necessary to prevent failures and extend the useful life of the System and equipment.

MSI shall ensure that all PM works are properly carried out with minimum interruption to the operation of the system. MSI shall submit a rolling quarterly maintenance work program as per an approved checklist. MSI shall also submit a PM report to the C-DAC. The C-DAC reserves the right to add and delete items on the check list without any additional cost.



Hardware PM shall include all scheduled servicing actions. Scheduled servicing shall include accomplishment of periodic inspection, condition monitoring, critical parts replacements, overhaul, adjustment, calibration, etc. In addition, servicing requirements (i.e. lubrication, cleaning, housekeeping, pest control etc.) shall also be included under the general category of schedule servicing. The PM works shall include at least the following:

- a. Checking and tightening the supports on all mounting poles and replacing them worn out. Cleaning of field equipment and focusing alignment cleaning of inside of equipment housing of dirt, dust etc.;
- b. Checking the mounting brackets for all field equipment and replacing them when damaged or when cracks are observed.
- c. Checking metal parts for corrosion, burst-off and repainting them as required.
- d. Carrying out cable insulation tests as and when required
- e. Checking the condition of earthing, electrical wiring and lightning arrestors and all outdoor equipment.
- f. Checking the foundation, base plate and bolts and nuts of all structure for corrosion, repainting when required as well as tightening or replacement of damaged bolts and nuts.
- g. Monitoring, optimization and fine tuning of the systems;
- h. Perform system backup and restoration for Command & Control Centres
- i. Ensuring security of the System and to report any security violations to C-DAC.
- j. Any other work which affects quality of its output.
- k. Software PM shall include but not limited to the following:
 - l. Installation, reconfiguration, testing and implementation of standard corrections, patches and updates of all software
 - m. Performing regular backup so as to restore the system in the shortest time possible;
 - n. In the event that the software support from the vendor is terminated, MSI shall be responsible for maintaining the affected software at no additional cost and with no adverse delay to the operation of system.
 - o. Licenses for all the operating and application software etc. shall be made available to C-DAC/Delhi Police at no additional cost. The original agreement documents of all the licenses shall be submitted to C-DAC within week of its renewal.
 - p. MSI shall be responsible to supply and install the latest anti-virus software and patches as well as the associated license. The anti-virus software shall include at least the following features:
 - Functions to automatically scan all file inputs, outputs, downloads, program execution and other system related activities;
 - Functions to clear or delete the infected file(s);
 - Ability to check specific files for viruses;
 - Ability to allow the creation of emergency floppy disk to start and clean infected boot sector virus; and
 - Ability to push signature files and upgrades from one main console to the rest of the hardware. There shall be no manual updates and upgrades on individual servers and workstations.



- MSI shall update the virus definition file as and when new update is available.

Any PM work carried out shall not cause any disruption to the operation of System and all the communication links. In the event that any System downtime is required during PM work, MSI shall seek C-DAC's approval prior to carrying out the works.

MSI shall recommend updates and improvements to the System to ensure the optimal operation and security of the System. Upon the approval by C-DAC, MSI shall install, configure and document the updates and/or improvements.

Spares, Consumables and Testing Equipment

MSI shall ensure that adequate spare parts, consumables and testing equipment are maintained for usage, repairs and replacement and ensure that they are available at all times throughout the maintenance period, so that the system functioning should not be affected due to shortage of spare parts.

The cost of the consumables (except diesel for running of the generator after Go-Live of Phase-1, 2 and 3) spare parts and testing equipment is deemed to have been included in the Contract Price for the maintenance in the price schedule.

MSI shall at his own expense obtain, store and maintain in serviceable condition the required number of spare parts and consumable necessary to meet the Maintenance Standards.

The MSI will undertake that supplies of necessary maintenance equipment and spare parts will be made available for all equipment's as well as the complete system for at least Five years, from the date of Commissioning/Acceptance of the System, on a continuing basis so as to ensure 24x7 uninterrupted functioning of the said Projects.

Maintenance Management Facilities

MSI shall ensure to set up a Call Centre and deploy full time maintenance staff for the maintenance of the system on a 24x7 basis. MSI shall provide a maintenance telephone number manned by English & Hindi speaking staff to which all Faults can be reported to at any time.

MSI shall provide C-DAC a list of names, addresses and contact numbers of all staff employed for the maintenance services and of any other persons who may be at any time be required to enter the work site to perform works relating to the Contract.

MSI shall ensure that his authorized representatives shall have their mobile phones switched on at all times to respond to service requests by C-DAC after office hours.

Upon receiving the alert for any fault or Fault reports lodged by other means, MSI shall ensure that the same is attended quickly within the Response Time, and repair, remove or rectify the Faults within the Repair Time stated in the Maintenance Standards. C-DAC shall impose liquidation Damages charges on MSI for failure to respond within Response time and failing to complete the repair work within the Repair Time, without any justifiable reason, as specified in the Maintenance Standards.



In the event MSI's personal encounters difficulty in rectifying any Fault within the Repair Time, MSI shall immediately notify C-DAC giving pertinent details including the time by which it expects to complete the rectification.

Damages to the System as a result of accidents and vandalism shall be included as Faults. MSI shall response to such Faults that arise from road or other accidents and vandalism shall be subjected to the Response Time as specified in the Maintenance Standards as mentioned in this document.

Ad-Hoc Works

TSP may from time to time issue variation to MSI to carry out ad-hoc repair, replacement and improvement works which are not covered under PM or RM works to relocation of equipment affected by road works, maintenance of additional equipment and cleaning and painting of assets.

For accident repair; MSI shall repair the damages as per provision of the contract mentioned at para No. 2.1.27 (v) of chapter 2 above and subsequently inform the C-DAC the cost incurred.

Such works also includes up-gradation of any equipment's viz. cameras, storage, backup, additional licenses, additional manpower etc., if required necessary for effective functioning, on chargeable basis, at the rates of the successful bidder.

Brief scope of the proposed Manpower to be deployed under Operation and Maintenance

Project Manager Responsibility:

- **Prepare roll-out plan for deployment & operationalization of equipment**

The Project Manager with his team shall prepare the overall Data Center establishment & their operational plan for this Project. The plan shall comprise deployment of all the equipment required under the Project. The implementation roll-out plan for setting up the Data Center shall be approved by the Authority. The detailed plan shall also comprise of the scalability, expandability and security that the Data Center will implement under this Project.

- **Preparation of Detailed FRD, SRD and SDD for the Surveillance System and for integration with other systems**

The Project Manager/ MSI will document the requirement in detail before the work on execution begins. Following documents are expected to be delivered as part of this documentation:

- Functional Requirements Documentation (FRD), giving complete details of the functional aspects of the Project.



- System Requirements Documentation(SRD), giving complete details of the entire system components and their inter relationships to execute the Project once operational.
- System Design Documentation (SDD), detailing out the design of the Surveillance System, Command Control Centers in particular, including integration with various IT enabled systems like Vehicle Tracking, e-Challan system, Delhi Police Himmat App, CCTNS, Community Surveillance, etc. currently available or being implemented by the Police Department.

The MSI / Project Manager shall prepare above mentioned documents in discussion with all key stakeholders (Delhi Police, CDAC, Consultants etc.). It is expected that the MSI/Project Manager brings in leading international best practices in this field and ensures that a progressive system is implemented for the IP CCTV Surveillance System in Delhi.

C4I Expert/ ICCC Expert Responsibility:

C4i Expert will provision to ensure that such video feeds can be streamed to the Command Control Centers, District Command & Control Center and if required to viewing centers too.

The Command Control Center (C4i) will also have a room identified for IT Analytics and Forensic Experts where they will analyze the incriminating video footage and certify its integrity & chain of custody. These experts along with C4i expert shall oversee the integration of ANPR with the other relevant databases and also undertake R&D to evaluate and analyze various analytics related technologies and their implementation over the years.

C4I Expert shall undertake detail assessment for integration of the Surveillance System with the Geographical Information System (GIS) so that physical location of cameras, GPS fitted police vehicles (Vehicle Tracking) are brought out on the GIS map. The primary objective of such an asset mapping will be to ensure quick and immediate response for incidents, using the assets available, PCR vans getting shortest possible route options to reach incident locations and ensuring route optimization. The Expert is required to carry out the seamless integration to ensure ease of use of GIS in Surveillance System Applications/Dashboards in Command Control Centers, District level Command and Control Center (C4I, C3i, C2i) & Near DR and by other authorized senior officials. GIS Base Map will be integrated by the C4i expert with all surveillance cameras and other assets as per Delhi Police requirements. The Expert should also ensure that GIS application is integrated with VMS to support the Command Centers to navigate on the map and use it for better spatial understanding. It should also help higher management of Police Department to analyses the events on a spatial perspective. GPS integration with GIS is required to locate all police vehicles (on which GPS units are fitted) on GIS Map. Vehicle tracking should happen even while any vehicle is parked/stationary/ignition-off. Delhi Police under its planned initiatives under SMART Policing, has already embarked on a project for GIS Based Decision support system called Dial112, hence the Expert should ensure seamless GIS integration under this project and consider to extend the features



available in Dial112 to this project at all command centers to ensure complete situational awareness and facilitate decision making and planning.

There are few more requirement/activities of the project which the C4i Expert should perform

SMS Gateway Integration

MSI shall carry out SMS Gateway Integration with the Surveillance System and develop necessary applications to send mass message or SMS to groups/individuals, which can be either manual or system generated. Any external/third party SMS gateway can be used.

Detailed assessment/analysis of video feeds & analytics at Command Control Center (C4i)

The Command Control Center (C4i) will also have a room identified for IT Analytics and Forensic Experts where they will analyze the incriminating video footage and certify its integrity & chain of custody. These experts shall oversee the integration of ANPR with the other relevant databases and also undertake R&D to evaluate and analyze various analytics related technologies and their implementation over the years in O&M Phase.

Integration of Community Surveillance/existing camera project through Edge Gateway on need basis

The C4i expert should be able to prepare and run the solution of integration of community surveillance camera systems spread across Delhi and also the Existing cameras of Delhi Police from Various project on need basis and it should be viewed as per the need/demand. The prime monitoring of community cameras will be done at District level Command & Control Center. As the community cameras are located at sensitive areas hence it is important that these cameras are integrated as a part of this new Surveillance System on need basis through edge gateway.

System Administrator Responsibility:

Server, Networking & Security equipment will be housed at the DC, to provide the compute capability to the applications in order to deliver the functionalities as proposed in the system. The compute capability needs to be designed by the MSI keeping in mind the compliance to SLAs. The system administrator needs to configure, maintain and manage the overall system to keep the highest performance level as per functional requirement and also maintaining the SLA. The Near DR shall be at 5% capacity of the DC analytics & 100% replication of flagged data, the DC- Near DR will remain in Active-Active mode, and the MSI shall design the RTO and RPO time as per requirements. The detailed calculation of the proposed design shall be provided as part of the technical proposal.

Database/Storage Administrator Responsibility:

Storage Administrator/ Database Administrator will have the capability to establish Data Integration layer which will provide connectivity to all source applications and perform complex transformations that would be required in the project. An ETL layer will be created in addition, which would perform extract, transform and load functions. In addition to ETL layer, it also offers business metadata layer for keeping all the business metadata related to the organization and the project. The data which is proposed to be



stored in the crime repository will be of historical nature, further a part of this data will come from legacy systems which have been in existence for decades, based on the condition of the data the cleansing activities will be planned. Solution should ensure accuracy, integrity, consistency, redundancy, de-duplication, clarity, timeliness and adherence to data integrity rules. The de-duplication engine will remove duplicates, cross-reference matching records, survive a single complete record, validate and enrich data

Formation of Data Lake:

- Database Administrator will equip police with actionable intelligence and analytical capabilities and also set up a BI & Analytics engine which will process the data from data warehouse. Shall perform the planning and process optimization. Following are the key functionalities envisaged from the this engine Perform intelligent search and heuristics on the integrated view of information.
- Identification of hidden and unobvious relationships and patterns leading to faster and accurate investigation and crime prevention.
- Forecast future criminal occurrences and determine areas that can be statistically defined as Hotspots.
- Generate intelligence using unstructured data.
- Dynamic Risk Assessment for rapidly changing circumstances for an operational incident, in order to implement the control measures necessary to ensure an acceptable level for safety
- Optimization of resources and operations.

NOC & Network Analyst Responsibility:

The network analyst will design, maintain, configure & monitor infrastructure like the core router, Network switch, Firewall, WAF, SD WAN as per functional requirement of the project. Network Analyst will be in DC and will also responsible for implementation of Security & Network Policies & Guidelines. He will also be helping CDAC & Third Party Auditor to help and assist for the reports required for audit purpose. Network Analyst will be responsible to configure field network & MPLS on Multicast and ensure the MPLS SLA should be as per the RFP/requirement to ensure data from the field systems and other locations. The network & security infrastructure will also include the transmission from DC to Near DR, All the data from Field to respective locations of C3i, C2i, Near DR & C4i. Security infrastructure will also include secured network and firewall, Antivirus, DLP, MFA to ensure the information residing at the DC-Near DR is protected from unauthorized access and malicious attacks from external sources.

Operators /Administrative Staff Responsibility:

There are client stations which include monitoring screens using which the operators at C4i shall monitor the camera feeds, log incidents and trigger SOPs. Centralized Helpdesk System should have integration with Network/Server Monitoring Systems so that the Helpdesk Operators can to associate alarms with Service Desk tickets to help surveillance operators that for what particular alarms corresponding helpdesk tickets got logged. The video feeds of surveillance cameras can also be viewed at each Police Stations of their respective jurisdiction by the operators sitting at C2i, C3i. All analyzed data and actionable



information / alerts would then be passed on for necessary action from the C4i Operator to Emergency Operation Centre where the Police Officials will validate and approve the information should be passed for necessary action to the MDT installed in the PCR vans (Prakhar) / Police stations through to the upgraded Dial-112 system and Mobile Device. The command and control is thus envisaged to help communicate, dispatch resources, coordinate response and carry out the complete incident management by operators at C4i.

The C4i Operator will also monitor, manage and disseminate alerts and information from all of the disparate video and security systems. The operations center will also conduct intelligent video analytics processing and third party data mining analysis on real-time basis. The Operator will have a graphical user interface for search, replay and dubbing which includes the ability to simultaneously search and replay recorded telephone, VOIP, Screen recording, GPS data on GIS maps, conventional and digital radio channels as well as trunked radio communications using captured data from system without any extraneous process by the operator also.

An operator shall also be able to browse to any 3rd party VMS web interface and access it from the built-in web interface of this VMS/IP camera.

SOC Administrator:

- Need to Analyze various logs of all devices and Applications
- To perform Threat Intelligence
- Event and Incident Management
- Anomalies pertaining network traffic (LAN /WAN)
- Analyze Application Access Patterns

2.1.19. Liquidated Damages

If MSI fails to supply, install or maintain any or all of the goods and services the period of Installation, Commissioning, Operation & Maintenance, Warranty and CAMC, C-DAC without prejudice to its other rights and remedies under the Contract, would deduct from the amount payable to MSI, as Liquidated Damages, a sum equivalent to half percent (0.5 %) of the price of the delayed goods or unperformed services for each and every week (part of a week being treated as a full week) of delay until actual delivery or performance, up to a maximum deduction of Ten (10%) percent of the price of undelivered goods or unperformed services.

- a. The MSI shall note that the Downtime for each Fault occurrence which shall be considered and computed independently.
 - i. The Downtime due to system migration, testing, preventive works or other works as approved by C-DAC or involvement of cameras in third party damage or due to fault in lease line connectivity (only in case of Master System Integrator or Vendors other than ISP, but it should be mentioned/indicated/ deducted in the claim of lease line charges furnished by Internet Service Provider) shall not be considered as Faults.

2.1.20. Penalties for Non/Under Performance

C-DAC reserves the right to levy and recover the penalties in case of non/under performance for the reasons attributed to the MSI. The nature, quantum and method of



computing these penalties shall be based on SLAs described at Para 4.13 Chapter 4 of this document.

2.1.21. Termination

C-DAC may, terminate this Contract in whole or in part by giving MSI a prior and written notice of 30 days in advance indicating its intention to terminate the Contract under the following circumstances:

- a. Where C-DAC is of the opinion that there has been such Event of Default on the part of MSI / MSI's Team which would make it proper and necessary to terminate this Contract and may include failure on the part of MSI to respect any of its commitments with regard to any part of its obligations under its Bid, the RFP or under this Contract.
- b. Where it comes to C-DAC's attention that MSI (or MSI's Team) is in a position of actual conflict of interest with the interests of C-DAC/Delhi Police, in relation to any of terms of MSI's Bid, the RFP or this Contract.
- c. Where MSI's ability to survive as an independent corporate entity is threatened or is lost owing to any reason whatsoever, including inter-alia the filing of any bankruptcy proceedings against MSI, any failure by MSI to pay any of its dues to its creditors, the institution of any winding up proceedings against MSI or the happening of any such events that are averse to the commercial viability of MSI. In the event of the happening of any events of the above nature, C-DAC shall reserve the right to take any steps as are necessary, to ensure the effective transition of the sites pilot site to a successor agency, and to ensure business continuity
- d. Termination for Insolvency: C-DAC may at any time terminate the Contract by giving written notice to MSI, without compensation to MSI, if MSI becomes bankrupt or otherwise insolvent, provided that such termination shall not prejudice or affect any right of action or remedy which has accrued or shall accrue thereafter to C-DAC.
- e. MSI may, subject to approval by C-DAC, terminate this Contract before the expiry of the term by giving C-DAC a prior and written notice at least 3 months in advance indicating its intention to terminate the Contract.
- f. MSI is expected to mobilize project team for commencement of work. Commencement of work means reporting and availability of MSI resources (90% Key personnel as per the RFP requirement at C-DAC office for the project within 30 days from the Award of the Contract and remaining 10% in next 15 days)

2.1.22. Consequence of Termination

- a. In the event of termination of the Contract due to any cause whatsoever, whether consequent to the stipulated Term of the Contract or otherwise C-DAC shall be entitled to impose any such obligations and conditions and issue any clarifications as may be necessary to ensure an efficient transition and effective business continuity of the project which MSI shall be obliged to comply with and take all available steps to minimize loss resulting from that termination/breach, and further allow and provide all such assistance to C-DAC and/ or the successor agency/ service provider, as may be required, to take over the obligations of MSI in relation to the execution/continued execution of the requirements of the Contract.



- b. Where the termination of the Contract is prior to its stipulated term on account of a Default on the part of MSI or due to the fact that the survival of MSI as an independent corporate entity is threatened/has ceased, or for any other reason, whatsoever, C-DAC, through unilateral re-determination of the consideration payable to MSI, shall pay MSI for that part of the Services which have been authorized by C-DAC and satisfactorily performed by MSI up to the date of termination. Without prejudice to any other rights, C-DAC may retain such amounts from the payment due and payable by C-DAC to MSI as may be required to offset any losses caused to C-DAC as a result of any act/omissions of MSI. In case of any loss or damage due to default on the part of MSI in performing any of its obligations with regard to executing the Schedule of Requirements under the contract, MSI shall compensate C-DAC for any such loss, damages or other costs, incurred by C-DAC. Additionally, members of its team shall perform all its obligations and responsibilities under the Contract in an identical manner as were being performed before the collapse of MSI as described above in order to execute an effective transition and to maintain business continuity. All third parties shall continue to perform all/any functions as stipulated by C-DAC and as may be proper and necessary to execute the Schedule of Requirements under the Contract in terms of MSI's Bid, the Bid Document and the Contract
- c. Nothing herein shall restrict the right of C-DAC to invoke the Bank Guarantee and other Guarantees furnished solely for the material breach committed / deviation in contract by the MSI hereunder and pursue such other rights and/or remedies that may be available to C-DAC under law.
- d. The termination hereof shall not affect any accrued right or liability of either Party nor affect the operation of the provisions of the Contract that are expressly or by implication intended to come into or continue in force on or after such termination.

2.1.23. Limitation of Liability:

Limitation of MSI's Liability towards C-DAC:

- a. Neither Party shall be liable to the other Party for any indirect or consequential loss or damage (including loss of revenue and profits) arising out of or relating to the Contract.
- b. Except in case of negligence or misconduct on the part of MSI or on the part of any person or company acting on behalf of MSI in carrying out the Services, MSI's liability will be limited to the unpaid amount of total Contract value.
- c. However, liability of the bidder in case of death, injury, damage caused to the personnel/property due to/arising out of/incidental to any act/omission/default/deficiency of bidder/contractor, will be at actuals.
- d. In no event shall either Party, its officers, directors, or employees be liable for any form of incidental, consequential, indirect, special or punitive damages of any kind.
- e. MSI, with respect to damage caused by MSI to C-DAC's property, shall not be liable to C-DAC:
 - For any direct loss or damage that exceeds (A) the total payments payable under the Contract to MSI hereunder, or (B) the proceeds MSI may be entitled to receive from any insurance maintained by MSI to cover such a liability, whichever of (A) or (B) is higher.
- f. This limitation of liability shall not affect MSI liability, if any, for damage to Third Parties caused by MSI or any person or company acting on behalf of MSI in carrying out the Services.



2.1.24. Indemnity

- a. MSI shall indemnify C-DAC from and against any costs, loss, damages, expense, claims including those from third parties or liabilities of any kind howsoever suffered, arising or incurred inter alia during and after the Contract period out of:
 - any gross negligence or misconduct act or omission by MSI or any third party associated with MSI in connection with or incidental to this Contract; or
 - any infringement of patent, trademark/copyright or industrial design rights arising from the use of the supplied goods and related services or any part thereof
- b. MSI shall also indemnify C-DAC against any privilege, claim or assertion made by a third party with respect to right or interest in, ownership, mortgage or disposal of any asset, property etc. Solely arising out of the actions of MSI and its Sub Contractor. Regardless of anything contained (except for MSI's liability for bodily injury and/ or damage to tangible and real property for which it is legally liable and its liability for patent and copyright infringement in accordance with the terms of this Agreement) the total liability of MSI, is restricted to the total value of the contract.

2.1.25. Security and Safety

- a. MSI shall comply with the directions issued from time to time by C-DAC and the standards related to the security and safety, in so far as it applies to the provision of the Services.
- b. MSI shall upon reasonable request by C-DAC, or its nominee(s) participate in regular meetings when safety and information technology security matters are reviewed.
- c. MSI shall arrange for safe and secure custody/storage of material received/delivered at site/s, at their own cost and risk. The MSI is advised to secure the said material with sufficient and suitable insurance cover.

2.1.26. Ownership of Material:

All risks, responsibilities, liabilities in respect of goods delivered at site shall remain with selected bidder till they are successfully installed and commissioned at site and taken over by end users. Part deliveries shall not be treated as deliveries. Only full deliveries of all items ordered will be considered as delivery.

2.1.27. Confidentiality

- a. MSI shall not, either during the term or after expiration of this Contract, disclose any proprietary or confidential information relating to the Services/Contract and/or C-DAC/Delhi Police's business/ operations, information, Application/software, hardware, business data, architecture schematics, designs, storage media and other information / documents without the prior written consent of C-DAC.
- b. C-DAC reserves the right to adopt legal proceedings, civil or criminal, against MSI in relation to a dispute arising out of breach of obligation by MSI under this clause.
- c. MSI shall do everything reasonably possible to preserve the confidentiality of the Confidential Information including execution of a confidentiality agreement with C-DAC to the satisfaction of C-DAC.



- d. MSI shall notify C-DAC promptly if it is aware of any disclosure of the Confidential Information otherwise than as permitted by the Contract
- e. MSI shall be liable to fully recompense C-DAC for any loss of revenue arising from breach of confidentiality.
- f. For the avoidance of doubt, it is expressly clarified that the aforesaid provisions shall not apply to the following information:
 - Information already available in the public domain;
 - Information which has been developed independently by the MSI;
 - Information which has been received from a third party who had the right to disclose the aforesaid information;
 - Information which has been disclosed to the public pursuant to a court order.
- g. Any handover of the confidential information needs to be maintained in a list, both by MSI & C-DAC, containing at the very minimum, the name of provider, recipient, date of generation of the data, date of handing over of data, mode of information, purpose and signatures of both parties.
- h. The requirement of this clause shall continue even after termination or completion of this Contract.

2.1.28. Events of Default by MSI

The failure on the part of MSI to perform any of its obligations or comply with any of the terms of this Contract shall constitute an event of default (the “Event of Default”) on the part of MSI. The Events of Default are but not limited to:

- a. MSI’s Team has failed to perform any instructions or directives issued by C-DAC which it deems proper and necessary to execute the scope of work or provide services under the Contract;
- b. MSI’s Team has failed to confirm / adhere to any of the key performance indicators as laid down in the Key Performance Measures / Service Levels, or if MSI has fallen short of matching such standards / benchmarks / targets as C-DAC have designated with respect to the system or any goods, task or service, necessary for the execution of the scope of work and performance of services under this Contract. The above mentioned failure on the part of MSI may be in terms of failure to adhere to performance, quality, timelines, specifications, requirements or any other criteria as defined by C-DAC;
- c. MSI has failed to remedy a defect or failure to perform its obligations in accordance with the specifications issued by C-DAC, despite being served with a default notice which laid down the specific deviance on the part of MSI/ MSI’s Team to comply with any stipulations or standards as laid down by C-DAC; or
- d. MSI/ MSI’s Team has failed to adhere to any amended direction, instruction, modification or clarification as issued by C-DAC during the term of this Contract and which C-DAC deems fit, proper and necessary for the execution of the scope of work under this Contract.
- e. MSI/ MSI’s Team has failed to demonstrate or sustain any representation or warranty made by it in this Contract, with respect to any of the terms of its Bid, the RFP and this Contract.



- f. There is a proceeding for bankruptcy, insolvency, winding up or there is an appointment of receiver, liquidator, assignee, or similar official against or in relation to MSI.
- g. MSI's Team has failed to comply with or is in breach or contravention of any applicable laws.
- h. Where there has been an occurrence of such defaults inter alia as stated above, C-DAC shall issue a notice of default to MSI, setting out specific defaults / deviances / omissions / non-compliances / non-performances and providing a notice of thirty (30) days to enable such defaulting party to remedy the default committed.
- i. Where despite the issuance of a default notice to MSI by C-DAC, MSI fails to remedy the default to the satisfaction of C-DAC, C-DAC may, where it deems fit, issue to the defaulting party another default notice or proceed to contract termination.

2.1.29. Severability and renegotiation

Should any provision of this Contract for any reason be declared invalid or un-enforceable by an order of any court of competent jurisdiction or any arbitral body pursuant to the provisions of arbitration hereof, such decision shall not affect the validity of the remaining provisions, while remaining provisions shall remain in full force and effect as if this Contract has been executed with the invalid or unenforceable provisions hereof eliminated. In the event any such provision of the Contract is so declared invalid or unenforceable, the Parties shall promptly renegotiate in good faith new provisions to eliminate such invalidity or un-enforceability and to restore this Contract as near as possible to its original intent and effect.

2.1.30. Non-Waiver:

The failure or neglect by MSI to enforce any of the terms of this Contract shall not be construed as a waiver of its rights preventing subsequent enforcement of such provision or recovery of damages for breach thereof.

2.1.31. Fall Clause:

The bidder shall undertake that the price charged/finalized for the store/services supplied under the tender shall in no event exceed the lowest price at which the bidder offers the store/services of identical description to the other organization during the currency of contract. If at any point of time during the period, the seller reduces the sale price, sells or offer to sell such store/service to any other organization including the Buyer at a price lower than the price chargeable under the present tender, he shall notify such reduction within 7 (Seven) days and the price payable under the contract shall stand correspondingly reduced. An undertaking shall be submitted by the bidder in this regard with the technical bid.

2.1.32. Jurisdiction

This document including the Contract Document shall be governed by and construed in accordance with the laws of India and exclusive jurisdiction of the Courts of Pune would lie.

2.2. General Conditions of Contract (GCC)

2.2.1. Term and Extension of the Contract



- a. The contract with the selected MSI shall remain valid till all the contractual obligations of the contract are fulfilled/discharged by MSI.
- b. The MSI shall be responsible to provide services for a period as stipulated in extension document.
- c. If the delay occurs due to circumstances beyond control of MSI such as strikes, lockouts, fire, accident, defective materials, delay in approvals or any cause whatsoever beyond the reasonable control of MSI, a reasonable extension of time shall be granted by C-DAC.
- d. C-DAC shall reserve the sole right to grant any extension to the term above mentioned and shall notify in writing to MSI, at least 3 (three) months before the expiration of the Term hereof, whether it shall grant MSI an extension of the Term. The decision to grant or refuse the extension shall be at C-DAC's discretion and such extension of the Contract, if any, shall be as per terms agreed mutually between C-DAC and MSI.
- e. Where C-DAC is of the view that no further extension of the term be granted to MSI, C-DAC shall notify MSI of its decision at least 3 (three) months prior to the expiry of the Term. Upon receipt of such notice, MSI shall continue to perform all its obligations hereunder, until such reasonable time beyond the Term of the Contract within which, C-DAC shall either appoint an alternative agency/MSI or create its own infrastructure to operate such Services as are provided under this Contract.
- f. Force Majeure shall not include any events caused due to acts/ omissions of MSI resulting in a breach/ contravention of any of the terms of the Contract and/or MSI's Bid. It shall also not include any default on the part of MSI due to its negligence or failure to implement the stipulated/ proposed precautions, as were required to be taken under the Contract.
- g. In case, the contract is extended, the MSI shall be responsible for: -
 - i. MSI shall carry out comprehensive on-site maintenance work including all required labour, tools, equipment, facilities, material (including temporary materials), adequate consumables and spares to perform Preventive Maintenance and Repair Maintenance on all hardware and software.
 - ii. The period of Maintenance shall be for a period as stipulated in the extension document, after expiry of the warranty period.
 - iii. CAMC may be further extended on the rates already offered by the MSI in the Bid.
 - iv. Contract Agreement for CAMC period will be extended after completion of period of present agreement, on the rates already offered by MSI within this contract.
 - v. The payment towards CAMC shall be payable to MSI quarterly after successful completion of the maintenance service during that period.
 - vi. The Quarterly Preventive Maintenance and diagnostics of the system on all the locations should be carried out by the MSI, during the CAMC period.
 - vii. During the period of CAMC, MSI shall ensure that the service/repair calls are to be attended within four (04) hours from the time of such calls. The defective card/item/equipment etc. should be repaired within 48 hours. In case of major defects requiring the defective card/item/equipment etc. to be taken to workshop, an immediate substitute card/item/equipment will be provided by the MSI for the smooth operation of the System and the defective card/item/equipment etc. should be returned/installed duly repaired within six weeks. The to and fro transportation of the card/item/equipment etc. will be the responsibility of MSI.
 - viii. Delays in attending the calls and or repairing the defective equipment beyond time limit given in this Clause, without providing the substitute or without



sufficient reason, will attract penalties. CAMC charges of the delayed period will not be paid if the delay is more than Six (06) hours from the specified time limit on pro-rata basis.

- ix. In case, MSI fails to perform any of the Services of the Contract within the time period specified in the tender, the C-DAC shall, without prejudice to its other remedies under the tender, deduct from, the pending bills/Performance Security, by way of penalty a sum equivalent to One (01) % for every week (part of a week being treated as full week) of delay until actual performance up to a maximum of 05% of the undelivered services/equipment.
- x. The MSI shall not retract from the responsibilities under the CAMC Contract once the Agreement is signed. However, in the unlikely case of violation, the C-DAC will be at liberty to forfeit the Performance Security and make recoveries from the MSI besides initiating legal proceedings against the MSI.

2.2.2. Dispute Resolution

Any dispute or difference between the parties arising out of this Contract shall in the first place be settled by mutual negotiations between the Heads of the organizations or their nominees and their decision shall be final and binding on the organizations.

- a. If the dispute or difference is not resolved as per the above clause within 30 days, it shall be referred to an arbitrator to be mutually agreed by both the parties. The provisions of Arbitration and Conciliation Act, 1996 and the rules there under shall be followed. Any statutory modification thereof for the time being in force shall be deemed to apply to the arbitration proceedings under this clause.
- b. The award of the arbitrator shall be final and binding on the parties.
- c. The common cost of the arbitration proceeding shall initially be borne equally by the parties and finally by the party against whom the award is passed. Any other costs or expenses incurred by a party in relation to the arbitration proceedings shall ultimately be borne by the party as the arbitrator may decide.
- d. The venue of the arbitration shall be Pune. The language of arbitration shall be English. Courts in Pune only shall have the exclusive jurisdiction to try, entertain and decide the matters which are not covered under the Arbitration and conciliation Act.
- e. Any letter, notice or other communications dispatched to MSI relating to either arbitration proceeding or otherwise whether through the post or through a representative on the address last notified to C-DAC by MSI shall be deemed to have been received by MSI although returned with the remarks, refused 'undelivered' where about not known or words to that effect or for any other reasons whatsoever.

2.2.3. Time is of the essence

Time shall be of the essence in respect of any date or period specified in this Contract or any notice, demand or other communication served under or pursuant to any provision of this Contract and in particular in respect of the completion of the activities by MSI by the specified completion date herein and/ or the RFP.

2.2.4. Conflict of interest



MSI shall disclose to C-DAC in writing, all actual and potential conflicts of interest that exist, arise or may arise (either for MSI or MSI's Team) in the course of performing the Services as soon as practical after it becomes aware of that conflict.

2.2.5. Publicity

MSI shall not make or permit to be made a public announcement or media release about any aspect of this Contract unless C-DAC first gives MSI its written consent.

2.2.6. Insurance

- a. The all Goods supplied under this Contract shall be comprehensively insured by MSI at his own cost, against any loss or damage, for the entire period of the Contract. MSI shall submit to C-DAC, documentary evidence issued by the insurance company, indicating that such insurance has been taken.
- b. MSI shall take out and maintain at its own cost, on terms and conditions approved by C-DAC, insurance against the risks, and for the coverages, as specified below :

At C-DAC's request, shall provide evidence to C-DAC showing that such insurance including all risks insurance for the value of contract has been taken out and maintained and that the current premiums therefore have been paid.

Employer's liability and workers' compensation insurance in respect of the Personnel of the Company, in accordance with the relevant provisions of the Applicable Law, as well as, with respect to such Personnel, any such life, health, accident, travel or other insurance as may be appropriate

- c. Insurance requirements

Type of Cover	Minimum cover for Insurance	
(i)	Goods and materials	The sum stated in the Agreement plus 20%
(ii)	Loss or damage to equipment	Full replacement cost
(iii)	Loss or damage to property of Third Party	Full replacement cost
(iv)	Personal injury or death insurance (b) For Third Party Rs 20.00 lakhs at Rs 5.00 lakhs for 4 persons. (c) For Contractor's employees or labor In accordance with the statutory requirements applicable as per the prevalent laws laid down from time to time by the government of Delhi NCT.	

2.2.7. Project Audits and Testing

The following types of Audits are required to be conducted under the project.

- a. Internal Audit (Half yearly for Network & Applications and operations) (sr no 2.16 of price bid format)
 - b. External Audit (Yearly for Network & Applications and operations) (sr no 2.17 of price bid format)
 - c. Third Party Audit
- Internal and External Audit will be conducted by MSI as scheduled.



C-DAC/Delhi Police will have the right to engage a Third Party for quality assurance. MSI will have to ensure compliance of the findings made by the third party so engaged, duly authorized by the C-DAC/Delhi Police, with regard to specifications, Tests, Quality and Material used for the Safe City Project of Delhi Police.

Though the third party audit will be arranged by C-DAC/Delhi Police, the MSI shall be responsible for arranging the setup required for such Audits. The MSI should extend their fullest cooperation for such Audits.

The brief scope for the Audits is as stipulated below.

A. Network Audit

Delhi Police will have the right to engage a Third party for quality assurance. There will be third party network audit to be conducted on yearly basis by CERT-In empaneled agencies. Total Service Provider will have to ensure compliance of the advice/suggestions made by the third party so engaged, dually authorized by the Delhi Police, with regard to specifications, Tests, Quality and Material used for the Safe City Project of Delhi Police. However, such advice/ suggestions have to be well within the scope of the project as framed in this agreement. The MSI will coordinate with ISP to ensure successful closure of the Audit by maintaining its all infrastructure (hardware and software) platforms up and running which might impact the purposed Audit adversely bandwidth Estimation.

The network implementation activities, which include laying of OFC and recurring bandwidth may be opted for distinct and parallel set of activities with respect to the other bundle of activities mentioned in this DPIP.

B. Security Risk Audits

It must be ensured that ISO 27001 (ISMS) Security Audits must be conducted yearly or as per the requirement of management to mitigate risk in regular operations and to stay compliant.

C. Implementation and Performance Audit

- a. The project implementation upon completion will undergo a complete implementation audit in terms of contractual role and responsibilities of the MSI or ISP. The third party audit will be conducted by CERT-In empanelled agency on behalf of C-DAC (TSP). The report will be submitted to Delhi Police.
- b. The performance audits by the aforementioned Third Party will be conducted every year by CERT-IN empanelled agency covering important parameters like networking, security, desired system performance as per terms of reference of RFP.

The proposed solution by MSI to the RFP requirement should support requirements of the auditors requiring technical audit of the whole system, which bidder should allow the auditors to access the system.

The required testing measures include:

- a. Factory Acceptance Testing



- b. User Acceptance Testing/ Final Acceptance Testing and conducting the prelaunch security audit of applications.

2.2.8. Final Acceptance at Site Test Procedure (FAT Procedure):

The MSI shall submit to the C-DAC the finalized FAT Procedure within 60 days from the date of signing of contract agreement. The MSI will get approval on FAT Procedure from C-DAC and assist C-DAC to get it approved from Delhi Police. Inspection and Testing of the system shall be performed in accordance with the FAT Procedure. The successful completion of the FAT Procedure will be the sole criterion for Final Acceptance of the System.

- a. For the purpose of taking over the system, Final Acceptance Testing shall be carried out at Delhi.
- b. After the system is fully installed, optimized and ready for the Final Acceptance Testing, the same will be carried out to validate system features and functional operation in the field in accordance with the FAT Procedure.
- c. An Inspection Team comprising the authorized nominees of the C-DAC respectively shall carry out the Final Acceptance Testing.
- d. The Inspection team shall test the complete system to ensure that the System meets the Agreed Specifications.
- e. After receipt of intimation of completion of FAT procedure and certificate of inspection by MSI, C-DAC will inspect the project and make a list of deficiencies, if any, noticed during this inspection and the same will be rectified/removed by the of MSI.
- f. MSI shall assists C-DAC to get the Final Acceptance of the project from Delhi Police.

Before final acceptance the component wise verification shall be conducted which will involve scrutiny of documents for various IT / Non-IT components to verify if the specifications conform to the technical and functional requirements mentioned in the RFP and subsequent corrigendum. CDAC reserves the right to conduct physical inspection of the equipment delivered to ensure that they arrive at the sites in good condition and are free from physical damage and incomplete shipments and shall return the products to the supplier at the supplier's expenses if required quality is not maintained. Physical inspection of hardware will also include physical checking and counting of the delivered equipment in presence of the Successful Bidder. This equipment will only be acceptable as correct when each received item corresponds with the checklist that will be prepared by the Successful Bidder prior to shipment. Any shortfalls in terms of number of items received may render the delivered equipment incomplete.

After successful installation of equipment in accordance with the requirements in the RFP, the Successful Bidder would need to carry out testing in 2 different phases - (a) Unit Testing and (b) Integration Testing. These tests would be carried out based on the test cases developed and validated by the CDAC. Apart from the functional testing of the entire system components, the testing would also verify following aspects:

- Configuration Testing (to ensure that all the components are configured properly)
- Security Testing (to review & evaluate security controls)
- Resilience and recovery testing- Resilience testing will confirm that the system can recover from expected or unexpected events without loss of data or functionality.



While recovery testing confirms that the affected system can be restarted successfully after an outage.

- Use Cases testing.

2.2.9. Transfer of Ownership

MSI must transfer all titles to the assets and goods procured for the purpose of the Project to C-DAC at the time of Acceptance of System. This includes all licenses, titles, source codes, certificates, hardware, devices, equipment etc. related to the system designed, developed, installed and maintained by MSI as a part of the implementation of the Project. MSI is expected to provide source codes, transfer IPRs and ownership rights of only those solutions which would be customized by MSI for the use of C-DAC.

Forthwith upon expiry or earlier termination of the Contract and at any other time on demand by C-DAC, MSI shall deliver to C-DAC, all Documents provided by or originating from C-DAC and all Documents produced by or from or for MSI in the course of performing the Services, unless otherwise directed in writing by C-DAC at no additional cost. MSI shall not, without the prior written consent of C-DAC store, copy, distribute or retain any such Documents.

2.2.10. Exit Management Plan

- A. An Exit Management plan shall be furnished by MSI in writing to C-DAC within 150 days from the date of signing the Contract, which shall deal with at least the following aspects of exit management in relation to the Contract as a whole and in relation to the Project Implementation, and Service Level monitoring:
 - i. A detailed program of the transfer process that could be used in conjunction with a Replacement Service Provider including details of the means to be used to ensure continuing provision of the services throughout the transfer process or until the cessation of the services and of the management structure to be used during the transfer;
 - ii. Plans for provision of contingent support to the Replacement Service Provider for a reasonable period after transfer.
 - iii. Exit Management plan in case of normal termination of Contract period
 - iv. Exit Management plan in case of any eventuality due to which Project is terminated before the contract period.
 - v. Exit Management plan in case of termination of MSI
- B. **Exit Management plan at the minimum shall adhere to the following :**
 - i. Three (03) months of support to Replacement Service Provider post termination of the Contract;
 - ii. Complete handover of the Planning documents, bill of materials, functional requirements specification, technical specifications of all equipment, change requests if any, sources codes, wherever applicable, reports, documents and other relevant items to the Replacement Service Provider/ C-DAC; Source code for any modifications done for the project shall be property of the C-DAC / Delhi Police.
 - iii. Certificate of Acceptance from authorized representative of Replacement Service Provider issued to MSI on successful completion of handover and knowledge transfer.



- C. In the event of termination or expiry of the Contract, either during Project Implementation or Service Level monitoring, both MSI and C-DAC shall comply with the Exit Management Plan.
- D. During the Exit Management period, MSI shall use its best efforts to deliver the services.

2.2.11. Intellectual Property Rights

- a. Retention of Ownership: Except for the rights expressly granted to the Licensee under this Contract, the Licensor shall retain all right, title and interest in and to the Licensed Technology of the software/solution, including all worldwide Technology and intellectual property and proprietary rights.
- b. Preservation of Notice Licensee shall not remove, efface or obscure any copyright notices or other proprietary notices or legends from any Licensed Technology or materials provided under this Contract, and shall reproduce all such notices and legends when incorporating Licensed Technology or materials into any Integrated Products.
- c. MSI must ensure that while using any software, hardware, processes, document or material in the course of performing the Services, it does not infringe the Intellectual Property Rights of any person/Company. MSI shall keep C-DAC indemnified against all costs, expenses and liabilities whatsoever, arising out of any illegal or unauthorized use (piracy) or in connection with any claim or proceedings relating to any breach or violation of any permission/license terms or infringement of any Intellectual Property Rights by MSI or MSI's Team during the course of performance of the Services. MSI's liability is excluded regarding any claim based on any of the following (a) anything C-DAC provides which is incorporated into the Solution; (b) C-DAC's modification of the solution; (c) the combination, operation, or use of the solution with other materials, if the third party claim has been caused by the combination, operation or use of the solution
- d. C-DAC shall own and have a right in perpetuity to use all newly created Intellectual Property Rights which have been developed solely during execution of this Contract, including but not limited to all processes, products, specifications, reports and other documents which have been newly created and developed by MSI solely during the performance of Services and for the purposes of inter-alia use or sub-license of such Services under this Contract. MSI undertakes to disclose all such Intellectual Property Rights arising in performance of the Services to C-DAC, execute all such agreements/documents and obtain all permits and approvals that may be necessary in regard to the Intellectual Property Rights of C-DAC.
- e. If C-DAC desires, MSI shall be obliged to ensure that all approvals, registrations, licenses, permits and rights etc. which are inter-alia necessary for use of the goods supplied / installed by MSI, the same shall be acquired in the name of C-DAC, prior to termination of this Contract and which may be assigned by C-DAC to MSI for the purpose of execution of any of its obligations under the terms of the Bid, Tender or this Contract. However, subsequent to the term of this Contract, such approvals, registrations, licenses, permits and rights etc. shall endure to the exclusive benefit of C-DAC.
- f. MSI shall not copy, reproduce, translate, adapt, vary, modify, disassemble, decompile or reverse engineer or otherwise deal with or cause to reduce the value of the Materials except as expressly authorized by C-DAC in writing.



- g. The MSI shall indemnify the C-DAC and Delhi Police against all third party claims of infringement of patent, trademark or industrial design rights arising from the use of the Equipment or any part thereof.

2.2.12. Failure to agree with the Terms & Conditions of the RFP

Failure of the Successful Bidder to agree with the Terms & Conditions of the RFP shall constitute sufficient grounds for the annulment of the LOI, in which event C-DAC may award the contract to the next best value Bidder or call for new Bids.

In such a case, C-DAC shall forfeit the Performance Bank Guarantee and/or forfeit the EMD as the case may be of such Successful Bidder/ MSI.

(End of Chapter – 2)



Chapter 3. Schedule of Requirements

3.1. SoR Format

3.1.1. Hardware and Software and Networking Components

Sr. No	Description	Unit	Total Quantity	Phase 1-quantity	Make	Model/Part No
Integrated Command, Control, Communication and Compute Centre at PHQ Delhi (C4I)- PHQ (Phase 1 only)						
I	Hardware components					
1	Video Wall Solution- 70" cubes in a 4 X 4 arrangement 3 Video Walls	Nos.	48	48		
2	Video Wall Controller	Nos.	4	4		
3	LED Monitor- 55" cubes in a 1 X 2 arrangement	Nos.	4	4		
4	Workstation for LED Monitors	Nos.	2	2		
5	Workstations with 3 nos. 24" UHD Touch Monitors for C4I application at multiple rooms on 6th & 7th Floor (EoC) Mike + webcam +speaker along with operator workstation	Nos.	16	16		
6	Video Wall Software	Lot.	1	1		
7	Workstations with 3 nos. 24" UHD touch Monitors for C4I application with Mike + webcam +speaker along with operator workstation	Nos.	21	21		
8	Network Colour Laser Printer	Nos.	5	5		
9	IP Phones	Nos.	39	39		
10	Civil, Interior, Electrical, Networking, Carpet, Furniture and Security, Chairs	Lot.	1	1		
11	Display port/ HDMI splitter (for C4i & C3i + C2i)	Nos.	50	50		
12	Racks 42U with Smart PDU	Nos.	2	2		
13	Workstation for Video wall without Monitor	Nos.	16	16		
14	Switch L2	Nos.	14	14		
15	Joystick for PTZ camera at Workstation	Nos.	39	39		
16	55" LED TV	Nos.	4	4		
17	Dual TV Stand With Power distribution	Nos.	2	2		



Sr. No	Description	Unit	Total Quantity	Phase 1-quantity	Make	Model/ Part No
II	Software components					
18	C4I Software including following modules -					
	Software Component (Unit Price)					
	1.ICCC Base platform with GIS engine, reporting, real-time dashboard, User Interface and Alarm Management with unrestricted client connections	Nos.	1	1		
	2. Threat Level Engine					
	3. Big data correlation Tool with crime insights					
	4. Incident Management, Rules Engine, Decision Management and collaboration tool					
	5.Active directory Integration or equivalent					
	6. Mobile App with unrestricted connections					
19	Automatic Vehicle Location System (AVLS)	Nos.	1	1		
20	Computer Aided Dispatch Software (CAD)	Nos.	1	1		
21	GPS Location Based Services and Software	Nos.	1	1		
22	Video Management & Recording Software – 10,000 camera licenses + 1000 cameras floating licensing for existing camera integration	Nos.	11000	11000		
23	Video Analytics Software for 2500 cameras (2 use cases on an average per camera)	Nos.	5000	5000		
24	Face Recognition Software for 370 FRS channels	Nos.	370	370		
25	Automatic Number/ License Plate Recognition Software with licensing	Nos.	1622	1622		
26	Video Summarization and Forensic Software	Nos.	1	1		
27	PIU (Picture Intelligence Unit) Software	Nos.	1	1		
28	Customized Interface software for integration with	Nos.	1	1		
	1. Community Surveillance					



Sr. No	Description	Unit	Total Quantity	Phase 1-quantity	Make	Model/Part No
	2. CCTNS					
	3. VAHAN					
	3. Himmat plus App					
	4. Dial 112					
	and other databases - Total 32 Interfaces (datasets)					
29	LDAP Software	Nos.	1	1		
30	SQL Server 2019 Standard License	Nos.	2	2		
31	Enterprise Management System including SLA Management, Network Management, Asset Management, Incident & Work Flow Management, Privilege & Identity Management.	Nos.	1	1		
32	Helpdesk Management	Nos.	1	1		
33	Security and networking Audits	Nos.	1	1		
34	Security Software Tools and commissioning support of all softwares- additional licenses, etc.	Lot	1	1		
#.	Description	Measuring Unit	Total Qty for the Project	Phase 1-quantity		
C3i- District Head Headquarters- phase 1, 2 & 3						
1	Workstations with 3 nos. 24" Monitors for C4I application	Nos.	57	24		
	Mike + webcam +speaker along with operator workstation					
2	LED Monitor- 55" monitor displays	Nos.	48	18		
3	Workstations for LED Display without Monitor	Nos.	16	6		
4	Network Colour Laser Printer	Nos.	16	6		
5	IP Phones	Nos.	57	24		
6	Secure Network Device	Nos.	16	6		
7	Layer 2 Network Switches - 24 Ports	Nos.	16	6		
8	Network Racks 16U	Nos.	16	6		
9	Passive Components required for completing Networking at each district headquarter as per layout and other details.	Lump Sum	16	6		



Sr. No	Description	Unit	Total Quantity	Phase 1-quantity	Make	Model/ Part No
10	10KVA UPS with 30 min battery backup at 80% load	Nos.	32	12		
11	Comfort AC 1.5/ 2 Ton	Nos.	32	12		
12	Civil, Interior, electrical, furniture, security required for completing at each district headquarter as per layout and other details.	Lump Sum	16	6		
13	Modular Furniture for workstation	Nos.	57	24		
14	Edge Gateway for Community Surveillance	Nos.	50	20		
15	Joystick for PTZ camera at Workstation	Nos.	57	24		
#.	Description	Measuring Unit	Qty.	Phase 2-quantity		
1	Workstations with 3 nos. 24" Monitors for C4I application	Nos.	57	14		
	Mike + webcam +speaker along with operator workstation					
2	LED Monitor- 55" monitor displays	Nos.	48	12		
3	Workstations for LED Display without Monitor	Nos.	16	4		
4	Network Colour Laser Printer	Nos.	16	4		
5	IP Phones	Nos.	57	14		
6	Secure Network Device	Nos.	16	4		
7	Layer 2 Network Switches - 24 Ports	Nos.	16	4		
8	Network Racks 16U	Nos.	16	4		
9	Networking Cost (Passive Components)	Nos.	16	4		
10	10KVA UPS with 30 min battery backup at 80% load	Nos.	32	8		
11	Comfort AC 1.5/ 2 Ton	Nos.	32	8		
12	Civil, Interior, electrical, furniture, security etc.	Nos.	16	4		
13	Modular Furniture for workstation	Nos.	57	14		
14	Edge Gateway for Community Surveillance	Nos.	50	12		



Sr. No	Description	Unit	Total Quantity	Phase 1-quantity	Make	Model/ Part No
15	Joystick for PTZ camera at Workstation	Nos.	57	14		
#.	Description	Measuring Unit	Qty.	Phase 3-quantity		
1	Workstations with 3 nos. 24" Monitors for C4I application	Nos.	57	19		
	Mike + webcam +speaker along with operator workstation					
2	LED Monitor- 55" monitor displays	Nos.	48	18		
3	Workstations for LED Display without Monitor	Nos.	16	6		
4	Network Colour Laser Printer	Nos.	16	6		
5	IP Phones	Nos.	57	19		
6	Secure Network Device	Nos.	16	6		
7	Layer 2 Network Switches - 24 Ports	Nos.	16	6		
8	Network Racks 16U	Nos.	16	6		
9	Networking Cost (Passive Components)	Nos.	16	6		
10	10KVA UPS with 30 min battery backup at 80% load	Nos.	32	12		
11	Comfort AC 1.5/ 2 Ton	Nos.	32	12		
12	Civil, Interior, electrical, furniture, security etc.	Nos.	16	6		
13	Modular Furniture for workstation	Nos.	57	19		
14	Edge Gateway for Community Surveillance	Nos.	50	18		
15	Joystick for PTZ camera at Workstation	Nos.	57	19		
Total for C3I						
#	Description	Measuring Unit	Quantity	Phase 1-quantity		
C2i- Police Stations- Phase 1, 2 & 3						
1	Workstations with 3 nos. 24" Monitors for C4I application Mike + webcam +speaker along with operator workstation	Nos.	240	101		
2	LED Monitor- 55" monitor displays	Nos.	81	37		



Sr. No	Description	Unit	Total Quantity	Phase 1-quantity	Make	Model/Part No
3	Workstations for LED Display without Monitor	Nos.	70	33		
4	IP Phones	Nos.	240	101		
5	Secure Network Device	Nos.	182	75		
6	Network laser printer	Nos.	182	75		
7	Layer 2 Network Switches - 24 Ports	Nos.	182	75		
8	Network Racks 16U	Nos.	182	75		
9	Networking Cost (Passive Components)	Nos.	182	75		
10	3KVA UPS with 30 min battery backup at 80% load	Nos.	174	71		
11	10KVA UPS with 30 min battery backup at 80% load	Nos.	8	4		
12	Comfort AC 1.5 ton	Nos.	182	75		
13	Civil, Interior, electrical, furniture, security etc.	Nos.	182	75		
14	Modular Furniture for additional workstation	Nos.	58	26		
15	Joystick for PTZ camera at Workstation	Nos.	240	101		
#	Description	Measuring Unit	Quantity	Phase 2-quantity		
1	Workstations with 3 nos. 24" Monitors for C4I application Mike + webcam +speaker along with operator workstation	Nos.	240	64		
2	LED Monitor- 55" monitor displays	Nos.	81	17		
3	Workstations for LED Display without Monitor	Nos.	70	13		
4	IP Phones	Nos.	240	64		
5	Secure Network Device	Nos.	182	45		
6	Network laser printer	Nos.	182	45		
7	Layer 2 Network Switches - 24 Ports	Nos.	182	45		
8	Network Racks 16U	Nos.	182	45		
9	Networking Cost (Passive Components)	Nos.	182	45		
10	3KVA UPS with 30 min battery backup at 80% load	Nos.	174	43		
11	10KVA UPS with 30 min battery backup at 80% load	Nos.	8	2		



Sr. No	Description	Unit	Total Quantity	Phase 1-quantity	Make	Model/ Part No
12	Comfort AC 1.5 ton	Nos.	182	45		
13	Civil, Interior, electrical, furniture, security etc.	Nos.	182	45		
14	Modular Furniture for additional workstation	Nos.	58	19		
15	Joystick for PTZ camera at Workstation	Nos.	240	64		
#	Description	Measuring Unit	Quantity	Phase 3-quantity		
1	Workstations with 3 nos. 24" Monitors for C4I application Mike + webcam +speaker along with operator workstation	Nos.	240	75		
2	LED Monitor- 55" monitor displays	Nos.	81	27		
3	Workstations for LED Display without Monitor	Nos.	70	24		
4	IP Phones	Nos.	240	75		
5	Secure Network Device	Nos.	182	62		
6	Network laser printer	Nos.	182	62		
7	Layer 2 Network Switches - 24 Ports	Nos.	182	62		
8	Network Racks 16U	Nos.	182	62		
9	Networking Cost (Passive Components)	Nos.	182	62		
10	3KVA UPS with 30 min battery backup at 80% load	Nos.	174	60		
11	10KVA UPS with 30 min battery backup at 80% load	Nos.	8	2		
12	Comfort AC 1.5 ton	Nos.	182	62		
13	Civil, Interior, electrical, furniture, security etc.	Nos.	182	62		
14	Modular Furniture for additional workstation	Nos.	58	13		
15	Joystick for PTZ camera at Workstation	Nos.	240	75		
Total for C2I						
#	Description	Measuring Unit	Qty require in Project	Quantity required for each phase (Phase -1 &Phase-2)		



Sr. No	Description	Unit	Total Quantity	Phase 1-quantity	Make	Model/Part No
	Mobile Command Control Vehicle (MCCV) comprising of following items per vehicle :	Nos.	02	1		
1	Custom designed & Fabricated Mobile Command Control Vehicle	Nos.	1			
2	Chassis: WB 4200mm (approx.) from reputed OEM like TATA, Eicher, Ashok Leyland etc.	Nos.	2			
3	Split Air Conditioner (1Ton)	Nos.	1			
4	Interiors design (as per the requirement)	Lump-sum	1			
5	Chairs / Seating Arrangement for two Operator and one ICS	Nos.	3			
6	Chairs / Seating Arrangement for Supervisor with mini seating area	Nos.	1			
7	Console with provision for display	Nos.	2			
8	Inter- communication Service Console	Nos.	1			
9	19" Rack with shock & vibration isolators for electronic	Nos.	1			
10	Mast	Nos.	1			
11	Storage	Nos.	1			
12	PC for Operator	Nos.	2			
13	32" LED Full HD TV	Nos.	2			
14	5KVA UPS System with Batteries for 1 hour backup	Nos.	1			
15	7.5 KVA Silent Petrol Generator Set	Nos.	1			
16	Vehicle Mast mounted PTZ Camera with Keyboard and Joystick	Nos.	1			
17	Vehicle mounted full HD Bullet Cameras	Nos.	2			
18	Industrial PC based Network Video Recorder	Nos.	1			
19	Video Management System	Lot	1			
20	Standalone Mobile Hand-held device	Nos.	1			
21	4 SIM based 4G Aggregator Device with Dongles	Nos.	1			
22	Network Hardware:- - 1 x 24Port GigE Switch	Lot	1			



Sr. No	Description	Unit	Total Quantity	Phase 1-quantity	Make	Model/ Part No
23	32" or better LED Full HD Video Display	Nos.	1			
24	Vehicle Mounted Water Dispenser	Nos.	1			
25	LED Flood Lights with 120-degree coverage (Mast Mounted)	Nos.	3			
26	Top Bar Light with Siren	Nos.	1			
27	PA System with 4 Speakers	Nos.	1			
28	Fire Extinguisher	Nos.	4			
29	First-Aid Box	Nos.	1			
30	4G Based live TV Streaming Device	Nos.	1			
31	Integration, Testing, Installation, Commissioning & Training	Nos.	1			
32	Interoperable Communication System with Operator Display, Pedal PTT, Speakers, GSM Modem, PTT Desk Mic & Record-Replay features.(Radios to be provided by end user)	Nos.	1			
33	Provision of Integration of APCO-P25 Radio Communication channel at MCCV	Nos.				
36	4G Aggregator/ Bonding Receiver with Unlimited bonding License	Lot	1			
37	SIM recurring charges for MCCV (16 SIM)- Annual	Year	5			
Total Price of 2 MCCV with 05 Years Support						
#	Description	Measuring Unit	Qty	Phase 1-quantity		
Data Centre- phase 1 only						
a	Servers					
1	C4I Servers at ICCC (PHQ)	Nos.	2	2		
2	Integration Servers	Nos.	3	3		
3	Video Management Servers	Nos.	2	2		
4	Video Recording Servers	Nos.	60	60		
5	Video Analytics Servers with 3x GPU in each server for 2500 cameras each having 2 use cases on an average	Nos.	42	42		



Sr. No	Description	Unit	Total Quantity	Phase 1-quantity	Make	Model/ Part No
6	Face Recognition Servers with 3x GPU in each server for 370 FRS Channels	Nos.	20	20		
7	AI Training and Continuous Learning Server	Nos.	2	2		
8	ANPR Servers for 1622 Channels	Nos.	44	44		
9	PIU (Picture Intelligence Unit) Server	Nos.	2	2		
10	Video Summarization/ Synopsis and Forensics Server	Nos.	4	4		
11	Domain Controller, EMS server	Nos.	2	2		
12	Antivirus Server- AI based	Nos.	2	2		
13	LDAP Server	Nos.				
14	Viewing Center Management Server	Nos.	4	4		
15	DLP Server	Nos.	2	2		
16	MFA Server + PKI Server	Nos.				
17	Total Host (combined together as specified above)	Nos.	191	191		
b	Storage					
1	Scale out Storage for surveillance video data for 30 days - 20 PB	Nos.	1	1		
2	SAN storage for database, boot, Flagged Data and Backup for 90 days - 2 PB	Nos.	1	1		
3	SAN Switches	Nos.	4	4		
c	Networking					
1	L2 Switch (100 Gbps) WAN	Nos.	2	2		
2	Layer 3 Core Switches - 48 ports 100G	Nos.	4	4		
3	Layer 2 TOR Switches - 48 Ports 10G (Storage)	Nos.	4	4		
4	L2/ KVM Management Switches	Nos.	15	15		
5	Layer 2 TOR Switches - 48Ports 10G	Nos.	15	15		
6	Racks with Smart PDU	Nos.	30	30		
d	Security					
1	Firewall- 100 gig streaming throughput	Nos.	2	2		
2	IPS & DDos for 65 Gig throughput	Nos.	2	2		
3	VAPT for 170000IP bands (IP Schema)	Nos.	1	1		
4	WAF (1 gig internet data)	Nos.	2	2		



Sr. No	Description	Unit	Total Quantity	Phase 1-quantity	Make	Model/ Part No
5	Secure Network Device	Nos.	2	2		
6	Anti-APT (sandboxing)	Nos.	2	2		
7	Anti-virus- AI Based software	Nos.	450	450		
8	Data Leakage Prevention (DLP)	Nos.	450	450		
9	SIEM Appliance	Nos.	1	1		
10	Backup Appliance & Solution	Nos.	1	1		
11	AAA Server (NAC)	Nos.	1	1		
12	Network Load Balancer	Nos.	1	1		
13	Multi-Factor Authentication (with Finger print biometric and hard token devices) at all workstations	Nos.	450	450		
14	OS for Servers, Virtualization etc.					
	Physical Servers 77 - Virtualization	Nos.	154	154		
	18 server Virtualization Security	Nos.	36	36		
	Windows OS -73 Server	Nos.	73	73		
	Additional items required if any	Lump -Sum	1	1		
e	NOC					
1	Layer 2 Network Switch 24 Ports	Nos.	2	2		
2	Wall mount 9U Rack for Switches	Nos.	1	1		
3	Workstation with single Monitor 24" for Management	Nos.	3	3		
4	IP Phone	Nos.	3	3		
5	Operator Console Desk	Nos.	3	3		
6	SMS Gateway (for alarms & notifications)	Nos.	1	1		
7	Laptop	Nos.	5	5		
8	IPPBX / Recording server + software	Nos.	1	1		
9	Installation , Configuration etc. and overall management	Nos.	1	1		
f	Non IT Component					
1	UPS (15 minutes backup) - 400 KVA	Nos.	2	2		
2	DG Set - 1000 KVA	Nos.	1	1		
g	Data Center Build					
1	Civil, Interior, Electrical, Networking, Furniture, Security, NOVEC, FAS, PAC, HVAC etc. for basement and (DC resided at)7th floor + 7th Floor strengthening for (both arms)	Nos.	1	1		



Sr. No	Description	Unit	Total Quantity	Phase 1-quantity	Make	Model/Part No
h	Operation and Maintenance					
1	Operation and maintenance cost for 4 years	Years	4	4		
Total for Data Centre						
#	Description	Measuring Unit	Qty	Phase 2-quantity		
Near Disaster Recovery Center- phase 2 only						
1	C4i servers	Nos.	11	11		
2	Video management Servers	Nos.				
3	Server (Recording)	Nos.				
4	ANPR Servers	Nos.				
5	Domain Controller	Nos.				
6	Antivirus Server	Nos.				
7	LDAP Server	Nos.				
8	Viewing Centre Management Server	Nos.	1	1		
9	Video Analytics Servers with 3x GPU in each server	Nos.	4	4		
10	Face Recognition Servers with 3x GPU in each server	Nos.	3	3		
11	Storage of application and tagged data (2 PB storage)- SAN/ Unified	Nos.	1	1		
12	L3 Switch 24 Port 10/25 GB	Nos.	2	2		
13	L2 Switch 24 Port 1GB	Nos.	2	2		
14	SAN Switch 12 port	Nos.	2	2		
15	RACK	Nos.	4	4		
16	Firewall- 3 Gig, IPS, DDos, Anti-APT, VAPT, server security- 3 GB throughput	Nos.	2	2		
17	Network Load Balancer (NLB)	Nos.	1	1		
18	Miscellaneous- Virtualization, OS for servers, etc. details are as below:					
	Virtualization Physical Servers	Nos.	12	12		
	Server Virtualization Security	Nos.	12	12		
	Windows OS –Server	Nos.	11	11		
	Civil, electrical wherever required	Nos.	1	1		
Total for Schedule DRC						
#	Description	Measuring Unit	Qty	Phase 1-quantity		



Sr. No	Description	Unit	Total Quantity	Phase 1-quantity	Make	Model/ Part No
Field Devices- phase 1, 2 & 3						
1	Outdoor Fixed Camera - 4MP	No.	6121	2,585		
2	Outdoor PTZ Camera - 4MP, 30x Optical Zoom and joystick control operations	No.	2246	951		
3	Outdoor Fixed ANPR Camera with IR Illuminator- 2 MP	No.	1622	686		
4	Poles - for Cameras with 1 mtr ARMs for fixed and PTZ	No.	3802	1,677		
5	Poles - Cantilever Poles for ANPR Cameras	No.	1559	712		
6	Network Access Switches - 8 or more ports	No.	4633	2,179		
7	Gun Shot solution	No.	200	200		
8	Public Address System + loudspeaker at 182(c2i) +16(c3i) +2(c4i) + 100(field) = 300 identified spots (locations) centrally regulated at C4i	No.	300	300		
9	Junction Box - Floor mounted (including last mile passive networking, earthing, etc.)	No.	1201	729		
10	Junction Box - Pole mounted (including last mile passive networking, earthing, etc.)	No.	3432	1,450		
11	Cat6A/ E Cable (UTP)	Mtr.	550000	232210		
12	Power Cable - Armoured 2 core 1.5 square MM	Mtr.	500000	211100		
13	Power-cable - Unarmoured 1.5 Square MM for Equipment Power with 3 PIN Top	No.	51760	550000		
14	12 port loaded LIU with LC port for OFC Termination at Junction Poles	No.	4633	2,179		
15	8 Port loaded Jack Panel for CAT-6 Cables	No.	4633	2,179		
16	SN Duplex LC-LC Duplex Patch Cord	No.	9266	4,358		
17	Surge Protector - single port internet RJ-45 Plug-in Surge Protector for PoE and PoE+ for All field cameras and L2 Switches	No.	10000	4,771		
18	1 Mtr Patch Cord from jack panel to surge Protector & Vice-Versa	No.	21064	10,618		
19	Field Terminal Connector	No.	9989	4,222		



Sr. No	Description	Unit	Total Quantity	Phase 1-quantity	Make	Model/Part No
20	16 AMP DP-MCB for Mains INPUT at Junction Box	No.	4633	2,179		
21	06-16 combine switch socket Box for UPS input	No.	4633	2,179		
22	24 VAC 5 AMP Power supply for ANPR IR	No.	1622	686		
23	Birds care for camera	No.	9989	4,222		
24	Digging, Piping & Re-filling (Trenching and Restoration)	Mtr.	782480	333538		
25	Earthing - 2 Mtrs GI with 25x3 GI strip connectivity to junction boxes	No.	1201	729		
26	Earthing - 1 Mtrs with 8mm GI wire for connectivity to Boxes	No.	5361	2,592		
27	1 KVA, 2 KVA UPS (60 minutes backup) - for camera	No.	4633	2,179		
28	Mobile hand-held devices for Police Officials	No.	220	220		
29	Any Additional Components including certification	Lump-sum	1	1		
	(miscellaneous)					
	Any Additional Components including certification (miscellaneous)					
	Items/Components consider under miscellaneous as as follows:					
	- Transit insurance					
	- Temporary storage Warehouse & watchmen cost					
	- Field device insurance like camera etc after deployment					
	- Fencing of poles if required					
	- Vehicles need to hire for engineer for supervising purpose at the time of installation period and for post installation purpose as well					
	- Electrical tape, OFC Marker, feruling & node points numbering, OTDR machine, Tie, cable manager, GI heavy grade conduit,					
	- Toolkit (spanner set, multimeter, digital analyzer,					



Sr. No	Description	Unit	Total Quantity	Phase 1-quantity	Make	Model/ Part No
	screwdriver set, torch etc) at every police station					
	- Pest control & sanitization at c4i,c3i,c2i 2 times in a year					
	- First aid kit at every control room					
#	Description	Measuring Unit	Qty	Phase 2-quantity		
1	Outdoor Fixed Camera - 4MP	No.	6121	1,538		
2	Outdoor PTZ Camera - 4MP, 30x Optical Zoom and joystick control operations	No.	2246	561		
3	Outdoor Fixed ANPR Camera with IR Illuminator- 2 MP	No.	1622	404		
4	Poles - for Cameras with 1 mtr ARMs for fixed and PTZ	No.	3802	877		
5	Poles - Cantilever Poles for ANPR Cameras	No.	1559	395		
6	Network Access Switches - 8 or more ports	No.	4633	1,118		
7	Gun Shot solution	No.	200	0		
8	Public Address System + loudspeaker at 182(c2i) +16(c3i) +2(c4i) + 100(field) = 300 identified spots (locations) centrally regulated at C4i	No.	300	0		
9	Junction Box - Floor mounted (including last mile passive networking, earthing, etc.)	No.	1201	349		
10	Junction Box - Pole mounted (including last mile passive networking, earthing, etc.)	No.	3432	769		
11	Cat6A/ E Cable (UTP)	Mtr.	550000	137665		
12	Power Cable - Armoured 2 core 1.5 square MM	Mtr.	500000	125150		
13	Power-cable - Unarmoured 1.5 Square MM for Equipment Power with 3 PIN Top	No.	51760	550000		
14	12 port loaded LIU with LC port for OFC Termination at Junction Poles	No.	4633	1,118		
15	8 Port loaded Jack Panel for CAT-6 Cables	No.	4633	1,118		



Sr. No	Description	Unit	Total Quantity	Phase 1-quantity	Make	Model/Part No
16	SN Duplex LC-LC Duplex Patch Cord	No.	9266	2,236		
17	Surge Protector - single port internet RJ-45 Plug-in Surge Protector for PoE and PoE+ for All field cameras and L2 Switches	No.	10000	2,372		
18	1 Mtr Patch Cord from jack panel to surge Protector & Vice-Versa	No.	21064	4,744		
19	Field Terminal Connector	No.	9989	2,503		
20	16 AMP DP-MCB for Mains INPUT at Junction Box	No.	4633	1,118		
21	06-16 combine switch socket Box for UPS input	No.	4633	1,118		
22	24 VAC 5 AMP Power supply for ANPR IR	No.	1622	404		
23	Birds care for camera	No.	9989	2,503		
24	Digging, Piping & Re-filling (Trenching and Restoration)	Mtr.	782480	191086		
25	Earthing - 2 Mtrs GI with 25x3 GI strip connectivity to junction boxes	No.	1201	349		
26	Earthing - 1 Mtrs with 8mm GI wire for connectivity to Boxes	No.	5361	1,254		
27	1 KVA, 2 KVA UPS (60 minutes backup) - for camera	No.	4633	1,118		
28	Mobile hand-held devices for Police Officials	No.	220	0		
29	Any Additional Components including certification	Lump-sum	1	1		
	(miscellaneous)					
	Any Additional Components including certification (miscellaneous)					
	Items/Components consider under miscellaneous as follows:					
	- Transit insurance					
	- Temporary storage Warehouse & watchmen cost					
	- Field device insurance like camera etc after deployment					
	- Fencing of poles if required					
	- Vehicles need to hire for engineer for supervising purpose at the time of installation period					



Sr. No	Description	Unit	Total Quantity	Phase 1-quantity	Make	Model/Part No
	and for post installation purpose as well					
	- Electrical tape, OFC Marker, feruling & node points numbering, OTDR machine, Tie, cable manager, GI heavy grade conduit,					
	- Toolkit (spanner set, multimeter, digital analyzer, screwdriver set, torch etc) at every police station					
	- Pest control & sanitization at c4i,c3i,c2i 2 times in a year					
	- First aid kit at every control room					
#	Description	Measuring Unit	Qty	Phase 3-quantity		
1	Outdoor Fixed Camera - 4MP	No.	6121	1,998		
2	Outdoor PTZ Camera - 4MP, 30x Optical Zoom and joystick control operations	No.	2246	734		
3	Outdoor Fixed ANPR Camera with IR Illuminator- 2 MP	No.	1622	532		
4	Poles - for Cameras with 1 mtr ARMs for fixed and PTZ	No.	3802	1,248		
5	Poles - Cantilever Poles for ANPR Cameras	No.	1559	452		
6	Network Access Switches - 8 or more ports	No.	4633	1,336		
7	Gun Shot solution	No.	200			
8	Public Address System + loudspeaker at 182(c2i) +16(c3i) +2(c4i) + 100(field) = 300 identified spots (locations) centrally regulated at C4i	No.	300			
9	Junction Box - Floor mounted (including last mile passive networking, earthing, etc.)	No.	1201	123		
10	Junction Box - Pole mounted (including last mile passive networking, earthing, etc.)	No.	3432	1,213		
11	Cat6A/ E Cable (UTP)	Mtr.	550000	180125		
12	Power Cable - Armoured 2 core 1.5 square MM	Mtr.	500000	163750		



Sr. No	Description	Unit	Total Quantity	Phase 1-quantity	Make	Model/ Part No
13	Power-cable - Unarmoured 1.5 Square MM for Equipment Power with 3 PIN Top	No.	51760	550000		
14	12 port loaded LIU with LC port for OFC Termination at Junction Poles	No.	4633	1,336		
15	8 Port loaded Jack Panel for CAT-6 Cables	No.	4633	1,336		
16	SN Duplex LC-LC Duplex Patch Cord	No.	9266	2,672		
17	Surge Protector - single port internet RJ-45 Plug-in Surge Protector for PoE and PoE+ for All field cameras and L2 Switches	No.	10000	2,851		
18	1 Mtr Patch Cord from jack panel to surge Protector & Vice-Versa	No.	21064	5,702		
19	Field Terminal Connector	No.	9989	3,264		
20	16 AMP DP-MCB for Mains INPUT at Junction Box	No.	4633	1,336		
21	06-16 combine switch socket Box for UPS input	No.	4633	1,336		
22	24 VAC 5 AMP Power supply for ANPR IR	No.	1622	532		
23	Birds care for camera	No.	9989	3,264		
24	Digging, Piping & Re-filling (Trenching and Restoration)	Mtr.	782480	257856		
25	Earthing - 2 Mtrs GI with 25x3 GI strip connectivity to junction boxes	No.	1201	123		
26	Earthing - 1 Mtrs with 8mm GI wire for connectivity to Boxes	No.	5361	1,515		
27	1 KVA, 2 KVA UPS (60 minutes backup) - for camera	No.	4633	1,336		
28	Mobile hand held devices for Police Officials	No.	220	0		
29	Any Additional Components including certification	Lump-sum	1	1		
	(miscellaneous)					
	Any Additional Components including certification (miscellaneous)					
	Items/Components consider under miscellaneous as follows:					
	- Transit insurance					



Sr. No	Description	Unit	Total Quantity	Phase 1-quantity	Make	Model/ Part No
	- Temporary storage Warehouse & watchmen cost					
	- Field device insurance like camera etc after deployment					
	- Fencing of poles if required					
	- Vehicles need to hire for engineer for supervising purpose at the time of installation period and for post installation purpose as well					
	- Electrical tape, OFC Marker, feruling & node points numbering, OTDR machine, Tie, cable manager, GI heavy grade conduit,					
	- Toolkit (spanner set, multimeter, digital analyzer, screwdriver set, torch etc) at every police station					
	- Pest control & sanitization at c4i,c3i,c2i 2 times in a year					
	- First aid kit at every control room					
Total for Field level						
#	Description	Measuring Unit	Qty			
Technical Manpower as per requirement given in Para.... stipulated....						
1	Manager - DC, C4I, C3I and C2I					
2	C4I Expert					
3	System Administrator					
4	Network and Security Manager along with Field Network Technician					
5	Storage Administrator					
6	Enterprise & Asset Manager					
7	Database Administrator					
Total for Technical Manpower						
#	Description	Measuring Unit	Qty			
Power Charges						
1	Power Meter Charges (Installation & Others)					



Sr. No	Description	Unit	Total Quantity	Phase 1-quantity	Make	Model/Part No
2	Power cabling from meter to site and miscellaneous					
3	Power meter & connection charges for Pilot (2 Districts)(unit rate is for 3 month)					
Total for Power Charges						
#	Description	Measuring Unit	Qty			
Operators for O&M phase						
1	Operator- Manpower at C2i for Phase I,II & III for 03 years					
2	Operator- Manpower at C3i for Phase I,II & III for 03 years					
3	Operator-Manpower at C4i for Phase I,II & III for 03 years					
4	Supervisor/Manager -Manpower at C4i for Phase I,II & III for 03 years					
5	Operator- Manpower at C2i for 2 Pilot Districts (approx. 27 Police Station)					
6	Operator- Manpower at C3i for 2 Pilot Districts					
7	Operator- Manpower at C4i for 2 Pilot Districts					
Total for Operators for)&M phase						
#	Description	Measuring Unit	Qty.			
Any other or miscellaneous						
1	Miscellaneous					
	Penta scanning & Certification					
	Insurance					
	Travel Allowance					
	Watchmen					
	Warehouse on Rent to store field material					
	Network Dressing					
	Risk - Power Charges, ROW, RI Charges, Taxation					
	2% Inventory spares to maintain SLA					



Sr. No	Description	Unit	Total Quantity	Phase 1-quantity	Make	Model/ Part No
	Additional Requirement in C4I for Interior					
	Additional Furniture, Chairs, Tables					
	Diesel for C4I					
	Insurance to Manpower working in the field					
	Freight Insurance					
	Light Bar for vehicles & poles					
	Logo Embossing on every equipment					
	Battery Replacement, Theft in the field, etc.					
	External DVD writer					
	Any other requirement to meet the solutioning for the Project Implementation					
Total for Miscellaneous						



3.1.2. Civil Works and interiors of C4i

Sr. No.	Description	Unit	Qty.	Unit Rate	Amount
A.	Demolition and Cartage of Rubbish				
B.	Civil Works				
1	PCC Up to 75mm/ Repair of existing floor with cement plaster before laying Tiles/ Floor carpet.	sqm	695		
2	Cement Sand Plaster	sqm	184		
3	POP Punning	sqm	300		
4	Floor/Wall Chasing	L/S	2		
C.	Joinery				
1	P9: Fire rated Partition panelling as per specification and designer	sqm	150		
2	P9A: Fire Rated Partition as per specification and designer	sqmt	310		
3	G: Full height 12mm thk. Toughened double glass partition	sqm	190		
4	P10: Modular extruded aluminium Partitions	sqm	200		
5	Extruded Aluminium Skirting	rm	500		
6	Pelmet with fire rated board and CILL	rm	95		
7	Laminated Window Cill 600mm wide fire rated	rm	95		
D.	Doors				
1	D1 -Fire rated door - up to 750 x 2100 -	nos	4		
2	D2 -Fire rated door - 1200 x 2100	nos	2		
3	Glass door - 1050 x 2100	nos	7		
E.	Ceiling				
1	Plain Gypsum Ceiling fire rated	sqm	520		
2	Vertical Bands with fire rated gypsum board	rm	140		
3	Cove with fire rated gypsum board	rm	140		
4	Mineral fibre Tile Grid Ceiling - 2' x 2' - Metal ceiling	sqm	255		
5	baffles Ceiling	sqm	405		
6	Access Panel of size 2' x 2'	nos	6		
7	Access Panel of size 6' x 6'	nos	1		
F.	Finishes				
1	Light Textured Paint	sqm	1,200		
2	Laminated Panelling fire rated board	sqm	60		
3	Corian Cladding 12 mm thk for corner and panelling	sqm	45		
4	Vinyl Film/ Graphic Panels	sqm	25		
5	Fabric Acoustic Panelling	sqmt	495		



Sr. No.	Description	Unit	Qty.	Unit Rate	Amount
6	Colour Back glass Panelling toughened	sqm	25		
G.	Built in storages				
1	Full Ht. Storage (Laminated) 400mm Deep fire rated	sqm	15		
H.	Flooring				
1	Raised Access Flooring (Range: 150mm-300mm) top unfinished	sqm	630		
2	Stainless Steel edge trims	rm	25		
I.	Signage				
1	General room Signage	nos	25		
2	General Information Signage	nos	15		
3	General Luminous Fire Exit Signages	nos	10		
4	Luminous Fire extinguisher Signage	nos	15		
5	Luminous Fire evacuation plans	nos	8		
J.	Loose Furniture				
1	Running Counter	rmt	5		
K.	Misc. Items				
1	Graphics as per designer	sq.ft.	2,000		
2	BLINDS - Roller with 3% visibility	Sq.mt.	0		
3	Black out blinds	Sq.mt.	0		
L.	Electrical				
a.	Wiring including termination for the following light points with 2 x 2.5 sq. mm PVC insulated FRLS copper conductor wires of 650/1100 Volts grade in concealed/exposed 16gauge MS conduits as called for including providing 6-amp flush type switches, anodized MS box for housing switches approved White Polycarbonate modular cover plate for switch boxes and earthing. All the circuit must dressed with circuit identification tags (the rates include: 6 AMP switch, 6 AMP socket, Modular Face plate, FRLS Cable with average length 20-30 m, 16-gauge MS conduits 20-30 meter, All the accessories and Workmanship.)				
1	First point controlled by one no. 6 amp switch.	Nos	60		
2	Same as item No. 1 above but LOOP POINT i.e. wiring including termination of point looped from first point with 2 x 1.5 sq. mm PVC insulated FRLS copper conductor wire of 650/1100 volt grade in	Nos	120		



Sr. No.	Description	Unit	Qty.	Unit Rate	Amount
	concealed/exposed 16-gauge MS conduit and earthing (controlling switch in item no. 1).				
b.	Wiring including termination for the following light points with 2 x 2.5 sq. mm PVC insulated FRLS copper conductor wires of 650/1100 Volts grade in concealed/exposed 16gauge MS conduits as called for including providing 16-amp flush type switches, anodized MS box for housing switches approved White Polycarbonate modular cover plate for switch boxes and earthing. All the circuit must dressed with circuit identification tags (the rates include: 6 AMP switch, 6 AMP socket, Modular Face plate, FRLS Cable with average length 20-30 m, 16 gauge MS conduits 20-30 meter, All the accessories and Workmanship.)				
1	First point controlled by one no. 16 amp switch.	Nos	40		
2	Same as item No. 3 above but LOOP POINT i.e. wiring including termination of point looped from first point with 2 x 1.5 sq. mm PVC insulated FRLS copper conductor wire of 650/1100-volt grade in concealed/exposed 16-gauge MS conduit and earthing (controlling switch in item no. 3).	Nos	90		
3	Wiring including termination for 6-amp socket outlet point with 2 x 1.5 sq. mm PVC insulated FRLS copper conductor wires in concealed/exposed 16gauge MS conduits or existing raceways including providing 6-amp switch, 3 pin 6A shuttered socket, anodised MS box for housing switches sockets, approved White Polycarbonate modular cover plate and earthing. (Looped to lighting circuit as shown in drawing). All the circuit must dressed with circuit identification tags	Nos	55		
c.	Wiring including termination for the following configuration of outlets for workstations with 3 core x 2.5 sq.mm. Copper conductor, PVC insulated PVC sheathed wires of 650/1100V grade in existing conduit/raceway including supplying and fixing following numbers socket and switch housed in anodized MS box with approved White polycarbonate modular cover plate as required. NOTE: - For UPS in one circuit maximum three workstations shall be looped. Colour coding shall be strictly followed for wiring. For Raw in one circuit maximum six workstations shall be looped. All the circuit must be dressed with circuit identification tags				
1	2 No. 13A, Universal Socket outlets controlled by 1 No. 16A switch. (UPS power at W/S)	Set	270		



Sr. No.	Description	Unit	Qty.	Unit Rate	Amount
2	1 No. 6A, round pin outlets, controlled by 1 no.6A switch. (Raw power at W/S)	Set	90		
3	Wiring including termination for 16 amp power socket outlet points with 2 x 6 sq. mm PVC insulated FRLS copper conductor wires for the first socket outlet and 2 x 4 sq. mm PVC insulated FRLS copper conductor wires for the second outlet of 650/1100 Volts grade in concealed/exposed 16 gauge MS conduits or existing raceway as called for including providing 16 amp flush type combined 6 pin shuttered sockets and switches, anodised MS outlet boxes for 16 A 6 pin sockets and switches, approved White Polycarbonate modular cover plate and earthing.(The item is for set of two outlets looped together as explained above) All the circuit must dressed with circuit identification tags	Set	20		
4	Wiring including termination for 16-amp power socket outlet point with 2 x 4 sq. mm PVC insulated FRLS copper conductor wire of 650/1100 Volts grade in concealed/exposed 16 gauge MS conduits or in existing raceway including providing 16 amp flush type combined 6 pin shuttered socket and switch, anodized MS boxes for 16 amp 6 pin socket and switch, approved White Polycarbonate modular cover plate and earthing. (Only one outlet shall be connected to each circuit). All the circuit must dressed with circuit identification tags	Nos	10		
5	Supplying and fixing of 32 amp 3-pin for 1-phase industrial socket outlet, Self-locking type of Neptune Balls make including supplying MS boxes of suitable size,32-amp DP MCB and a plug top, complete as required and as per specifications.	Nos	16		
6	Supplying and fixing of 32 amp 3-phase industrial socket enclosure, IP 65 including supplying boxes of suitable size,40-amp TP MCB and complete as required and as per specifications.	Nos	R.O		
7	Supplying and fixing in position of the following sizes of exposed/concealed 16gauge MS conduit including all accessories complete as required and as per specifications.				
8	25 mm dia MS conduit	RM	150		
9	Supplying, drawing, termination of the following size of FRLS PVC insulated copper conductor wires 650/1100 V grade in existing conduits, complete as required and as per specifications.				
10	2 x 6 sq. mm with 1 no.2.5 sq. mm PVC insulated copper conductor earth wire.	RM	180		



Sr. No.	Description	Unit	Qty.	Unit Rate	Amount
M.	CONDUITS AND MS PAINTED CHANNELS FOR STRUCTURED CABLING				
1	Supplying and fixing in position MS anodised box for data/voice outlet suitable for fixing of RJ 45 jack complete as required.	Nos	180		
2	Supplying and fixing in position following sizes of 16-gauge MS conduits including providing all accessories concealed/ exposed as required.				
3	25 mm dia MS conduit (For Data/Voice wiring) (16 GAUGE) Complete with all fixing accessories	RM	1,000		
4	32 mm dia MS conduit (For Data/Voice wiring) (16 GAUGE) Complete with all fixing accessories	RM	200		
5	Supply and fixing of following sizes of MS painted channel colour coded Orange for power, Blue for Data ,14 gauge, with openable cover and all accessories as required for fixing on wall/column/ceiling complete as required including providing junction boxes, bends and tees as required.				
6	300 mm x 50 mm	RM	400		
7	200 mm x 50 mm	RM	120		
8	200 mm x 40 mm	RM	90		
9	100 mm x 50 mm	RM	150		
10	Supply and fixing of following sizes of MS painted channels, 14 gauge, with all accessories as required including junction boxes of depth more than the raceway (approx. 65 mm), colour coded with orange colour for power and blue colour for data, laid in floor including marking the routing, getting it approved, filling and plastering after laying the raceway, grouting the raceway to the floor, sealing of raceway cover, joints and junction boxes complete as required. Required junction boxes will be provided for smooth pulling of structured and power cabling. It will be the responsibility of the contractor to coordinate with structured cabling contractor for laying of cable.				
11	300mm x 40mm (3 mm thick cover)	RM	400		
12	200mm x 40mm (3 mm thick cover)	RM	290		
13	100mm x 40mm (2 mm thick cover)	RM	150		
14	Supply and fixing in position MS anodised box for T.V. outlet including white poly carbonate modular cover plate and co-axial type T.V. socket outlet complete as required.	Nos	120		
15	Supply, drawing, termination of RG-6 co-axial cable for TV in existing conduit complete as required.	RM	100		



Sr. No.	Description	Unit	Qty.	Unit Rate	Amount
16	Providing and fixing in position following sizes of MS conduits including providing all accessories concealed/ exposed as required along with G.I. pull wire,14 SWG				
17	25 mm dia MS conduit	RM	200		
18	Supply and, installation of Novar/ Steel ways make floor mounted box 250 mm by 250 mm for housing UPS power and data/voice boxes complete as required.	Nos.	R. O		
N.	INSTALLATION OF PANELS; SUPPLY AND INSTALLATION OF DB, CABLES AND EARTHING				
a.	Receiving, storing properly, installation, testing and commissioning of following panels complete as required.				
1	MDB's	Set	1		
2	UMDB	Set	8		
3	Supply, installation, testing & commissioning of 125 Amp TP MCCB with heavy duty solid neutral link, rotary operating handle, 25 KA service breaking capacity with required arrangement of incoming & outgoing cables required.	Set	8		
b.	Supplying, installing in position, testing and commissioning of the following Distribution Boards made of 16-gauge powder coated MS sheet steel, wall mounted/fully recessed in wall, indoor industrial type, with dust & vermin proof, hinged and lockable doors, double door design, complete with inter connecting wires of proper gauge, aluminium coated copper thimbles and with the circuit identification tags, colour coded wiring from Incomer MCB to each ELCB along with earthing terminal. The DB shall be suitable for taking cable/conduit as incoming/outgoing.				
1	12-way TPN DB with 30 Nos of 10/20 amps SP MCB's i.e. 10 Nos. of 10/20 amp SP MCB's arranged in 3 rows arranged in 3 tier one above other and controlled by 1 No. 63 amp TPN MCB and neutral link. Each row of MCB's shall be provided with 40-amp DP ELCB of 100 mA sensitivity.	Nos	10		
2	12-way TPN DB with 30 Nos of 10/20 amps SP MCB's i.e. 10 Nos. of 10/20 amp SP MCB's arranged in 3 rows arranged in 3 tier one above other and controlled by 1 No. 63 amp TPN MCB and neutral link. Each row of MCB's shall be provided with 40-	Nos	10		



Sr. No.	Description	Unit	Qty.	Unit Rate	Amount
	amp DP ELCB of 100 mA sensitivity. (All MCB to be "D" Curve)				
3	10-way TPN DB with 24 Nos of 10/20 amps SP MCB's i.e. 6 Nos. of 10/20 amp SP MCB's arranged in 3 rows arranged in 3 tier one above other and controlled by 1 No. 63 amp TPN MCB and neutral link. Each row of MCB's shall be provided with 40-amp DP ELCB of 100 mA sensitivity.	Nos	3		
4	6-way TPN DB with 18 Nos of 10/20 amps SP MCB's i.e. 6 Nos. of 10/20/32 amp SP MCB's arranged in 3 rows arranged in 3 tier one above other and controlled by 1 No. 63 amp TPN MCB and neutral link. (All MCB shall be D curve)	Nos	2		
5	Sheet metal enclosed 12-way SPN DB with 8 Nos. 10/20 Amp SP MCB and controlled by 1 no. 40 Amp DP MCB with ELCB (100 mA) complete as required. For emergency lighting.	Nos	8		
6	Supply ,installation, testing and commissioning of earth pits comprising 600 x 600 x 3 mm. thick Copper electrode, 50 mm dia medium class GI pipe, GI funnel with 20 gauge GI wire mesh, masonry chamber with concrete base, CI manhole cover with frame (300 mm. x 300 mm.) painted with bitumastic paint, test link joint and alternate packing the mixture of Charcoal and salt around plate electrode, depth should not less than 3 meters, The thickness of earthing pipe should not be less than 2 mm complete as required ,as per specifications and as per IS: 3043	Nos.	6		
c.	Supply and fixing in position the following insulated wires including providing all fixing accessories and effecting proper connections.				
1	6 sq. mm. dia pvc insulated copper conductor wire.	RM	600		
d.	Supplying, unloading, storing, laying, testing and commissioning of following sizes PVC insulated (Heavy duty) Copper conductor cables suitable for working voltage up to and including 1100 Volts, laid and tied on existing overhead cable trays; or laid and tied over MS supports in masonry trenches including providing MS supports and clamps for fixing to supports in an approved manner complete as required and as per specifications. Circuit identification tag should be attached with the concerned cable along with the test report of following sizes of cable to be submitted by the contractor at the time of delivery of material at site				
1	50 sq. mm. cable, armoured for earthing.	RM	1,200		



Sr. No.	Description	Unit	Qty.	Unit Rate	Amount
2	95 sq.mm. cable unarmoured for UPS	RM	600		
3	25 sq.mm. cable unarmoured for UPS	RM	200		
4	50 sq.mm. cable unarmoured for UPS	RM	200		
e.	Termination of the following sizes of PVC insulated Copper conductor cable including providing terminal lugs, single compression glands crimping the joints, providing insulation tape, effecting terminal connections to the equipment complete as required.				
1	50 sq. mm. cable, armoured for earthing.	Nos.	12		
2	95 sq.mm. cable unarmoured for UPS	Nos.	20		
3	70 sq.mm. cable unarmoured for UPS	Nos.	24		
4	50 sq.mm. cable unarmoured for UPS	Nos.	8		
f.	Supplying, unloading, storing, laying, testing and commissioning of following sizes of XLPE insulated (Heavy duty) Aluminium/copper conductor armoured cables suitable for working voltage up to and including 1100 Volts, laid and tied on existing overhead cable trays; or laid and tied over MS supports in masonry trenches including providing MS supports and clamps for fixing to supports in an approved manner complete as required and as per specifications.				
1	3.5 x 150 sq.mm. Aluminium Cable	RM	100		
2	3.5 x 70 sq.mm. Aluminium Cable	RM	R. O		
3	4 x 25 sq.mm. Al. Cable	RM	R. O		
4	4 x 16 sq.mm. copper Cable	RM	200		
5	4 x 10 sq.mm. copper Cable	RM	100		
6	4 x 6 sq.mm. copper Cable	RM	50		
7	2 x 10 sq.mm. copper Cable	RM	50		
8	2 x 6 sq.mm. copper Cable (For Dedicated earthing of DB's)	RM	100		
g.	Termination of the following sizes of PVC insulated Aluminium conductor cable including providing terminal lugs, single compression gland, crimping the joints, providing insulation tape, effecting terminal connections to the equipment complete as required				
1	3.5 x 150 sq.mm. Aluminium Cable	Nos.	18		
2	4 x 16 sq.mm. copper Cable	Nos.	8		
3	4 x 10 sq.mm. copper Cable	Nos.	4		
4	4 x 6 sq.mm. copper Cable	Nos.	4		
5	2 x 10 sq.mm. copper Cable	Nos.	4		
6	2 x 6 sq.mm. copper Cable (For Dedicated earthing and body earthing of DB's)	Nos.	4		



Sr. No.	Description	Unit	Qty.	Unit Rate	Amount
7	Supply, installation, testing and commissioning of Earth box made of 2mm thick MS painted, with a glass cover and having 25 x 3 mm Cu strip with insulators complete as required.	Set	1		
h.	Supply, laying in position & proper connection by welding/bolting or brazing for the following GI tape/wires including providing all fixing accessories and effecting proper connections.				
1	25 x 6 mm GI tape	RM	800		
i.	Supply and installation of following sizes of MS perforated type cable trays with stove enamel paint of approved colour and necessary bends, tees, reducer couplers, dash-fasteners, GI nuts bolts including cutting, bending, drilling, bolting required suspension arrangement fabricated from steel etc. complete as per specifications and as approved by Engineer - in - charge. The suspension of MS cable tray, only GI or SS round rods with ceiling anchoring facility should be used.				
1	600 mm wide, 40 mm high (2 mm thick)	RM	200		
2	450 mm wide, 40 mm high (2 mm thick)	RM	400		
3	300 mm wide, 40 mm high (2 mm thick)	RM	300		
4	150mm wide, 40 mm high (2 mm thick)	RM	200		
5	450 mm wide, 100 mm high (Data Centre)	RM	150		
6	300 mm wide, 100 mm high (Data Centre)	RM	R. O		
O.	SUPPLY OF LIGHTING FIXTURES				
	NOTE: 1. The fixtures shall be suitable for single phase, 50 cycles, 230 Volts, A.C. supply system. 2.All fixtures shall be factory wired with copper conductor wires. 3.All fixtures shall be supplied with Electronic ballasts, fluorescent lamps/bulbs, as specified. 4.The rate shall be quoted for the Catalogue no. specified for the fixture however if contractor wants to supply equivalent then sample shall have to be got approved from Architect before procurement. 5.All the samples shall be submitted within two weeks of the issue of work order, for approval from the Architect. 6.Supply, unloading storing at site of the following fixtures with all accessories, such as spring-loaded side holders, starters, power factor compensators, MS				



Sr. No.	Description	Unit	Qty.	Unit Rate	Amount
	housing to house ballasts, complete with lamps. All the lamps shall be colour 84 or as approved.				
a.					
1	Soft light as per designer	Nos	80		
2	Suspend/Recessed light line system with 1 x 28 w TL 5 Lamp.	Nos	18		
3	Cove light, T5 lamp, 4 feet with all accessories	Nos	150		
4	Cove light, T5 lamp, 2 feet with all accessories	Nos	50		
5	Linear Light Fixture 4 feet long as per designer	Nos	60		
b.	Supply, unloading storing at site of following PL lamp / halogen fixtures complete with all accessories and PL lamp / halogen lamps with toroidal transformer, electronic ballast completes as required.				
1	2 x 18W, CFL down lighter OR EQUIVELLENT.	Nos	60		
2	1 x 18/10 W, CFL down lighter OR EQUIVELLENT.	Nos	50		
3	Artlite Cat. No. RL 2784, with 12V, 50W Halogen (Adjustable Light) Wall Washer	Nos	10		
4	Ratite Cat. No. RL 6044 Wall lamp	Nos	RO		
5	Intercraft Channel, 1 x 54 W Surface mounted light	RM	RO		
6	Intercraft Channel, 1 x 54 W Recessed light	RM	RO		
7	Intercraft Channel, 1 x 54 W Suspended light	RM	R.O		
P.	FIXING OF LIGHTING FIXTURES				
a.	The rates for fixing of lighting fixtures shall include all fixing accessories that are required to make the installation complete in all respects including the following: - 1. Providing connecting wires and channel support wherever required. 2. Internal wiring between accessories. 3. Self-interlocking connector blocks for connecting the wires from fixtures to the points. 4. Earthing of fixtures with 1.5 sq. mm. PVC insulated copper conductor wire. 5. Approved colour powder coated down rods, clamps and other components and fixing accessories wherever required. 6. Testing of fixtures before Installation. 7. Identification tags with a distance not more 3 meters to be use for circuit identification				
1	Receiving, fixing in position, effecting proper connections, testing and commissioning of 1 x 36-watt fluorescent fixtures/2 x 36 watt/1 X 18-watt fluorescent fixtures surface mounted on ceiling or wall	Nos	120		



Sr. No.	Description	Unit	Qty.	Unit Rate	Amount
	mounted or kept in cove/pelmet or suspended from existing raceway with all fixing accessories as required.				
2	Receiving, fixing in position, effecting proper connections, testing and commissioning of 1 x 36 /2 x 36 watt CFL fixtures fixed recessed in ceiling with chains hung from slab with all fixing accessories as required, along with providing PVC flexible conduit from junction box at slab level to fixture on the false ceiling.	Nos	250		
3	Receiving, fixing in position, effecting proper connections, testing and commissioning of PL lamp/Halogen lamp fixture fixed recessed in ceiling complete as required and with all accessories, along with providing PVC flexible conduit from junction box at slab level to fixture on the false ceiling.	Nos	266		
Q.	CONSTRUCTION POWER AND LIGHTING				
1	Providing temporary construction lighting and power on the third floor including by using required nos. 1 x 36 Watt phatti type fixtures (minimum 250 Lux), required flexible double insulated copper wiring, distribution board, minimum 3 nos. 400 W halogen flood light, earthing, main panel with incoming MCCB and required MCCB in the outgoing for distributing the power thought the duration of the project. It will be the responsibility of Electrical Contractor to distribute power to all the contractors working at site. The rates shall be all inclusive. The material bought by the contractor shall be the property of the contractor and after the work is completed it can be taken back by him. (All item mentioned above, shall be new and of good quality by considering site safety parameter. Old and repaired item shall never be allowed to use at site.)	LS	1		
R.	Networking				
a.	Supply, Installation, Testing and commissioning of Data and Voice System (4 Node Outlet at Each Location).				
1	Supply & fixing 24-port Loaded, Modular Jack Panel, 1U (For Data UTP Field Cables)	Each	15		
2	Cat-6 E UTP Cable	RM	15000		
3	I/O Crimped	Each	400		
4	4 - Port Face Plate	Each	90		



Sr. No.	Description	Unit	Qty.	Unit Rate	Amount
5	2 - Port Face Plate	Each	20		
6	Cat-6 UTP Jack with Strain Relief	Each	1050		
7	Supply & fixing server rack (42 U Size)	Each	1		
8	Supply & fixing Vertical Wire Manager single side.	Each	40		
9	Supply & fixing 2U Horizontal Cable Manager (For Field Cables & Switches)	Each	16		
10	Smart PDU 6 AMP x 12 sockets in the Rack	Each	16		
11	UTP Termination for both ends, labelling, testing.	Each	800		
12	25 Years Certification from Tyco / AMP / Penta Scanning	L.S.	800		
13	AMP Cat 6, UTP Mounting Cords for Data Rack End 4 Feet (Yellow)	no's	200		
14	AMP Cat 6, UTP Mounting Cords for Data Rack End 7 Feet (Yellow)	no's	200		
15	AMP Cat 6, UTP Mounting Cords for Data Server Rack Both end 7 Feet (RED)	no's	650		
16	AV Cabling	rmt	1520		
17	Rack mounting hardware	no's	15		
18	Rack fixing ladder for cable	no's	15		
19	6" PVC Cable Tie (Pack of 100)	pkt	112		
S.	ACS, FDS, RRS				
a.	ACS				
1	Access Controller capable of controlling 4doors and 4reader	Nos	2		
2	Finger print reader with lock output.	Nos	9		
3	Power Supply	Nos	18		
4	Proximity Reader	Nos	9		
5	Proximity Card	Nos	100		
6	Electro Magnetic Lock (Single leaf door)	Nos	11		
7	Power Supply for Lock	Nos	11		
8	Magnetic Contact	Nos	11		
9	Exit Push Button	Nos	11		
10	Emergency Release Switch	Nos	11		
11	4 core x 0.75 Sq.mm shielded Cable in PVC conduit	Mtrs	1,200		
b.	FDS				
1	Addressable Fire Alarm Panel (with Auto- Sprinkling system)	No	1		
2	Smoke detector	Nos.	40		
3	Heat detector	Nos.	6		
4	Manual Pull Station	Nos.	1		
5	Response Indicator	Nos.	6		
6	Sounder	Nos.	5		



Sr. No.	Description	Unit	Qty.	Unit Rate	Amount
7	2 core x 1.5 sq.mm Armoured cable	Mtrs.	600		
8	Hand held fire extinguisher Co2 4.5 KG - ISI Approved (for manual operations as per fire safety norms)	Nos	10		
c.	RODENT REPELLENT SYSTEM (RRS)				
1	Master Console with 12 satellites	Set	6		
2	Wire Bundle	Lot	6		
3	PVC Conduit	Mtrs	100		
T.	UPS System				
1	Supply, Installation, Testing and Commissioning of microprocessor based 150 KVA/ 200 KW UPS with In Built Isolation Transformer using Continuous duty, three phase, Monolithic True Online Double Conversion UPS using PWM IGBT technology, Dual Feed input, 3 Phase input 415 V +10% -15%, Online mode efficiency of 95% from 25% to 100% loading. 3 phase input and 3 phase output. UPS shall be capable of operating in parallel redundant load sharing mode configuration up to 8 units. 15 min. backup with SMF VRLA Lead Acid- Battery. Warranty: 5Years	Set	2		
2	UPS Incoming Panel	No	1		
3	Ups Out going panel	No	1		
4	Base structure for the UPS and Battery bank	No	4		
5	Battery Rack as per design approved	No	2		
U.	Carpet				
a.	Providing, supplying & installing carpet in the specified areas as per patterns specifications as below: a. Specifications 1 STYLE NAME THE ORIGINALONE FIRST /MT086 2 PILE WEIGHT (24.0 oz. per sq. yd.) 3 Pile thickness: 0.76" 4 PILE THICKNESS .132" (3.35 MM.) 5 STITCHES PER INCH 10.7 (42.13 per 10 cm) 6 PROTECTIVE TREATMENT Sentry Plus DENSITY 7 Tile size - 50cmx50cm 8 Dye method -100% solution dyed only 9 Secondary backing -Thermoplastic Composite Tile b. Product testing 1 FLAMMABILITY ASTM E 648 Class 1 (Glue Down) 2 CRI RATING Severe Traffic 3 STATIC PROPENSITY AATCC-134 Under 3.5 KV				



Sr. No.	Description	Unit	Qty.	Unit Rate	Amount
	4 SMOKE DENSITY ASTM E 662 Less than 450 c. Adhesive system-Pre-applied - micro encapsulated tackifier / approved adhesive-Solvent free 1 Trim carpet neatly at walls and around interruptions 2 Completed carpet to be smooth and free of bubbles, puckers and other defects 3 Warranties-Lifetime Ultra Set Modular Warranty, Lifetime Limited Colourfastness to Light, life time Limited Colourfastness to Atmospheric Contaminants, 10 Year Stain Warranty, Lifetime Static 4 Product-Modular Square Carpet tile, 5 Cost to include wastages for patterns, plastic covering protection after installation not less than 100microns thickness, all handling and transportation. 6 Layout- Site measurements should be carried out by the vendor in advance to confirm quantities of carpet required. 7 Tile based carpet				
1	Actual Quantity	sqmt	700		
V.	Modular Furniture (with Chairs) Sub-Total				
1	1800x900mm: Linear workstation Panel based system, .25mm thk. prelam table top shade-laminate, powder coating shade; grey - All tiles will be fabric: supported on gable end along with 25mm thk partition. total ht of workstations - 1200mm	Nos	38		
2	1 No. Three drawer (unequal) fixed pedestal per work station with one lock for all three drawers				
3	all complete with wire management and wire risers				
4	Fire Rated material for workstation				
5	MEETING TABLE -10 PAX - 2400X1200				
6	Meeting room table of size 2400mmx1200mm finished with laminate. Providing and fixing of table made of 25mm thk pre-laminated table top with pvc edge lipping. Table to have necessary perforated powder coated metal / laminate modety panel as per architects' instructions. Table to be supported with metal powder coated legs. Table to have necessary cable management with fliptop mechanism 2nos). Table to have levellers to adjust the heights as per architects' instructions.	Nos	4		
a	Chairs				



Sr. No.	Description	Unit	Qty.	Unit Rate	Amount
1	Workstations as described above:	Nos.	39		
2	Meeting chairs:	Nos.	49		
W.	HVAC Sub-Total				
1	HVAC- CENTRALIZED CONSDITIONIG THROUGHOUT C4i PREMISES	Nos.	1		
	C4i Non-IT TOTAL				#####



3.1.3. Civil Works and interiors of C3i

Sr. No.	Description	Unit	Quantity	Unit Rate	Amount
A.	Interior Works & Furnishings				
a.	CIVIL WORKS				
1	PCC Upto 75mm/ Repair of existing floor with cement plaster (manual PCC: 1:2:4 mix) before laying Tiles	sqm	80		
2	POP Punning	sqm	65		
b.	CEILING				
1	Plain Gypsum Ceiling	sqm	40		
2	Tile Grid Ceiling - 2' x 2' - ceiling	sqm	40		
3	Access Panel of size 2' x 2'	nos	1		
c.	FINISHES				
1	Light Textured Paint	sqm	190		
2	Laminated Panelling (include 18 mm Commercial board with Grey colour Matt finish laminate)	sqm	5		
B.	Electrical Works				
a.	Wiring and sockets- Wiring including termination for the following light points with 2 x 2.5 sq. mm PVC insulated FRLS copper conductor wires of 650/1100 Volts grade in concealed/exposed 16gauge MS conduits as called for including providing 6-amp flush type switches, anodized MS box for housing switches approved White Polycarbonate modular cover plate for switch boxes and earthing. All the circuit must dressed with circuit identification tags				
1	First point controlled by one no. 6 amp switch.	Nos	10		
2	Same as item No. 1 above but LOOP POINT i.e. wiring including termination of point looped from first point with 2 x 1.5 sq. mm PVC insulated FRLS copper conductor wire of 650/1100-volt grade in concealed/exposed 16 gauge MS conduit and earthing (controlling switch in item no. 1).	Nos	18		
3	2 No. 16A, Universal Socket outlets controlled by 1 No. 16A switch. (UPS power at W/S)	Set	8		
4	1 No. 6A, round pin outlets , controlled by 1 no.6A switch.(Raw power at W/S)	Set	4		
5	Supplying and fixing of 32 amp 3-pin for 1-phase industrial socket outlet, Self-locking type of Neptune Balls make including supplying MS boxes of suitable size, 32 amp DP MCB and a plug top, complete as required and as per specifications.	Set	4		



Sr. No.	Description	Unit	Quantity	Unit Rate	Amount
b.	Supplying, drawing, termination of the following size of FRLS PVC insulated copper conductor wires 650/1100 V grade in existing conduits, complete as required and as per specifications.				
1	2 x 6 sq. mm with 1 no.2.5 sq. mm PVC insulated copper conductor earth wire.	RM	20		
c.	Supplying and fixing in position of the following sizes of exposed/concealed 16gauge MS conduit including all accessories complete as required and as per specifications.				
1	25 mm die MS conduit	RM	40		
C	INSTALLATION OF PANELS; SUPPLY AND INSTALLATION OF DB, CABLES AND EARTHING				
a.	Receiving, storing properly, installation, testing and commissioning of following panels complete as required.				
1	MDB's	Set	1		
2	UMDB	Set	1		
b.	Supply and fixing in position the following insulated wires including providing all fixing accessories and effecting proper connections.				
1	6 sq. mm. dia pvc insulated copper conductor wire.	RM	40		
c.	Supplying, unloading, storing, laying, testing and commissioning of following sizes PVC insulated (Heavy duty) Copper conductor cables suitable for working voltage up to and including 1100 Volts, laid and tied on existing overhead cable trays; or laid and tied over MS supports in masonry trenches including providing MS supports and clamps for fixing to supports in an approved manner complete as required and as per specifications. Circuit identification tag should be attached with the concerned cable along with the test report of following sizes of cable to be submitted by the contractor at the time of delivery of material at site				
1	50 sq. mm. cable, armoured for earthing.	RM	40		
d.	Termination of the following sizes of PVC insulated Copper conductor cable including providing terminal lugs, single compression glands crimping the joints, providing insulation tape, effecting terminal connections to the equipment complete as required.				
1	50 sq. mm. cable, armoured for earthing.	Nos.	40		
e.	Supplying, unloading, storing, laying, testing and commissioning of following sizes of XLPE insulated (Heavy duty) Aluminium/copper conductor armoured				



Sr. No.	Description	Unit	Quantity	Unit Rate	Amount
	cables suitable for working voltage up to and including 1100 Volts, laid and tied on existing overhead cable trays; or laid and tied over MS supports in masonry trenches including providing MS supports and clamps for fixing to supports in an approved manner complete as required and as per specifications.				
1	2 x 10 sq.mm. copper Cable	RM	20		
2	2 x 6 sq.mm. copper Cable (For Dedicated earthing of DB's)	RM	40		
f.	Termination of the following sizes of PVC insulated Aluminium conductor cable including providing terminal lugs, single compression gland , crimping the joints ,providing insulation tape, effecting terminal connections to the equipment complete as required				
1	4 x 10 sq.mm. copper Cable	Nos.	4		
2	4 x 6 sq.mm. copper Cable	Nos.	4		
3	2 x 10 sq.mm. copper Cable	Nos.	4		
4	2 x 6 sq.mm. copper Cable (For Dedicated earthing and body earthing of DB's)	Nos.	4		
5	Supply, installation, testing and commissioning of Earth box made of 2mm thick MS painted, with a glass cover and having 25 x 3 mm Cu strip with insulators complete as required.	Set	1		
g.	Supply, laying in position & proper connection by welding/bolting or brazing for the following GI tape/wires including providing all fixing accessories and effecting proper connections.				
1	25 x 6 mm GI tape	RM	40		
h.	Supply and installation of following sizes of MS perforated type cable trays with stove enamel paint of approved colour and necessary bends, tees, reducer couplers, dash-fasteners, GI nuts bolts including cutting, bending, drilling, bolting required suspension arrangement fabricated from steel etc. Complete as per specifications and as approved by Engineer - in - charge. The suspension of MS cable tray, only GI or SS round rods with ceiling anchoring facility should be used.				
1	150mm wide, 40 mm high (2 mm thick)	RM	10		
D.	FIXING OF LIGHTING FIXTURES				
a	Receiving, fixing in position, effecting proper connections, testing and commissioning of 1 x 36 /2 x 36 watt CFL fixtures fixed recessed in ceiling with chains hung from slab with all fixing accessories as required, along with providing PVC flexible conduit	Nos	30		



Sr. No.	Description	Unit	Quantity	Unit Rate	Amount
	from junction box at slab level to fixture on the false ceiling.				
E.	SUPPLY OF LIGHTING FIXTURES				
a.	The fixtures shall be suitable for single phase, 50 cycles, 230 Volts, A.C. supply system.				
b.	All fixtures shall be factory wired with copper conductor wires.				
c.	All fixtures shall be supplied with Electronic ballasts, fluorescent lamps/bulbs, as specified.				
d.	The rate shall be quoted for the Catalogue no. specified for the fixture however if contractor wants to supply equivalent then sample shall have to be got approved from Architect before procurement.				
e.	All the samples shall be submitted within two weeks of the issue of work order, for approval from the Architect.				
f.	Supply, unloading storing and installation at site of the following fixtures with all accessories as per ceiling design, such as spring loaded side holders, starters, power factor compensators, MS housing to house ballasts, complete with lamps. All the lamps shall be colour 84 or as approved.				
1	2x2 feet or 4 feet light 430 (2X36 W)	Nos	4		
2	LED 18 Watt	Nos	10		
F.	CONSTRUCTION POWER AND LIGHTING				
a	Providing temporary construction lighting and power on the third floor including by using required nos. 1 x 36 Watt phatti type fixtures (minimum 250 Lux), required flexible double insulated copper wiring, distribution board, minimum 3 nos. 400 W halogen flood light, earthing, main panel with incoming MCCB and required MCCB in the outgoing for distributing the power through the duration of the project. It will be the responsibility of Electrical Contractor to distribute power to all the contractors working at site. The rates shall be all inclusive. The material bought by the contractor shall be the property of the contractor and after the work is completed it can be taken back by him. (All item mentioned above, shall be new and of good quality by considering site safety parameter. Old and repaired item shall never be allowed to use at site.)	LS	1		
G.	MODULAR FURNITURE FOR WORKSTATIONS				



Sr. No.	Description	Unit	Quantity	Unit Rate	Amount
1	1800x750mm: Linear workstation Panel based system, .25mm thick. Pre-lam table top shade-laminate, powder coating shade; grey - All tiles will be fabric: supported on gable end along with 25mm thick partition. Height of workstations - 1200mm 1, No. Three drawer with one lock, all complete with wire management and wire risers Fire Rated material for workstation The requisite certifications include: ASTM D2571 (for surface burning), ANSI/NEMA LD3 certified scratch-resistant laminate.	Nos	1		
2	Chair	Nos	1		

3.1.4. Civil Works and interiors of C2i

S No.	Description	Unit	Qty.	Unit Rate	Amount
A.	INTERIOR WORKS & FURNISHINGS				
a.	Civil Works				
1	Manual PCC (1:2:4 mix) Up to 75mm/ Repair of existing floor with cement plaster before laying Tiles	sqm	10		
2	Floor Tiles (C2i average area is 600 to 800 SQFT but in most of the site Floor tile work was done so repair and match with existing tile cost will be Lump sum)	L/S	1		
b.	CEILING				
1	Plain Gypsum Ceiling	sqm	20		
2	Mineral fibre Tile Grid Ceiling size: 2' x 2' -	sqm	20		
3	Access Panel of size 2' x 2'	nos	1		
c.	FINISHES				
1	Light Textured Paint	sqm	84		
B	Electrical Works				



S No.	Description	Unit	Qty.	Unit Rate	Amount
a.	Wiring including termination for the following light points with 2 x 2.5 sq. mm PVC insulated FRLS copper conductor wires of 650/1100 Volts grade in concealed/exposed 16gauge MS conduits as called for including providing 6-amp flush type switches, anodized MS box for housing switches approved White Polycarbonate modular cover plate for switch boxes and earthing. All the circuit must dress with circuit identification tags (the rates include: 6 AMP switch, 6 AMP socket, Modular Face plate, FRLS Cable with average length 20-30 m, 16 gauge MS conduits 20-30 meter, All the accessories and Workmanship.)				
1	First point controlled by one no. 6 amp switch.	Nos	2		
2	Same as item No. 1 above but LOOP POINT i.e. wiring including termination of point looped from first point with 2 x 1.5 sq. mm PVC insulated FRLS copper conductor wire of 650/1100-volt grade in concealed/exposed 16-gauge MS conduit and earthing (controlling switch in item no. 1).	Nos	4		
b.	Wiring including termination for the following light points with 2 x 2.5 sq. mm PVC insulated FRLS copper conductor wires of 650/1100 Volts grade in concealed/exposed 16gauge MS conduits as called for including providing 16-amp flush type switches, anodized MS box for housing switches approved White Polycarbonate modular cover plate for switch boxes and earthing. All the circuit must dressed with circuit identification tags (the rates include: 16 AMP switch, 16 AMP socket, Modular Face plate, FRLS Cable with average length 20-30 m, 16 gauge MS conduits 20-30 meter, All the accessories and Workmanship.)				
1	First point controlled by one no. 16 amp switch.	Nos	2		
2	Same as item No. 3 above but LOOP POINT i.e. wiring including termination of point looped from first point with 2 x 1.5 sq. mm PVC insulated FRLS copper conductor wire of 650/1100-volt grade in concealed/exposed 16-gauge MS conduit and earthing (controlling switch in item no. 3).	Nos	4		



S No.	Description	Unit	Qty.	Unit Rate	Amount
3	Wiring including termination for 6-amp socket outlet point with 2 x 1.5 sq. mm PVC insulated FRLS copper conductor wires in concealed/exposed 16gauge MS conduits or existing raceways including providing 6-amp switch, 3 pin 6A shuttered socket, anodised MS box for housing switches sockets, approved White Polycarbonate modular cover plate and earthing. (Looped to lighting circuit as shown in drawing). All the circuit must be dressed with circuit identification tags	Nos	2		
c.	fixing following numbers socket and switch housed in anodised MS box with approved White polycarbonate modular cover plate as required. NOTE: - For UPS in one circuit maximum three workstations shall be looped. Colour coding shall be strictly followed for wiring. For Raw in one circuit maximum six workstations shall be looped. All the circuit must be dressed with circuit identification tags				
1	2 No. 16A, Universal Socket outlets controlled by 1 No. 16A switch. (UPS power at W/S)	Set	2		
2	1 No. 6A, round pin outlets, controlled by 1 no.6A switch. (Raw power at W/S)	Set	4		
3	Wiring including termination for 16 amp power socket outlet points with 2 x 6 sq. mm PVC insulated FRLS copper conductor wires for the first socket outlet and 2 x 4 sq. mm PVC insulated FRLS copper conductor wires for the second outlet of 650/1100 Volts grade in concealed/exposed 16 gauge MS conduits or existing raceway as called for including providing 16 amp flush type combined 6 pin shuttered sockets and switches, anodized MS outlet boxes for 16 A 6 pin sockets and switches, approved White Polycarbonate modular cover plate and earthing. (The item is for set of two outlets looped together as explained above) All the circuit must be dressed with circuit identification tags (the rates includes 16 AMP switch, 16 AMP socket, Modular Face plate, 2x 6 SQ. MM FRLS Cable with average length 20-30 m, 16 gauge MS conduits 20-30 meter, All the accessories and Workmanship.):	Set	2		



S No.	Description	Unit	Qty.	Unit Rate	Amount
4	Supplying and fixing of 32 amp 3-pin for 1-phase industrial socket outlet, Self-locking type of Neptune Balls make including supplying MS boxes of suitable size, 32-amp DP MCB and a plug top, complete as required and as per specifications.	Nos.	2		
d.	Supplying and fixing in position of the following sizes of exposed/concealed 16 gauge MS conduit including all accessories complete as required and as per specifications.				
1	25 mm die MS conduit	RM	40		
e.	Supplying, drawing, termination of the following size of FRLS PVC insulated copper conductor wires 650/1100 V grade in existing conduits, complete as required and as per specifications.				
1	2 x 6 sq. mm with 1 no. 2.5 sq. mm PVC insulated copper conductor earth wire.	RM	20		
C.	INSTALLATION OF PANELS; SUPPLY AND INSTALLATION OF DB, CABLES AND EARTHING				
a.	Receiving, storing properly, installation, testing and commissioning of following panels complete as required.				
1	MDB's	Set	1		
b.	Supply and fixing in position the following insulated wires including providing all fixing accessories and effecting proper connections.				
1	6 sq. mm. dia pvc insulated copper conductor wire.	RM	20		
c.	Supplying, unloading, storing, laying, testing and commissioning (SITC) of following sizes PVC insulated (Heavy duty) Copper conductor cables suitable for working voltage up to and including 1100 Volts, laid and tied on existing overhead cable trays; or laid and tied over MS supports in masonry trenches including providing MS supports and clamps for fixing to supports in an approved manner complete as required and as per specifications. Circuit identification tag should be attached with the concerned cable along with the test report of following sizes of cable to be submitted by the contractor at the time of delivery of material at site.				
1	50 sq. mm. cable, armoured for earthing.	RM	5		



S No.	Description	Unit	Qty.	Unit Rate	Amount
d.	Termination of the following sizes of PVC insulated Copper conductor cable including providing terminal lugs, single compression glands crimping the joints, providing insulation tape, effecting terminal connections to the equipment complete as required.				
1	50 sq. mm. cable, armoured for earthing.	Nos.	4		
e.	Supplying, unloading, storing, laying, testing and commissioning of following sizes of XLPE insulated (Heavy duty) Aluminium/copper conductor armoured cables suitable for working voltage up to and including 1100 Volts , laid and tied on existing overhead cable trays; or laid and tied over MS supports in masonry trenches including providing MS supports and clamps for fixing to supports in an approved manner complete as required and as per specifications.				
1	4 x 6 sq.mm. copper Cable	RM	5		
2	2 x 10 sq.mm. copper Cable	RM	5		
f.	Termination of the following sizes of PVC insulated Aluminium conductor cable including providing terminal lugs, single compression gland, crimping the joints, providing insulation tape, effecting terminal connections to the equipment complete as required				
1	4 x 10 sq.mm. copper Cable	Nos.	4		
2	4 x 6 sq.mm. copper Cable	Nos.	4		
3	2 x 10 sq.mm. copper Cable	Nos.	4		
4	2 x 6 sq.mm. copper Cable (For Dedicated earthing and body earthing of DB's)	Nos.	4		
5	Supply, installation, testing and commissioning of Earth box made of 2mm thick MS painted, with a glass cover and having 25 x 3 mm Cu strip with insulators complete as required.	Set	1		
6	25 x 6 mm GI tape	RM	20		
7	Supply and installation of following sizes of MS perforated type cable trays with stove enamel paint of approved colour and necessary bends, tees, reducer couplers, dash-fasteners, GI nuts bolts including cutting, bending, drilling, bolting required suspension arrangement fabricated from steel etc. (100 mm to 300 mm with 40 mm height) Complete as per specifications and as approved by Engineer - in - charge. The suspension of MS cable tray, only GI or SS round rods with ceiling anchoring facility should be used.	RM	2		



S No.	Description	Unit	Qty.	Unit Rate	Amount
D.	SUPPLY & FIXING OF LIGHTING FIXTURES				
a.	Supply, unloading storing and installation at site of following PL lamp / halogen fixtures complete with all accessories and PL lamp / halogen lamps with toroidal transformer, electronic ballast completes as required.				
1	LED 18-watt light	Nos	4		
E.	MODULAR FURNITURE FOR WORKSTATIONS				
1	Panel based system, Pre-lam table top shade-laminate, with drawer fixed pedestal per work station	Nos	1		
2	Chair	Nos	1		
	TOTAL OF C2i NON-IT COMPONENTS				

3.1.5. Civil Works and interiors of Data Centre

Sr. No.	Description	Unit	Qty.	Unit Rate	Amount
A	Civil Works				
1	PCC Up to 75mm/ Repair of existing floor with cement plaster before laying Tiles/ Floor carpet.	sqm	810		
2	Cement Sand Plaster	sqm	146		
3	Floor/Wall Chasing	L/S	2		
B	JOINERY				
1	P8: Partition Above false ceiling with one layer of gypsum on both sides	sqm	145		
2	P9: Fire rated Partition panelling	sqm	448		
3	P9A: Fire Rated Partition	sqmt	95		
4	G: Full height 12mm thick. Toughened double glass partition	sqm	12		
5	P10: Modular extruded aluminium Partitions	rm	12		
6	Extruded Aluminium Skirting	rm	120		
C	DOORS				
1	D1 -Fire rated door - up to 750 x 2100	nos	6		
2	D2 -Fire rated door - up to 1200 x 2100	nos	1		
3	D1 -Fire rated door - up to 900 x 2100	nos	1		
D	CEILING				
1	Plain Gypsum Ceiling fire rated	sqm	-		
2	Vertical Bands with fire rated gypsum board	rm	-		
3	Cove with fire rated gypsum board	rm	-		
4	Tile Grid Ceiling - 2' x 2' - Metal ceiling	rm	390		



Sr. No.	Description	Unit	Qty.	Unit Rate	Amount
E	FINISHES				
1	Light Textured Paint	sqm	1952		
2	Laminated Panelling fire rated board	sqm	48		
F	STORAGE				
1	Full Ht. Storage (Laminated) 400mm Deep fire rated	sqm	8		
G	FLOORING				
1	Raised Antistatic Access Flooring (Range: 300mm-600mm)	sqm	460		
2	Stainless Steel edge trims	rm	16		
3	Base structure for additional support of raised floor	sqm	395		
H	SIGNAGES				
1	General Information Signage	nos	12		
2	Luminous Fire evacuation plans	nos	4		
I	LOOSE FURNITURE				
1	Guard Table - 1500 X 700 WIT HPEDESTAL	nos	1		
2	CHAIRS	nos	4		
3	Running counter in DATA Centre (BMS Room)	nos	4		
J	MISCELLANEOUS INTERIOR ITEMS				
1	MS STANDS FOR PAC	nos	7		
2	Graphics as per designer	sqft	250		
K	HVAC: AIR HANDLING UNIT, CHILLED WATER PIPING, AIR DISTRIBUTION, INSULATION				
a.	EQUIPMENT				
	AIR HANDLING UNITS				
	Supply, Installation, Testing & Commissioning of Double skin AHUs of following capacities.				
1	13,000 CFM @ 50mm SP - Floor Mounted	Nos	2		
b.	INLINE FANS				
	Supply, Installation, Testing and commissioning of circular inline duct mounted fans for exhaust air having backward/ forward curve impeller directly driven with single phase motor complete with bird screen. The fan shall have following capacities:				
1	600 cfm @ 10 mmwg for Ladies Toilet Exhaust	Nos.	-		
2	700 cfm @ 10 mmwg for Gents Toilet Exhaust	Nos.	-		
3	650 cfm @ 15 mmwg for Cafeteria Exhaust	Nos.	-		
c.	PIPING				
	CHILLED WATER PIPING				



Sr. No.	Description	Unit	Qty.	Unit Rate	Amount
	Providing and fixing in position the following MS heavy class pipes cut to required lengths and installed with all welded joints. Providing and fixing in position the necessary fittings like elbows, tees, reducers, hanging arrangements including vibration isolation arrangements etc. as required.				
1	125 mm dia	RM	20		
2	80mm dia	RM	20		
3	40mm dia	RM	50		
d.	Providing and fixing in position the following wafer type Butterfly Valves complete with companion flanges, nuts, bolts, gaskets etc. as required. Butterfly valves shall conform to PN -16 rating as per specifications. Quoted price shall be inclusive of insulation as per the specifications.				
1	80mm dia	Nos.	2		
e.	Providing and fixing in position the following Ball Valves as per the specifications. Quoted price shall be inclusive of insulation as per the specifications.				
1	40mm dia	Nos.	2		
f.	Providing and fixing in position the following specified make balancing valves. Balancing valves shall conform to PN-16 rating as per the specifications. Quoted price shall be inclusive of insulation as per the specifications.				
1	125 mm dia	Nos.	1		
2	80mm dia	Nos.	1		
g.	Supply, Installation, Testing & commissioning of two way diverting valves with modulating motor, transformer, copper control wiring & temperature sensors for AHUs. The valves shall be of the following sizes.				
1	125 mm dia	Nos.	1		
2	80mm dia	Nos.	1		
h.	Providing and fixing in position the following 'Y' strainers complete with insulation for AHUs & FATUs.				
1	125 mm dia	Nos.	1		
2	100mm dia	Nos.	R.O.		
3	80mm dia	Nos.	1		
4	Providing and fixing in position industrial type pressure gauges constructed out of SS 304 material. SS siphon shall be factory insulated with closed cell elastomeric insulation in tubing form. Pressure gauges shall be factory fitted with a ball valve at the tube.	Nos.	4		
5	Supply and fixing in position V-form industrial type thermometers as per the specifications.	Nos.	4		



Sr. No.	Description	Unit	Qty.	Unit Rate	Amount
i.	Providing and fixing in position the following GI medium class pipes for condensate drain cut to required lengths & installed with all screwed joints and providing and fixing in position the necessary elbows, tees & reducers.				
1	50mm dia	RM	20		
2	40mm dia	RM	20		
3	25mm dia	RM	20		
j.	AIR DISTRIBUTION				
	Supply, installation and testing of factory fabricated ductwork of galvanised sheet metal, fire retardant gaskets, slip on flanges, GI fully threaded rods, GI channel supports etc. in accordance with the approved shop drawings and specifications.				
1	26-gauge GSS	SqM	60		
2	24 gauge GSS	SqM	60		
k.	Supply, Fabrication at site, Installation and Testing of sheet metal ducts in accordance with the approved shop drawings and specifications.				
1	0.63mm (24 gauge) GSS	SqM	10		
2	0.8 mm (22 gauge) GSS	SqM	10		
3	1.0mm (20 gauge) GSS	SqM	10		
4	1.25mm (18 gauge) GSS	SqM	10		
5	Supply, Installation and Testing of 125mm deep Anti-vibration Flexible Joints made out of imported fire-retardant fabric with extruded aluminium frame/ flange on both sides of approved make.	Nos	3		
6	Supply, Installation and Testing of multi blade type key operated louver dampers of G.I. steel sheet for collars to be provided with suitable links, levers and quadrants for manual control of volume of air flow and for proper balancing of the air distribution system as per the approved shop drawings and specifications.	Sqm	5		
7	Supply, Installation and Testing of multi-blade box type G.I. steel sheet dampers for ducts to be provided with suitable links, levers and quadrants for manual control of volume of air flow and for proper balancing of the air distribution system as per the approved shop drawings and specifications.	SqM	3		
l.	Supply, Installation, Testing and Commissioning of smoke cum fire dampers of at least 90-120 minutes' fire rating as per the approved shop drawings and specifications. Interlocking of fire dampers using copper control wiring shall be affected as required				
1	Bare fire dampers	SqM	4		



Sr. No.	Description	Unit	Qty.	Unit Rate	Amount
2	Actuator with control panel, temperature sensor and spring return action and suitable for 8 NM Torque.	No	6		
m.	Supply, Installation, Testing and Balancing of square supply air diffusers as per the approved shop drawings and specifications. Each diffuser shall be equipped with fixed air distribution grid, removable key-operated volume control damper. The diffusers shall be anti-smudge ring/flush type.				
1	Powder coated extruded aluminium diffusers of approved colour & shade of following sizes:	Sqm	5		
n.	Supply, Installation, Testing and Balancing of square diffusers same as supply air diffusers but without volume control dampers for return air as per the approved shop drawings & specifications.				
1	Powder coated extruded aluminium diffusers of approved colour & shade of following sizes:	Sqm	5		
2	Supply, Installation and Testing of extruded aluminium powder coated linear grilles for supply/ return air.	RMT	45		
o.	Supply, Installation, Testing and Commissioning of pre-insulated factory fabricated flexible ducts inner as well as outer skin constructed out of aluminium sheet. Ducts shall be of following sizes				
1	300mm dia	RM	20		
2	250mm dia	RM	90		
3	200mm dia	RM	20		
4	150mm dia	RM	20		
5	Supply, Installation and Testing of extruded aluminium powder coated air transfer grilles to be provided at toilets & kitchen doors.	SqM	1		
6	Supply, Installation and Testing of fresh air grilles of powder coated / anodized extruded aluminium with filters, inlet louvers dampers and bird screen, as per approved shop drawings and specifications.	SqM	1		
p.	INSULATION				
	Supply and Application of acoustic lining/ internal thermal insulation of supply air ducting with fibre glass insulation 48 Kg/cum density and as per the specifications and drawings.				
1	25mm thick	Sq.	45		
q.	Supply and Application of external thermal insulation of ducting using closed cell elastomeric insulation with adhesive, longitudinal & transverse joints sealed with adhesive as per specifications.				
1	6 mm thick	SqM	550		
r.	Supply and Application of 50mm thick expanded polystyrene insulation in tubing form/ flat sections of				



Sr. No.	Description	Unit	Qty.	Unit Rate	Amount
	20 Kg/cum density for chilled water piping finished with 24 G Al sheet cladding and as per the specifications				
1	125 mm dia	RM	20		
2	80mm dia	RM	20		
3	40mm dia	RM	50		
s.	Supply and Application of 9 mm thick closed cell elastomeric insulation in tubing form for condensate drain piping as per the specifications.				
1	50mm dia	RM	20		
2	40mm dia	RM	20		
3	25mm dia	RM	20		
t	Supply and Application of thermal/acoustic lining of walls & ceiling of AHU rooms using fibre glass insulation 32 Kg/cum density, mounted on a suitable frame work made out of 24 G GI sheet channels, covered with RP tissue and finished with 24 gauge perforated aluminium sheet as per the specifications.				
1	50mm thick	SqM	70		
L	PAC				
a-1	Name of Work :- Supply, installation, testing & commissioning of precision Air-conditioning unit (7 x 20 TR) capacity FOR 7TH FLOOR DATA CENTRE Part A (PAC High Side & Low Side) Precision Air Conditioning Units - For server room (With Heater & and Humidifier)				
a-2	Supply, installation, testing and commissioning of microprocessor based, Precision Air Conditioning Unit comprising Indoor & outdoor units interconnected with refrigerant piping. The indoor evaporator unit, shall be BOTTOM discharge. The fan section should be below false floor to provide high power savings compared to fans inside the cabinet. The fans should be mounted in a separate cabinet and the cabinet should be located under the false floor. The Indoor fan shall be with centrifugal blowers with latest innovative EC fan technology with "COMPOSITE Blade material ", and other accessories, in all respect. 95% down to 5 micron filters with filter section & minimum 4 row deep slant type copper cooling DX-coil with aluminium fins, SS drain tray duly insulated, high technology fixed speed scroll compressor suitable for R407C refrigerant, Compressor refrigerant circuit (Two compressors with Independent Circuits) shall have vibration absorbers at suction & discharge lines, with strip type reheated & steam electrode humidifier.				



Sr. No.	Description	Unit	Qty.	Unit Rate	Amount
	Compressor EER should not be less than 11.1 Btuh / Watt (COP not less than 3.25 at ARI conditions), electronic expansion valve & electrical control panel, all inside a cabinet. The Indoor cabinet shall be with double skin side panels & front & back panels shall be with 25mm thick acoustic mineral wool insulation. The outdoor air cooled condensing unit shall be oversized to handle high ambient conditions. Condenser shall have copper condensing coil with aluminium fins. The outdoor condenser shall have EC fans which will vary speed depending upon ambient temperature and suitable for vertical or horizontal hot air discharge as per the site conditions. Separate condenser unit shall be provided for each refrigerant circuit. A heat rejecting coil block shall be constructed out of copper tubes with expanded aluminium fins to give a good mechanical bond for maximum heat transfer. The number of fins shall not be less than 12 fins per inch. The minimum face area of the coil should be more than 1.3 sq.m. and should be minimum 3 Rows deep. Fins thickness shall not be less than 0.1 mm and shall be provided with epoxy /suitable weather proof coating. A minimum of two numbers axial flow fans (dia 500) directly driven by Electronically Commutated (EC) fan motor unit with variable speed drive shall be provided for each condenser unit. Condensers with AC fan motors are strictly not accepted as EC fan motors are more efficient than AC fan motors. The condenser unit shall suitably design for noise level ≤ 75 dB at a distance of 1 meter away from outdoor unit. The outdoor condenser must be provided with Electronically commutated motors which must include micro-controller with option to set ambient temperatures / system pressure etc. The logic of operation of EC motor must be to maintain a constant discharge pressure in the circuit irrespective of ambient temperatures. The Condenser unit shall be suitable for round-the-clock operation. The body of the condenser unit shall be made out of 16 SWG (1.6mm) corrosion resistant G.I. Sheet. The entire stand shall be supported by epoxy coated frame. The condensers should have anti-corrosive coating from factory. The indoor unit shall also have heater. The				



Sr. No.	Description	Unit	Qty.	Unit Rate	Amount
	external static pressure of fan shall not be less than 10mm Wg. The controller of the unit shall be intelligent. The controller shall also have auto sequential operation of Precision Air Conditioning Units. PAC shall have at least two dry contacts for remote alarms. The quoted price shall be inclusive of interconnected insulated refrigerant piping, insulated drain piping with in the room & from each machine, vibration isolation pads and associated electrical & control cabling between indoor & outdoor units and MS base frame / MS Platform duly painted with black enamel paint for mounting of condensing units and suitable vibration isolation pads.(Each unit should have a inbuilt card for Bacnet/Modbus output for BMS monitoring). The raised flooring height from true floor shall have to be 600 MM				
a-3	The Unit shall be with Two Fixed scroll Compressor with two independent refrigerant circuit				
a-4	The unit shall be suitable for 380-415 Volts / 50HZ /3 Phase supply.				
a-5	The refrigerant piping of copper duly insulated with 13/19mm thick nitrile rubber class "O" having K value as 0.032 W/ m Deg. K shall be to the extent of 30M (Max.) one way on each unit. Bidder to include suitable size (dia) of this much length of piping in the BOQ. (20M horizontal + 10M of Vertical piping).				
a-6	Units shall also be suitable to deliver the desired capacity after deration for such a distance of piping. deration for such a distance of piping.				
a-7	Bidder to include suitable size (dia) extra length of piping in the BOQ along with kit (solenoid valve, NRV, extra oil charge & extra refrigerant charge.				
a-8	Water connection shall be provided at one point with in 5m in the room. The entire onward piping up to the machines shall be done by other agency.				
a-9	Drain piping with insulation and connection up to 10 M the nearest drain point in the room shall be included. The drain piping shall be of 25mm dia GI 'B' Class duly insulated with 9mm thick nitrile rubber.				
a-10	The interconnecting copper conductor control & power cabling with earthing between indoor & outdoor units of adequate size & quantity to be considered along with GI cable tray.				



Sr. No.	Description	Unit	Qty.	Unit Rate	Amount
a-11	The incoming copper cabling along with earthing from the indoor isolator to AC unit shall also be accounted for in the scope of work.				
a-12	Outdoor Unit's power isolator in weather proof IP66 Plastic enclosure mounted on the outdoor unit itself for power ON/OFF to outdoor.				
a-13	Nitrogen testing, vaccumising and testing and commissioning of the unit complete in all respect.				
a-14	Each unit should have a inbuilt card for Bacnet/Modbus output for BMS monitoring.				
a-15	The unit shall have water leak detection sensing tape with alarm initiation system, on detection of water leakage under the machine in the vicinity.				
a-16	The unit shall have a feature to trip off automatically in the event of receiving a fire signal from the fire detection system. The necessary cabling between the fire relay control module with in the space/room and the unit's controller shall be considered				
1	20 TR actual capacity Floor Discharge Type Precision AC Units for Data centre. (1W + 1S) at 45°C outdoor temperature. Inside design conditions Cold Aisle Condition = 20 +/- 1°C Return Air Condition = 30 Deg C [The cost of (a). Installation, Testing & Commissioning charges for complete Precision Air Conditioning Unit & (b) Handling & Positioning of units at site (Without Crane) to be included in the quoted price.]	Nos	7		
b	ADVANCED AIR TERMINAL DISTRIBUTION (Supply Air modulator Grilles) COMPRISING OF :				
1	Top Cover, GI Powder Coated with perforations to deliver airflow of 1000 CFM, with aerofoil aluminium damper, suitable to take the load of the rack up to 800kgs per tile of size 595mmX595mm, provision for fitment and operation of microprocessor controller with display.	Nos.	80		
2	Actuator to modulate the vanes from 0 to 100% to take feedback from the sensors.	Nos.	40		
3	Microprocessor controller or PLC based interface with programmable control logic protocol, including two sensors to modulate the airflow from 0 to 100% based on the rack temperature and regulating the right amount of air volume. The average of both sensors to be input for actual conditions to the control logic. Display to be settable for temperature, communication on Modbus to be available.	Nos.	40		
c	Supply, installation, balancing and commissioning of fabricated at site GSS sheet metal rectangular/round				



Sr. No.	Description	Unit	Qty.	Unit Rate	Amount
	ducting complete with neoprene rubber gaskets , elbows, splitter dampers, vanes, hangers, supports etc. as per approved drawing and specification of following sheet thickness complete as required.				
1	22 gauge (0.83 mm)	sqmtr	45		
2	24 gauge (0.63 mm)	sqmtr	45		
d	LOW SIDE INSTALLATION WORKS				
1	Refrigerant R 407C	Kgs	450		
2	Refrigeration Piping: Supply, Installation, Testing & Commissioning of high-pressure copper refrigerant piping suitable for R 407c refrigerant of suitable size as required and duly insulated with 19mm/13mm thick closed cell elastomeric insulation in tubing form inclusive of glass cloth and UV treatment as per specification/requirement. External Refrigerant piping shall be laid on GI covered cable trays. Piping inside occupied spaces shall be supported using GI ladder type cable trays. The cost of GI covered cable tray and supports to be included in the quoted price. Entire refrigerant piping work be carried out in accordance with the specifications.	RM	320		
e	Control & Transmission Wiring: Supply and fixing of PVC insulated armoured COPPER cables 1100 Volts grade from main panel boards to various equipment through walls/ceiling with appropriate clamps, cable termination, and fixing arrangements, cable tray/ms conduit etc. as per specifications and drawings.				
1	3 c x 4 sqmm	RM	320		
f	Humidifier Piping: Supplying, laying/ fixing, testing and commissioning of G.I 'B' class pipe with 19 mm nitrile insulation of following sizes for drain water piping on surface / underground (including fabrication of bends, tees, reducers) with support and fittings as per standard specification complete as required for humidifier connection.				
1	25 mm O.D.(insulation : 13 mm)	RM	140		
2	32 mm O.D.(insulation : 13 mm)	RM	140		
3	Supply, Fabrication and Installation of MS frame using channels/angle iron sections as required for IDU & ODU stand for PAC units. The frame work shall be applied with red oxide primer and thereafter, two coats of enamel paint of approved colour. The general arrangement drawing for frame work shall be got approved from the Architects/Structural Engineers prior to commencement of fabrication.	No's	16		



Sr. No.	Description	Unit	Qty.	Unit Rate	Amount
g	Drain Piping Supply & Installation of heavy duty PVC drain pipe with min. wall thickness of 4 mm with insulation. Insulation shall be of 6 mm thick sleeve of nitrile rubber/polyethylene foam having K value 0.027 W/mk at a mean temp. of 10°C and min. density of 26 Kg/m ³ . Insulation on drain pipe shall be carried out only where the pipe is running within the wall. Exposed pipe shall be without insulation. The insulation joints shall be properly sealed with rubber based adhesive to ensure proper bonding.				
1	50 mm dia	RM	40		
2	40 mm dia	RM	40		
3	32 mm dia	RM	60		
4	25 mm dia	RM	60		
h	Power Cable Supply, laying, affecting connections and Testing of the following sizes of 1.1 KV armoured PVC insulated copper conductor cables. Cables shall be inclusive of all clamps, saddles, screws, cable identification tags, cable terminal joints including terminal lugs, insulating tapes, affecting terminal connections to the equipment as per the specifications and as required. Quoted price shall be inclusive of GI perforated cable tray, support.				
1	4C x 25 Sq mm copper Cable	RM	400		
2	Providing & fixing of thermal insulation with aluminium foil faced nitril rubber/closed cell expended polyethylene insulation of following thickness class 'O' (25-30kg/m ³) on existing surface with dendrite etc. complete as required. (for Floor / Walls/ Ceiling Insulation) - 19mm Nitrile rubber with Silver Coating	sqmtr	1480		
M	Electrical Works				
a	Wiring and sockets Wiring including termination for the following light points with 2 x 2.5 sq. mm PVC insulated FRLS copper conductor wires of 650/1100 Volts grade in concealed/exposed 16gauge MS conduits as called for including providing 6 amp flush type switches, anodized MS box for housing switches approved White Polycarbonate modular cover plate for switch boxes and earthing. All the circuit must dressed with circuit identification tags				
1	First point controlled by one no. 6 amp switch.	Nos	30		
2	Same as item No. 1 above but LOOP POINT i.e. wiring including termination of point looped from first point	Nos	40		



Sr. No.	Description	Unit	Qty.	Unit Rate	Amount
	with 2 x 1.5 sq. mm PVC insulated FRLS copper conductor wire of 650/1100-volt grade in concealed/exposed 16 gauge MS conduit and earthing (controlling switch in item no. 1).				
b	Wiring including termination for the following light points with 2 x 2.5 sq. mm PVC insulated FRLS copper conductor wires of 650/1100 Volts grade in concealed/exposed 16gauge MS conduits as called for including providing 16-amp flush type switches, anodized MS box for housing switches approved White Polycarbonate modular cover plate for switch boxes and earthing. All the circuit must dressed with circuit identification tags				
1	First point controlled by one no. 16 amp switch.	Nos	5		
2	Same as item No. 3 above but LOOP POINT i.e. wiring including termination of point looped from first point with 2 x 1.5 sq. mm PVC insulated FRLS copper conductor wire of 650/1100-volt grade in concealed/exposed 16 gauge MS conduit and earthing (controlling switch in item no. 3).	Nos	15		
3	6-amp socket outlet point with 2 x 1.5 sq. mm PVC insulated FRLS copper conductor wires in concealed/exposed 16gauge MS conduits or existing raceways including providing 6-amp switch, 3 pin 6A shuttered socket, anodised MS box for housing switches sockets, approved White Polycarbonate modular cover plate and earthing. (Looped to lighting circuit as shown in drawing). All the circuit must dressed with circuit identification tags	Nos	25		
c	Wiring including termination for the following configuration of outlets for workstations with 3 core x 2.5 sq.mm. Copper conductor, PVC insulated PVC sheathed wires of 650/1100V grade in existing conduit/raceway including supplying and fixing following numbers socket and switch housed in anodised MS box with approved White polycarbonate modular cover plate as required. NOTE: - For UPS in one circuit maximum three workstations shall be looped. Colour coding shall be strictly followed for wiring. For Raw in one circuit maximum six workstations shall be looped. All the circuit must be dressed with circuit identification tags				
1	2 No. 16A, Universal Socket outlets controlled by 1 No. 16A switch.(UPS power at W/S)	Set	25		
2	1 No. 6A, round pin outlets, controlled by 1 no.6A switch. (Raw power at W/S)	Set	10		



Sr. No.	Description	Unit	Qty.	Unit Rate	Amount
3	Wiring including termination for 16 amp power socket outlet points with 2 x 6 sq. mm PVC insulated FRLS copper conductor wires for the first socket outlet and 2 x 4 sq. mm PVC insulated FRLS copper conductor wires for the second outlet of 650/1100 Volts grade in concealed/exposed 16 gauge MS conduits or existing raceway as called for including providing 16 amp flush type combined 6 pin shuttered sockets and switches, anodised MS outlet boxes for 16 A 6 pin sockets and switches, approved White Polycarbonate modular cover plate and earthing.(The item is for set of two outlets looped together as explained above) All the circuit must dressed with circuit identification tags	Set	5		
4	Wiring including termination for 16 amp power socket outlet point with 2 x 4 sq. mm PVC insulated FRLS copper conductor wire of 650/1100 Volts grade in concealed/exposed 16 gauge MS conduits or in existing raceway including providing 16 amp flush type combined 6 pin shuttered socket and switch, anodised MS boxes for 16 amp 6 pin socket and switch, approved White Polycarbonate modular cover plate and earthing. (Only one outlet shall be connected to each circuit). All the circuit must dressed with circuit identification tags	Nos	10		
5	Supplying and fixing of 16/20 amp 3-pin for 1-phase industrial socket outlet including supplying MS boxes of suitable size,32 amp SP MCB and a plug top, complete as required and as per specifications.	Nos	R.O		
6	Supplying and fixing of 32 amp 3-pin for 1-phase industrial socket outlet, Self-locking type of Neptune Balls make including supplying MS boxes of suitable size,32 amp DP MCB and a plug top, complete as required and as per specifications. (DATA CENTRE)	Nos	224		
7	Supplying and fixing of 32 amp 3-phase industrial socket enclosure, IP 65 including supplying boxes of suitable size, 40 amp TP MCB and complete as required and as per specifications.	Nos	R.O		
d	Supplying and fixing in position of the following sizes of exposed/concealed 16gauge MS conduit including all accessories complete as required and as per specifications.				
1	25 mm dia MS conduit	RM	150		
e	Supplying, drawing, termination of the following size of FRLS PVC insulated copper conductor wires 650/1100 V grade in existing conduits, complete as required and as per specifications.				



Sr. No.	Description	Unit	Qty.	Unit Rate	Amount
1	2 x 6 sq. mm with 1 no.2.5 sq. mm PVC insulated copper conductor earth wire.	RM	180		
N	CONDUITS AND MS PAINTED CHANNELS FOR STRUCTURED CABLING				
a	Anodized box				
1	Supplying and fixing in position MS anodised box for data/voice outlet suitable for fixing of RJ 45 jack complete as required.	Nos	180		
b	Supplying and fixing in position following sizes of 16 gauge MS conduits including providing all accessories concealed/ exposed as required.				
1	25 mm dia MS conduit (For Data/Voice wiring) (16 GAUGE) Complete with all fixing accessories	RM	1000		
2	32 mm dia MS conduit (For Data/Voice wiring) (16 GAUGE) Complete with all fixing accessories	RM	200		
c	Supply and fixing of following sizes of MS painted channel colour coded Orange for power, Blue for Data ,14 gauge, with openable cover and all accessories as required for fixing on wall/column/ceiling complete as required including providing junction boxes, bends and tees as required.				
1	300 mm x 50 mm	RM	200		
2	300 mm x 40 mm	RM	100		
3	200 mm x 50 mm	RM	120		
4	200 mm x 40 mm	RM	90		
5	150 mm x 50 mm	RM	R.O		
6	100 mm x 50 mm	RM	150		
7	450 mm x 200 mm MS powder coated	RM	120		
d	Supply and fixing of following sizes of MS painted channels, 14 gauge, with all accessories as required including junction boxes of depth more than the raceway (approx. 65 mm), colour coded with orange colour for power and blue colour for data, laid in floor including marking the routing, getting it approved, filling and plastering after laying the raceway, grouting the raceway to the floor, sealing of raceway cover, joints and junction boxes complete as required. Required junction boxes will be provided for smooth pulling of structured and power cabling. It will be the responsibility of the contractor to coordinate with structured cabling contractor for laying of cable.				
1	300mm x 40mm (3 mm thick cover)	RM	300		
2	200mm x 40mm (3 mm thick cover)	RM	210		
3	100mm x 40mm (2 mm thick cover)	RM	150		



Sr. No.	Description	Unit	Qty.	Unit Rate	Amount
4	Supply and fixing in position MS anodised box for T.V. outlet including white poly carbonate modular cover plate and co-axial type T.V. socket outlet complete as required.	Nos	40		
5	Supply , drawing, termination of RG-6 co-axial cable for TV in existing conduit complete as required.	RM	100		
e	Providing and fixing in position following sizes of MS conduits including providing all accessories concealed/ exposed as required along with G.I. pull wire,14 SWG				
1	25 mm dia MS conduit	RM	200		
2	Supply and ,installation of Novar/ Steel ways make floor mounted box 250 mm by 250 mm for housing UPS power and data/voice boxes complete as required.	Nos.	R.O		
f	SUPPLY OF MDB,UMDB,USDB				
f-1	MDB'S / UMDB / MCCB PANELS				
f-2	Design, manufacture, testing at works & supply of 2 mm thick MS sheet steel fabricated cubicle type Panel dust and vermin proof complete with hinged and lockable doors. All the panels shall be floor mounted and dead front construction complete with interconnections by copper tapes/ wires and painting.				
f-3	Each outgoing feeder shall be provided with one no. ON indication lamp. All MCBs shall be C curve type, except UMDB/ USDB in which MCB shall be D curve type.				
f-4	Multifunction, Ammeter, Voltmeter meters installed in MDB/UMDB shall be BMS Compatible, capable of delivering Bacnet, Modbus or Lon works protocol etc.				
f-5	MDB PANEL				
f-6	Incoming				
f-7	1 No. 800 amp FP MCCB, with microprocessor based release, minimum 25 KA service breaking capacity and Trip setting as required with phase setting at 50%. The two incomers and bus coupler shall be interlocked.				
f-8	Indicating Panel				
f-9	The Indicating panel of each incomer shall be provided with the following :				
f-10	Digital Ammeter ,CT's , Digital Voltmeter				
f-11	3 Nos. phase indicating lamps; backed up with HRC fuse/MCB.				
f-12	2 Nos. ON/OFF indicating lamp on incomer feeder for indicating the status of feeder.				
f-13	Bus Bar				
f-14	Outgoing				



Sr. No.	Description	Unit	Qty.	Unit Rate	Amount
f-15	Each outgoing feeder shall be provided with ON indication lamp.				
f-16	4No. 225 amp FP MCCB, with microprocessor based release, minimum 25 KA service breaking capacity and Trip setting as required.				
f-17	8 Nos. 63 A FP MCB,10 KA breaking capacity.				
1	MDB PANEL AS DESCRIBE ABOVE	Set	1		
g-1	UPS O/P PANEL				
g-2	Incoming				
g-3	1 nos 800 amp TP + 200% neutral MCCB, with microprocessor based release, minimum 25 KA service breaking capacity and Trip setting as required.				
g-4	Indicating Panel				
g-5	The Indicating panel of each incomer shall be provided with the following :				
g-6	Digital Ammeter ,CT's , Digital Voltmeter				
g-7	3 Nos. phase indicating lamps; backed up with HRC fuse/MCB.				
g-8	2 Nos. ON/OFF indicating lamp on incomer feeder for indicating the status of feeder.				
g-9	Bus Bar				
g-10	1 No. 800 amp TPN Copper Bus bar of suitable length with current density of 1.0 sq.mm/amp with neutral bus bar double size of phase bus bar.				
g-11	Outgoing				
g-12	Each outgoing feeder shall be provided with ON indication lamp.				
g-13	4 No. 220 amp FP MCB & 2 no of 63 amp DP MCB with 10 KA service breaking capacity as required.				
1	UPS PANEL FLOOR DISTRIBUTION PANEL	Set	1		
h	INSTALLATION OF PANELS; SUPPLY AND INSTALLATION OF DB, CABLES AND EARTHING				
	Receiving, storing properly, installation, testing and commissioning of following panels complete as required.				
1	MDB's	Set	1		
2	UMDB	Set	2		
3	Supply, installation, testing & commissioning of 225 Amp TP MCCB with heavy duty solid neutral link, rotary operating handle, 25 KA service breaking capacity with required arrangement of incoming & outgoing cables required.	Set	4		



Sr. No.	Description	Unit	Qty.	Unit Rate	Amount
i	Supplying, installing in position, testing and commissioning of the following Distribution Boards made of 16-gauge powder coated MS sheet steel, wall mounted/fully recessed in wall, indoor industrial type, with dust & vermin proof, hinged and lockable doors, double door design, complete with inter connecting wires of proper gauge, aluminium coated copper thimbles and with the circuit identification tags, colour coded wiring from Incomer MCB to each ELCB along with earthing terminal. The DB shall be suitable for taking cable/conduit as incoming/outgoing.				
1	14 way TPN DB with 36 Nos of 10/20 amps SP MCB's i.e. 12 Nos. of 10/20 amp SP MCB's arranged in 3 rows arranged in 3 tier one above other and controlled by 1 No. 63 amp TPN MCB and neutral link. Each row of MCB's shall be provided with 40 amp DP ELCB of 100 mA sensitivity.	Nos	R.O		
2	12 way TPN DB with 30 Nos of 10/20 amps SP MCB's i.e. 10 Nos. of 10/20 amp SP MCB's arranged in 3 rows arranged in 3 tier one above other and controlled by 1 No. 63 amp TPN MCB and neutral link. Each row of MCB's shall be provided with 40 amp DP ELCB of 100 mA sensitivity.	Nos	3		
3	12 way TPN DB with 30 Nos of 10/20 amps SP MCB's i.e. 10 Nos. of 10/20 amp SP MCB's arranged in 3 rows arranged in 3 tier one above other and controlled by 1 No. 63 amp TPN MCB and neutral link. Each row of MCB's shall be provided with 40 amp DP ELCB of 100 mA sensitivity.(All MCB to be "D" Curve)	Nos	3		
4	10 way TPN DB with 24 Nos of 10/20 amps SP MCB's i.e. 6 Nos. of 10/20 amp SP MCB's arranged in 3 rows arranged in 3 tier one above other and controlled by 1 No. 63 amp TPN MCB and neutral link. Each row of MCB's shall be provided with 40 amp DP ELCB of 100 mA sensitivity.	Nos	10		
5	6 way TPN DB with 18 Nos of 10/20 amps SP MCB's i.e.6 Nos. of 10/20/32 amp SP MCB's arranged in 3 rows arranged in 3 tier one above other and controlled by 1 No. 63 amp TPN MCB and neutral link. (All MCB shall be D curve)	Nos	10		
6	Sheet metal enclosed 12 way SPN DB with 8 Nos. 10/20 Amp SP MCB and controlled by 1 no. 40 Amp DP MCB with ELCB (100 mA) complete as required. For emergency lighting .	Nos	14		
7	Supply ,installation, testing and commissioning of earth pits comprising 600 x 600 x 3 mm. thick Copper	Nos.	6		



Sr. No.	Description	Unit	Qty.	Unit Rate	Amount
	electrode, 50 mm dia medium class GI pipe, GI funnel with 20 gauge GI wire mesh, masonry chamber with concrete base, CI manhole cover with frame (300 mm. x 300 mm.) painted with bitumastic paint, test link joint and alternate packing the mixture of Charcoal and salt around plate electrode, depth should not less than 3 meters, The thickness of earthing pipe should not be less than 2 mm complete as required ,as per specifications and as per IS: 3043				
j	Supply and fixing in position the following insulated wires including providing all fixing accessories and effecting proper connections.				
1	6 sq. mm. dia pvc insulated copper conductor wire.	RM	600		
k	Supplying, unloading, storing, laying, testing and commissioning of following sizes PVC insulated (Heavy duty) Copper conductor cables suitable for working voltage up to and including 1100 Volts, laid and tied on existing overhead cable trays; or laid and tied over MS supports in masonry trenches including providing MS supports and clamps for fixing to supports in an approved manner complete as required and as per specifications. Circuit identification tag should be attached with the concerned cable along with the test report of following sizes of cable to be submitted by the contractor at the time of delivery of material at site				
1	50 sq. mm. cable, armoured for earthing.	RM	500		
2	95 sq.mm. cable unarmoured for UPS	RM	400		
3	25 sq.mm. cable unarmoured for UPS	RM	300		
4	50 sq.mm. cable unarmoured for UPS	RM	200		
5	225 sq.mm cable for UPS distribution panel	RM	590		
l	Termination of the following sizes of PVC insulated Copper conductor cable including providing terminal lugs, single compression glands crimping the joints, providing insulation tape, effecting terminal connections to the equipment complete as required.				
1	50 sq. mm. cable, armoured for earthing.	Nos.	12		
2	95 sq.mm. cable unarmoured for UPS	Nos.	18		
3	70 sq.mm. cable unarmoured for UPS	Nos.	24		
4	50 sq.mm. cable unarmoured for UPS	Nos.	8		
5	225 sq.mm. cable for UPS distribution panel	Nos.	24		
m	Supplying, unloading, storing , laying, testing and commissioning of following sizes of XLPE insulated (Heavy duty) Aluminium/copper conductor armoured cables suitable for working voltage up to and including 1100 Volts , laid and tied on existing overhead cable trays; or laid and tied over MS supports in masonry				



Sr. No.	Description	Unit	Qty.	Unit Rate	Amount
	trenches including providing MS supports and clamps for fixing to supports in an approved manner complete as required and as per specifications.				
1	3.5 x 150 sq.mm. Aluminium Cable	RM	200		
2	3.5 x 70 sq.mm. Aluminium Cable	RM	R.O		
3	4 x 25 sq.mm. Al. Cable	RM	R.O		
4	4 x 16 sq.mm. copper Cable	RM	150		
5	4 x 10 sq.mm. copper Cable	RM	50		
6	4 x 6 sq.mm. copper Cable	RM	50		
7	2 x 10 sq.mm. copper Cable	RM	50		
8	2 x 6 sq.mm. copper Cable (For Dedicated earthing of DB's)	RM	100		
n	Termination of the following sizes of PVC insulated Aluminium conductor cable including providing terminal lugs, single compression gland , crimping the joints ,providing insulation tape, effecting terminal connections to the equipment complete as required				
1	3.5 x 150 sq.mm.Aluminium Cable	Nos.	50		
2	3.5 x 70 sq.mm.Aluminium Cable	Nos.	R.O		
3	4 x 25 sq.mm.Al.Cable	Nos.	R.O		
4	4 x 16 sq.mm.copper Cable	Nos.	6		
5	4 x 10 sq.mm. copper Cable	Nos.	80		
6	4 x 6 sq.mm. copper Cable	Nos.	40		
7	2 x 10 sq.mm. copper Cable	Nos.	40		
8	2 x 6 sq.mm. copper Cable (For Dedicated earthing and body earthing of DB's)	Nos.	40		
9	Supply, installation, testing and commissioning of Earth box made of 2mm thick MS painted ,with a glass cover and having 25 x 3 mm Cu strip with insulators complete as required.	Set	4		
o	Supply, laying in position & proper connection by welding/bolting or brazing for the following GI tape/wires including providing all fixing accessories and effecting proper connections.				
1	25 x 6 mm GI tape	RM	1400		
2	25 x 3 mm Cu tape	RM	600		
p	Supply and installation of following sizes of MS perforated type cable trays with stove enamel paint of approved colour and necessary bends, tees, reducer couplers, dash-fasteners, GI nuts bolts including cutting, bending, drilling, bolting required suspension arrangement fabricated from steel etc. complete as per specifications and as approved by Engineer - in - charge. The suspension of MS cable tray, only GI or SS				



Sr. No.	Description	Unit	Qty.	Unit Rate	Amount
	round rods with ceiling anchoring facility should be used.				
1	600 mm wide, 40 mm high (2 mm thick)	RM	220		
2	450 mm wide, 40 mm high (2 mm thick)	RM	400		
3	300 mm wide, 40 mm high (2 mm thick)	RM	300		
4	150mm wide, 40 mm high (2 mm thick)	RM	200		
5	450 mm wide, 100 mm high (Data Center)	RM	150		
0	FIXING OF LIGHTING FIXTURES.				
a-1	The rates for fixing of lighting fixtures shall include all fixing accessories that are required to make the installation complete in all respects including the following:-				
a-2	Providing connecting wires and channel support wherever required.				
a-3	Internal wiring between accessories.				
a-4	Self-interlocking connector blocks for connecting the wires from fixtures to the points.				
a-5	Earthing of fixtures with 1.5 sq. mm. PVC insulated copper conductor wire.				
a-6	Approved colour powder coated down rods, clamps and other components and fixing accessories wherever required.				
a-7	Testing of fixtures before Installation.				
a-8	Identification tags with a distance not more 3 meters to be use for circuit identification				
1	Receiving, fixing in position, effecting proper connections, testing and commissioning of PL lamp/Halogen lamp fixture fixed recessed in ceiling complete as required and with all accessories, along with providing PVC flexible conduit from junction box at slab level to fixture on the false ceiling.	Nos	120		
P	SUPPLY OF LIGHTING FIXTURES				
a-1	The fixtures shall be suitable for single phase, 50 cycles, 230 Volts, A.C. supply system.				
a-2	All fixtures shall be factory wired with copper conductor wires.				
a-3	All fixtures shall be supplied with Electronic ballasts, fluorescent lamps/bulbs, as specified.				
a-4	The rate shall be quoted for the Catalogue no. specified for the fixture however if contractor wants to supply equivalent then sample shall have to be got approved from Architect before procurement.				



Sr. No.	Description	Unit	Qty.	Unit Rate	Amount
a-5	All the samples shall be submitted within two weeks of the issue of work order, for approval from the Architect.				
a-6	Supply, unloading storing at site of the following fixtures with all accessories, such as spring loaded side holders, starters, power factor compensators, MS housing to house ballasts, complete with lamps. All the lamps shall be colour 84 or as approved.				
1	2x2 LED Light Fixture	Nos	120		
Q	CONSTRUCTION POWER AND LIGHTING				
1	Providing temporary construction lighting and power on the floor including by using required nos. 1 x 36 Watt phatic type fixtures (minimum 250 Lux), required flexible double insulated copper wiring, distribution board, minimum 3 nos. 400 W halogen flood light, earthing, main panel with incoming MCCB and required MCCB in the outgoing for distributing the power through the duration of the project. It will be the responsibility of Electrical Contractor to distribute power to all the contractors working at site. The rates shall be all inclusive. The material bought by the contractor shall be the property of the contractor and after the work is completed it can be taken back by him. (All item mentioned above, shall be new and of good quality by considering site safety parameter. Old and repaired item shall never be allowed to use at site.)	LS	1		
R	Networking				
a	Supply, Installation, Testing and commissioning of Data and Voice System. (4 Node Outlet at Each Location).				
1	Supply & fixing 24-port Loaded , Modular Jack Panel, 1U (For Data UTP Field Cables)	Each	32		
2	Cat-6 E UTP Cable .	RM	6000		
3	Supply & fixing Slime line RJ45 jack	Each	120		
4	4 - Port Face Plate	Each	30		
5	Cat-6 UTP Jack with Strain Relief	Each	120		
6	AMP Cat 6, UTP Mounting Cords for Data Rack End 4 Feet (Yellow)	no's	200		
7	AMP Cat 6, UTP Mounting Cords for Data Rack End 7 Feet (Yellow)	no's	200		
8	AMP Cat 6, UTP Mounting Cords for Data Server Rack Both end 7 Feet(RED)	no's	480		
S	ACS, FDS, WLDS, VESDA, RRS, BMS, PAS, NOVEC				
a	Access Control System				



Sr. No.	Description	Unit	Qty.	Unit Rate	Amount
1	Access Controller capable of controlling 4 doors and 4 reader	Nos	3		
2	Finger print reader with lock output.	Nos	7		
3	Power Supply	Nos	7		
4	Proximity Reader	Nos	7		
5	Proximity Card	Nos	100		
6	Electro Magnetic Lock (Single leaf door)	Nos	6		
7	Power Supply for Lock	Nos	6		
8	Magnetic Contact	Nos	6		
9	Exit Push Button	Nos	3		
10	Emergency Release Switch	Nos	3		
11	4 core x 0.75 Sq.mm shielded Cable in PVC conduit	Mtrs	400		
b	Fire Detection System				
1	Addressable Fire Alarm Panel	No	1		
2	Smoke detector	Nos.	30		
3	Heat detector	Nos.	6		
5	Manual Pull Station	Nos.	1		
6	Response Indicator	Nos.	6		
7	Sounder	Nos.	5		
8	Fire Exit Signage	Nos	10		
10	2 core x 1.5 sq.mm Armoured cable	Mtrs.	400		
11	Hand held fire extinguisher Co2 4.5 KG - ISI Approved	Nos	10		
c	Water Leak Detection System				
1	4 Zone Water Leak detection panel with battery. UL Approved	Nos.	1		
2	Water Leak detection module	Nos.	18		
3	Water leak detection cable sensor (15 Mtrs)	Nos.	10		
4	Electronic Hooter	Nos.	2		
5	2 core x 1.5 sq.mm Armoured cable	Mtrs	100		
d	VESDA				
1	Single Zone Laser Focus Detector - VLF 250	Nos	1		
2	Power Supply Unit for above Detector	Nos	1		
3	Aspiration Tubes	Mtrs	100		
4	Capillary Tubes	Nos.	6		
5	Air Termination Nozzles	Nos.	2		
6	Electronic Hooter	Nos.	1		
7	2 core x 1.5 sq.mm Armoured cable	Mtrs.	100		
e	Rodent Repellent System				
1	Master Console with 12 satellites	Set	6		
2	Wire Bundle	Lot	6		
3	PVC Conduit	Mtrs	100		
f	Building management System				
1	BMS GUI Software to monitor critical alarms	No	1		
2	Temperature & Humidity Sensor	Nos.	8		
3	4 core x 0.75 Sq.mm shielded Cable in PVC conduit	Mtrs	1200		



Sr. No.	Description	Unit	Qty.	Unit Rate	Amount
4	Communication cable in PVC Conduit	Mtrs	1200		
g	Public Address System				
1	PA System Lot	Lot	1		
h	NOVEC DATA CENTRE				
1	100 Litre cylinder with Valve / SITC of CCOE / NOVEC 1230 Cylinders 100 Ltrs.	Nos	8		
2	Novec 123 supply	kg	840		
3	Primary Completer Kit complete with Solenoid & Gauge Assembly, Discharge Tube, Manual Pneumatic Actuator, Flex Hoses, Warning Sign, Nameplate and Connectors.	Nos	1		
4	Discharge Nozzle	Nos	14		
5	Pressure Switch	Nos	1		
6	Cylinder strap, warning sign stickers	Lot	1		
7	M.S. Seamless pipes as per ASTM A 106 Gr. B, schedule 40 with necessary fittings.	Nos	1		
8	Hooter	Nos	1		
9	Manual Release Switch	Nos	1		
10	Abort Switch	Nos	1		
11	2 Zone Gas Release Panel	Lot	1		
12	Supply installation of Circuit Integrity Cable for fire suppression, power and Signalling.	Mtr	290		
13	Supply installation of Analogue Photoelectric Type Smoke Detector.	no's	14		
T	7th Floor strengthening for both arms				
	TOTAL OF DC NON-IT COMPONENTS				

(End of Chapter 3)



Chapter 4. : Specifications and allied Technical Details

4.1. Executive Summary

4.1.1. At a Glance- summarized scope for implementation

This project involves the convergence of multiple type of fields camera feeds to a common centralized point which is the Data Center. The DC is located at Police Headquarter, Delhi Police, Jai Singh Road, near Bangla Sahib Gurudwara, New Delhi 110001.

There will be Fixed Box, PTZ and ANPR cameras deployed across Delhi serving for the purpose of Women, Child and elderly people safety. The camera feeds will travel from source to destination through a multi-cast enabled MPLS cloud environment across all multi-cast enabled devices. The network backbone & last mile connectivity is the responsibility of the Internet Service Provider. All the District Head Quarters and Police Stations will communicate with the DC through a Hub-&-spoke model.

At the Data Center, Tier III provisions will be ensured with High Availability measures for IT and Non- IT associated components. The DC will be prepared with highly secured environment which will enable all Video Management algorithms facilitating and bridging all Video Analytics, Facial Recognition, ANPR outcomes to communicate with VMS clients located at all DHQs and Police Stations in the placed Work Stations.

The VMS will act as a central bridging point in between the Command & Control, Visualization layer (Video-wall and display screens) and the storage at DC with real time replication at near Data Recovery site.

The Video Analytics using AI and ML methodologies is the driving force behind the success of this project and the useful impacts of all the investments done in the envisaged project. The MSI is subjected to write and execute well considered SoPs and workflows of all the use-cases as desired to make this project a success. The implemented platform will be used to leverage video feeds from existing/ planned cameras in other schemes as well, henceforth all the data lake formulations and approach should be clearly defined considering scalable aspects.

The system will be integrated with the existing Government Data sets of various departments (32 No.) which will be coordinated with MSI for seamless integrations and outcome driven operations.

The project implementation has to be conducted in a time bound professional way so as to meet the desired results meeting all the outlined objectives with clear Aim and vision of the project by Delhi Police.

4.2. Aim, Objectives and Benefits of Delhi Safe City to be realized through MSI

The Scope of Work for the project as envisaged is focused on the following aspects:

4.2.1. Aim

The aim of this system is to capture all activities at the places under surveillance, generate alarms, warnings in case of any potential threat to women's safety, especially physical, targeting women, followed by real-time technology aided assistance to women in distress.

The broad aims to achieve through this envisaged project are:



- i. Enhanced surveillance and demonstrative presence / visibility in public places by installing CCTV cameras and deploying dedicated women's mobile police vans (Prakhar Vans) and Mobile Command Control Vehicle [MCCV].
- ii. A fast and efficient emergency response program, for assisting women in distress
- iii. Focus on ensuring rapid availability of professionally trained police personnel to address the needs of women in distress through the use of technology.

4.2.2. Objective

The objective of the proposed project is to:

- i. Ensure, through use of technology, prompt availability of professionally equipped police personnel to reach women in distress.
- ii. Increased and demonstrative presence/visibility in public places through installation of CCTV cameras in deployment of dedicated safety mobile Police Vans (Prakhar Vans).
- iii. Quick and effective response system to address the needs of women in distress.
- iv. 24x7 CCTV monitoring of public areas frequently visited by women and susceptible to female crime.
- v. Integration of location-based services and crime and criminal databases with CCTV feeds for prompt and effective resolution of women safety issues at public places.
- vi. Analysis of video and creation of actionable warnings/alerts for preventive and curative actions.

Following are the key objectives and intended outcomes, which have been kept in mind for women's safety:

i. Security and Safety- Quick and effective emergency response system

- a. Live surveillance and alerts in case of an incident through a network of cameras
- b. Greater coverage and surveillance of public places frequently used by women within the city, with more eyes on the streets
- c. Supporting operations to meet any contingency situation
- d. Prevention and detection of street crimes against women and apprehending offenders to deter criminal activities.

ii. Improved responsiveness

- a. Providing women with easy access to the police for quick and effective response, along with improved visibility, transparency and concern
- b. Improved response times and a general reduction of crime propensity in the area
- c. Improved response in case of women related distress situation
- d. Enhancement in prediction capability through AI based analytics, which will help in preventive and predictive measures
- e. Providing surveillance in areas having higher concentration of women residences based on Hot Spots, especially of students and working women (e.g. localities having



women hostels, paying guest accommodations, etc.)

- f. Identification of Areas prone to crime against women or crime targeting women such as snatching incidences, eve teasing etc.
- g. Identification of areas frequented by women, such as girls' Schools/Colleges, Market places, transport hubs, etc.
- h. Provide emergency service assistance to women in distress.

iii. Effective Policing

- a. Mitigating threats of crimes against women
- b. Assisting in the management and policing of large-scale events (gatherings like events and political/religious rallies) and putting a check on anti-social elements
- c. Assisting police investigation by integrating the analytical tools
- d. Assisting in preserving the electronic evidences for criminal and civil actions in the courts.

iv. Improved Management

- a. Decision making tool in maintaining law and order in the city
- b. Acting as a tool for Police and other government agencies in monitoring and maintaining their functions
- c. Providing a framework to all the stakeholders, so that there is proportionality and transparency in their use of surveillance
- d. Ensuring scalability and interoperability of systems

v. Reduction in crime

- a. A reduction in the number of complaints
- b. Helps to reduce fear of crime in the area and prevents crime by deterring criminal activity by detecting such activity and helping to identify and apprehend offenders, leading to their prosecution
- c. Reduction in number of cases or crime against women
- d. Under monitoring of camera the personal behavior changes so this will result in at least at those spots change in behavior that are under threat
- e. Reduction in the number of assaults on police officers
- f. Officer skill enhancement through the review of performance at incidents
- g. Reduction in officer time spent on paperwork with the help of search operation using AI platform

vi. Integrations and scalability

- a. Integration of various existing database CCTNS, Traffic e-challans, PCC, ERSS-112 etc. which help in training of data and implementing AI algorithm for women safety
- b. Identification of sensitive hot spots in the city



- c. Ensures scalability and interoperability of systems
- d. Integration of existing / proposed cameras of different CCTV projects of Delhi Police
- vii. Process Commissioning through ICT (Information and communication Technology)**
 - a. Installation of CCTV surveillance covering the priority hot spot areas
 - b. Automated number plate recognition i.e. ANPR to be deployed in extremely sensitive areas around hotspots of crime
 - c. Intensive patrolling in vulnerable areas beyond the identified hot spots
 - d. Provides greater coverage of surveillance within the city

viii. Skill enhancement

The system as envisaged, will enhance the skills of operations through ICT interventions, which will enable Police Personnel to effectively utilize technology to monitor and reduce crime and with efficiently achieving the objectives.

4.2.3. Intended Benefits

The benefits of the Safe City Project of Delhi Police are as follows:

- a. Increased and demonstrative presence/visibility in public places through installation of CCTV cameras
- b. Quick and effective response system to address the needs of women in distress.
- c. Increased public confidence in policing
- d. A reduction in the number of crimes against women and allegations against police officers
- e. De-escalation of anti-social behavior
- f. Ability to deploy BWV in areas not covered by other forms of CCTV
- g. Officer skill enhancement through the review of performance at incidents
- h. Integration of various existing database CCTNS, Traffic e-challans, PCC, ERSS-112 and etc. which help in training of data and implementing AI algorithm for women safety
- i. Identification of sensitive hot spots at regular intervals
- j. Installation of CCTV surveillance covering the hot spot
- k. Automated number plate recognition (ANPR) cameras to be deployed in selected areas
- l. Intensive patrolling in vulnerable areas beyond the identified hot spots
- m. Provides greater coverage of surveillance within the city
- n. Ensures scalability and interoperability of systems
- o. Acts as a crime deterrent in sensitive zones like procession routes and public gathering spots
- p. Assists the police in gaining evidential quality recording of incidents
- q. Helps in controlling incident escalations by providing improved response time.
- r. Helps to reduce fear of crime in the area and prevents crime by deterring criminal activity by detecting such activity and helping to identify and apprehend offenders, leading to their prosecution



4.3. Delhi Safe City- Targeted Impact & Outcome on Delhi Police and Citizens through successful Project Implementation by MSI

With the advance envisaged surveillance solution for Delhi, the number of eyes to monitor the crime incidents on field will increase substantially. The number of case detections are likely to increase with the rise in the number of cameras commissioned on ground. In such scenario the ICT driven system comprises of Intelligent and Smart systems like different Command & Control (C4i, C3i, C2i) platform, VNMS (Virtual Network Management System) layers, applications and interoperability, etc. will serve beneficial and impactful as follows:

- i. There will be an immediate assistance to the enquiry officer or investigating officer on ground from the C4i, C3i and C2i
- ii. Collaborative monitoring ensured a safe and secure environment for women safety
- iii. Video summarization with the photo image help the investigating officer to expertise the process of investigation.
- iv. Better situation alert generation in case of women related distress situation
- v. Increase in number of alerts generated for women specific areas
- vi. Reduction in response time by the law enforcement agencies to handle the situation or to track and identify criminals
- vii. Increased response (through system generated alerts) to women safety issues at public places.
- viii. Reduction in 'Response Time' of emergency response vehicles in respect of women related distress situations.
- ix. Improved prediction capability of any women safety related incident, leading to better preventive action, thus causing reduction in actual incidents involving women safety.
- x. The number of preventive actions taken against individuals with apprehension of participating in crime against women or crime targeting women

The desirable outcomes in safe city projects relate to increased comfort for women to move in public spaces with reduced threat perceptions. Critical outcomes of the Safe City projects, inter-alia include:

- i. Increase in approachability of women to police stations for counselling and reporting crime (as evidenced in footfalls)
- ii. Increase in confidence of women to visit public places (evidenced in increased footfalls), even in early mornings and late night
- iii. Reduction in crimes against women in cities
- iv. Reduction in response time by the law enforcement agencies to react to crisis or to track and identify criminals and safety audits by Third party agency at regular intervals.



4.4. Key components- Project Requirement & understanding for MSI

The Key components of the project are focused for the following prime purpose:

- i. 24x7 CCTV monitoring of public areas frequently visited by women and susceptible to female crime.
- ii. Integration of location-based services and crime and criminal databases with real time CCTV feeds for prompt and effective resolution of women safety issues at public places.
- iii. Analysis of real-time video and creation of actionable warnings/alerts for preventive and curative actions.

The following below are the components envisaged under the Scope of Work to be executed in order to meet the project objective and operational outcomes:

4.4.1. Cameras

Under the project approximately 10,000 CCTV cameras are to be installed. CCTV feed sharing with field units in real time: police patrol vans like Prakhar vans, emergency police station officers, beat patrolling personnel, emergency response vehicles, etc. involved in redressing women's safety-related situation of distress.

4.4.2. Other field devices

Beside camera there are other field devices such as the industrial grade Switches, OFC network, poles with cantilevers/ arms, junction boxes, Gun-shot detection system (200 No.) and Public Address System with loudspeaker (300 No.), etc. Also, there will be provision of 220 Mobile Hand-Held Devices for Police Officials to have dedicated interface with platform.

4.4.3. Data Center, near Data Recovery site & Integrated Command, Control, Communication & Compute (C4i)

The Data Center, near Data Recovery site and Command & Control is important component of this project. Multi-level command & control at Police Station (C2i), District Offices (C3i) and Police Headquarter (C4i) for successful information sharing, coordinating decision-making and implementation in order to resolve women's safety- related circumstances of distress promptly.

All police stations, district offices & headquarter will be connected to Data Center for viewing and retrieval of stored video footage as and when require. Data Center, which stores the entire lot of live streaming feeds and the triggered transactional data at one place. Provision for two Emergency Operation Centers (EOC) incorporated with C4i as a specialized command room for dealing with serious issues related to women's security in real time.

The Data Center has been envisaged at PHQ with all necessary hardware and software deployments to operate the system on real time basis, effectively and efficiently. A backup of flagged/ incident flagged / Incident stored data will be preserved in a nearby site termed as near Data Recovery site.

4.4.4. Databases Integration

Existing databases such as Traffic, Crime & Criminal related database e.g. CCTNS, e-challan system, VAAHAN, SARTHI etc. will be integrated in the proposed system for the real-time monitoring and tagging of suspicious persons and generating warnings.

The integration plugins of various external datasets which will communicate with our envisaged system will be regulated through a PIU exchange. All the data being bi-directionally shared among the applications (envisaged and any external) will be logged and indexed in the PIU along with all the triggers and meaningful structured data records will be managed by PIU for quick customized post analyses search modules. Also, the PIU exchange will enable



quick learning of the system to get matured based on the AI and ML methodologies defined and the catalogues of the data exchange with external are external datasets.

Integration of different Govt. Applications & Systems

The integration of Safe City platform with other existing applications will be an integral part of this project implementation. The integration will ensure optimum and best utilization of available databases to enable productive analyses.

There will be database integration of various other applications with the envisaged system for inter-operable effective actions of Delhi Police. The major applications for integrations with the envisaged system include:

- i. Emergency response support system integration (ERSS, dial 112) for real-time updates on emergencies focused on women's safety
- ii. Integration with Himmat Plus SOS mobile App. for real time inputs from women in distress. The inputs include location, auto-video of distress scene, etc.
- iii. Provision of aggregation of audio-visual feeds from specific ground sources – private / public IP-based CCTV devices, etc. mapped through the C4i on need basis.
- iv. Himmat Plus App caller's mobile camera feed and their real-time collaboration with on-site staff working to resolve a woman's distress in a public place
- v. ITMS feed
- vi. AFIS, e-Sarthi, eVaahan and e-Beat Book
- vii. Provision for Integration of other CCTV Surveillance cameras installed/proposed in other projects of Delhi Police

Integration of existing or other camera feeds into the system

This layer also incorporates the integration of existing or any other CCTV cameras for either viewing/ analytics at C4i. For the integration activity, edge gateways (2 No. at each District or more as per the requirement at Police Stations based on the existing viewing and storage facilities) have been provisioned which will interface with the existing NVRs at Police Stations recording old IP cameras feed and integrate them with the envisaged system.

It must be noted in order to use video streams and operate analytics on the existing cameras' feed, the regular camera feeds from newly envisaged Safe City Cameras will be dropped momentarily. There will be no provision of additional hardware and licenses at the Data Centre for parallel viewing of camera feeds under different schemes. Same methodology for any other department will be adopted which is required to use the envisaged platform.

Considering this aforementioned methodology for integration of cameras from other departments, 800 cameras from NDMC will be covered as PILOT integration. Based on the successful results through integration of these cameras, feasibility of integration of cameras from other departments/ projects like IGI Airport, Railways, Metro, etc. will be examined and incorporated.



4.4.5. AI, ML & Video Analytics Tools

The Video Analytics shall be based upon Machine Learning and Deep Learning framework. Facial recognition system, Automatic Number Plate Recognition, Video Analytics such as People detection, vehicular analytics etc. with specific time-stamped video feeds recorded by CCTV cameras in public places for real-time identification of crime & criminal details.

The outcomes derived from the Analytical Platform and the related structured data along with the datasets and application data handshake with other existing Government Applications will create a data lake/ container which will facilitate effective and considered outcomes of analyses on the metadata fields. Also, to facilitate big data analyses with other applications the learning platform will bring more efficiency as the system get matured.

4.4.6. Video Management & Facial Recognition System

A VMS has to be provisioned at Data Center which will work with the ICCV platform and coordinate with the available agents at C3i and C2i for bringing every captured feed from cameras into a visual layer for the use of police Personnel.

Facial recognition system, analytic applications for people, object and vehicle detection with automatic number plate readers have been provisioned with specific time-stamped video feeds recorded by CCTV cameras in public places for real-time identification of crime & criminal details.

Video analytic tool and other applications like FRS, ANPR will be installed centrally at Data Center to work upon the camera feeds. This will help Police officials to conduct customized result-oriented analytics related to people and vehicles related to different attributes, facial recognition measures, etc.

4.4.7. Mobile Command Control Vehicle (MCCV) & Prakhar Vans

There will be 2 Mobile Command Control vehicles equipped with all hardware and software feature and interface with C4i to take immediate actions on field as per the inputs received from field level cameras.

Also, there are 88 Prakhar vans across NCT, Delhi which will be operating under SOP are interfaced on MDT to handle all concerns regarding women and elderly people. The SOP regarding this will be defined by Delhi Police.

4.4.8. Cyber Security

Project comprised of a highly complex, interdependent network of devices, systems, platforms etc., which leads to cyberattacks on critical infrastructure, firewall, Intrusion Detection & Prevention, Anti-Virus, Network Traffic Analyzer (NTA), Behavioral Analysis & Anomaly Detection Tool, and End Point Detection etc. are an essential component for Cyber Security.

4.4.9. GIS Maps

The Map view is a fully functional GIS view of the facility. It provides functionality to allow the security operator to manage the view of the facility in order to provide better situational awareness during an incident.

The GIS maps will be created using various useful layers like camera positioning, nearby building structures, hotspots based on criminal activity trend, etc. GIS maps incorporating layers of utilities and resources across Delhi will help in accurate decision making by



implementing and operationalizing the envisaged project in coordination with other departments, urban local bodies, etc.

4.4.10. Network Backbone

Network Connectivity is one of the most important components of the project. All Police Stations and District Offices will be connected to Data Center for viewing and retrieval of stored video footage as and when require for evidence, based on their right. Using IP/MPLS connectivity from an Internet Service Provider with required redundancy and symmetrical bandwidth, the cameras will be connected to the system through a wired network. The video feeds from the cameras will be transported via secured IP / MPLS / Fiber Optic network to the respective Police Stations, District Offices, Data Center and Command & Control Center.

There are two Network Setup

Internal & External – Responsibility of MSI – The cable laying from Junction Box to Camera, the multi cast enabled network setup from camera to Servers, Storage through all security devices and connecting entire IT infrastructure under defined SLA, monitoring and maintaining the entire network and delivering the required desired network performance

External – Last Mile connectivity – Providing multi cast enabled MPLS network till Junction Boxes and connecting all the Police stations (C2i), District Police Head Quarters (C3i), Police Head quarter (C4i), Near DR & DC through MPLS network and providing required bandwidth under defined SLA and providing Internet facility for connecting multiple databases running at different locations at Delhi.

C-DAC/Delhi Police will provide necessary details/documents and would undertake to provide assistance, to the extent of writing letters to concerned agencies, for getting necessary approvals from civic agencies for various schemes both prior to execution and after completion. However, MSI, ISP, Vendor, etc. will be responsible to apply for approvals/permissions from civic agencies, pursue and completing of all formalities with such civic agencies

4.4.11. Type of components:

The proposed solution will offer Delhi Police the flexibility to adopt new technology to meet evolving operational requirements, including real-time decision-making and networked Command & Control. This include:

- a. Cameras & Sensors
 - i. Outdoor CCTV Surveillance Cameras – Fixed and PTZ
 - ii. Automatic Number plate recognition Camera – ANPR
 - iii. Camera mounted Two Mobile Command Control Vehicle
 - iv. Mobile phone / App based Surveillance
 - v. Community Camera feeds on need basis
 - vi. Prakhar Vans fitted with roof top mounted cameras
 - vii. Other sensors – Gun shot detection, etc.
- b. Network Layer
 - i. Network Back Bone Infrastructure – MPLS, Switching, Routing Fiber Backbone
 - ii. Last Mile Connectivity – OFC, 4G / 5G



- c. Enterprise Computing
 - i. Servers
 - ii. Storage and Back up
 - iii. Virtualization
 - iv. Other IT components
 - v. Load Balancer, Firewall, L3 switches
- d. Application Portfolio
 - i. Integrated Command & Control Center –ICCC
 - ii. Video Management System (VMS)
 - iii. Mobile Command Control Vehicle
 - iv. GIS
 - v. Video Analytics and Social Analytics
 - vi. Picture Intelligence Unit (PIU)

4.5. Implementation Approach- Essential & Planned approach by MSI

There will be four phases in our implementation approach. 06 Dist. needs to be completed in first phase within 09 months of awarding the contract / issuing the LOI; whereas it has been decided to prepare 02 districts as a pilot phase of the project within 5 months of awarding the contract to MSI; and another 4 Districts implementation will be completed in phase two within 11 months & last 6 Districts will be completed in 14 Months respectively from the day of awarding the contract. The documentation and completion certificate will be completed before or at the time of Go-Live of entire project. Phase four will Operation and maintenance phase, which will be of three years duration, and it will start after project Go-live.

Two districts out of Phase I (in coordination among MSI and ISP) will be implemented on priority to ensure PILOT execution. The timeline for the PILOT will be 4.5 months from the contract signing.

There will be four phases in our implementation approach. 06 Dist. needs to be completed in first phase (Phase –I) within 09 months of awarding the contract / issuing the LOI; whereas it has been decided to prepare 02 districts as a pilot phase of the project within 5 months of awarding the contract to MSI; and another 4 Districts implementation will be completed in phase two (Phase-II) within 11 months & last 6 Districts will be completed in 14 Months respectively from the day of awarding the contract. The documentation and completion certificate will be completed before or at the time of Go-Live of entire project. Phase four will Operation and maintenance phase, which will be of three years duration, and it will start after project Go-live.

Two districts out of Phase I (in coordination among MSI and ISP) will be implemented on priority to ensure PILOT execution. The timeline for the PILOT will be 4.5 months from the contract signing.

The details of complete project is envisaged to be completed in four phases as given below.

Phase 1 includes 06 Districts of Delhi covering 75 Police Stations (C2I) and 1360 Locations. The Go Live of Phase 1 would be in 09 months. This would also involve ‘as-is assessment’ and the Blueprinting of a Data Centre, Integrated Command, Control, Communication & Compute center (C4I) at Police HQ, Command, Control & Communication (C3I) at District Head Quarter and Command & Control center(C2I) at Police Stations along with respective IT and Non IT



Infrastructure including installation and commissioning of the Filed devices. Phase1 includes the procurement of 1 MCCV & also Integration of 32 existing Databases.

Phase 2 shall cover additional 04 districts with 45 Police Stations (C2I) with 836 Locations. The Go Live of Phase 2 would be in 11 months from Kick-Off Date. This would involve commissioning of near Disaster Recovery Center (nDR), Command, Control & Communication (C3I) at District Head Quarter and Command & Control center(C2I) at Police Stations along with respective IT and Non IT Infrastructure including installation and commissioning of the Filed devices. Phase 2 includes the second MCCV procurement.

Phase 3 shall cover additional 06 districts with 62 Police Stations (C2I) and 1155 Locations. The Go Live of Phase 3 would be in 14 months from Kick-Off Date. This would involve commissioning of Command, Control & Communication (C3I) at District Head Quarter and Command & Control center(C2I) at Police Stations along with respective IT and Non IT Infrastructure including installation and commissioning of the Filed devices.

Phase 2 and Phase 3 will be running concurrently, so that the whole project should be completed in the given timeline.

Phase 4 Warranty and Operation and Maintenance Phase: The bidder shall carry out the operation and maintenance services towards the implemented system for the period of 3 years. The Warranty (5 years) and the O & M (3 years) will run in parallel.

The following districts and the Data Centre setup are the priority requirements of Delhi Police to be implemented first during phase I:

1. East
2. North
3. North-West
4. South
5. South West
6. West

Following 04 district and its Police stations along with nDR have been covered in Phase-2

1. Dwarka
2. Rohini
3. New Delhi
4. South East

Following 06 district and its Police stations have been covered in Phase-3

1. Central
2. North-East
3. Outer
4. Outer North
5. Railway
6. Shahdara



Phase- 4 will be Operation & Maintenance Phase which will start after Go Live of all the phases.

The Data Centre setup with all the civil part (non-IT) and establishment of compute, security and network layer will be conducted for full completion from day one of the commencement of implementation activities, except the progressive elements as per phase-wise need basis, which includes:

1. Placing servers inside the rack chassis.
2. Installation of ToR switches.
3. Passive cabling and infrastructure management at DC
4. Installation and commissioning of Field Network layer and progressive aggregation of throughput at DC
5. Procurement of software licenses based on phase wise progress and requirement as per district-wise cumulative load.
6. Installation of equipment and commissioning of nDRC in the tailing stage.
7. MSI has to strictly follow CIS guidelines to deploy Data center system's, all command controls and field devices etc. with CIS level-1 benchmarking while go-live & First security audit conduction is whichever is expected. All policy methodology has to be design and approved from C-DAC and followed from day-1.

CIS Hardened Images (for all operating systems has to be followed while installations for windows and Linux flavour's) can be used to securely configured virtual machine images or Host OS based on CIS Benchmarks hardened to either a Level 1 at the beginning of project execution and Level 2 CIS benchmark after deployment of all the application's if required by security audit.

The implementation in a staggered approach will realize a substantial saving on the warranty terms associated with every hardware and software element of the project requirement.

4.5.1. MSI's key responsibilities under the Scope of Work

The summary of MSI responsibilities is as follows:

- **Initiation and Planning for each Phase**
 - a. Define Project Implementation Plan as per phased approach.
 - b. Conducting site survey, obtaining necessary permissions, developing system requirements, standard operating procedures, etc.
 - c. Finalization of exact locations of the Cameras, Junction Boxes, Pole, Power Metres at different junctions
 - d. Finalization and submission of a detailed scalable & secured technical architecture and submission of detailed project plan which includes
 - Deployment of the Team, Project Manager, Their Roles & Responsibility
 - Responsibility Matrix of the stakeholders



- Approach & Methodology to be adopted
- e. Risk & Its mitigation
- f. Detailed project Plan, Specifying dependencies between various projects activities/Sub activities, Coordination with Civic agencies, & The timeline of the project
- g. Quality Management plan
- h. Communication Plan
- i. Stakeholder management plan
- j. Finalize the detailed Technical Architecture in coordination with ISP, Coordination & Execution Plan for seamless Integration
- k. Design the LAN connectivity diagrams for 3351 Locations from each Junction Box to Pole, From Power Meter to Junction Box & Prepare the Implementation plan in coordination with ISP
- l. Design the Architecture, Concept of Operations for C4i, C3i, C2i & Datacenter and prepare the 3D Diagrams, DC Floor Strengthening Plan
- m. Assessment of IT Infrastructure and Non-IT Infrastructure requirements, assessment of business processes, assessment of software requirements, assessment of integration requirements, assessment of connectivity requirement all locations (including buildings).
- n. MSI will adopt latest finishing items and construction materials so that better finish and quality is achieved at reasonable cost.
- o. Formulation of solution architecture, detailed design of Women Centric safe city solutions, development of test cases (Unit, System Integration and User Acceptance), SoP documentation
- p. Finalization of Bill of Material for the Tier 3 Datacenter, Near DR, C4i, C3i, C2i for designing & Building
- q. Finalization of Bill of Material of Cameras, UPS, Field Switches, PA system, Gun Shot Solution, Mobile Devices etc.
- r. Finalization of Bill of Material of Application Softwares
- s. Prepare the Approach & Methodology document for Integration
 - Datacenter Equipment/Hardware Integration
 - Near DR Equipment/Hardware Integration
 - C4i Equipment Integration
 - C3i Equipment Integration
 - C2i Equipment Integration
 - Field Equipment Integration
 - Field Equipment to C4i, C3i & C2i Integration (Hardware Integration)
 - New Application Software Integration



- Existing Database Integration
- Overall Application Integration & Installation
- GIS, CAD Integration
- AVLS Integration
- t. Plan to Integrate Community Surveillance & Existing Cameras in other projects
- u. SMS Gateway Integration & other Mobile app Integration
- v. Inventory management for all items/ equipment, software, licenses, Warranty, CAMC Certificates, etc.
- w. MSI will define the formats for data exchange between various services and systems in agreement with TSP (C-DAC).
- x. MSI shall ensure that system confirms technical specifications, however, equipment/items of better version may be acceptable.
- y. Any other, meeting the RFP requirement.

- **Implementation**

- a. Phase-wise time bound procurement and implementation. The phase-wise implementation schedule and targets are mentioned in para 5.1 of this chapter of the RFP.
- b. Obtain all necessary Legal/Statutory Clearance for Installing Poles & Junction Boxes
- c. Provisioning for Electricity
- d. Develop, Deploy, Test & Commission the surveillance system
- e. Supply, Install & Configure all User Level Components (Active & Passive)
- f. Installation of DC, Near DR IT Infrastructure
- g. Supply & Installation of MCCV
- h. Installation of Video wall, Workstations, LEDs, UPS, TV at C4i, C3i, C2i, DC and NOC
- i. Project Implementation & Phase wise Planning
- j. Physical Setup of ICCV as per the layout approved by Delhi Police.
- k. Helpdesk setup, procurement of equipment, edge devices, COTS software (if any), licenses. Physical Security and Housekeeping setup
- l. IT and Non-IT Infrastructure installation, development, testing and production environment setup
- m. Safety and security of IT and Non-IT Infrastructure
- n. Establishment and configuration of Network Connectivity in coordination with ISP (provided by service provider) as per service level between PHQ (C4I), 16 DHQ (C3I), 182 Police Stations (C2I), Near DR and various other applications for integration.



- o. Software Application customization (if any), development of bespoke solution (if any), data migration, integration with third party services/application (if any) User Manuals, training curriculum and training materials Role-based training(s)
- p. Preparation of Standard Operating Procedures (SOPs) for operation of the system and to ensure implementation/ operation of the system as per SOPs
- q. SOP preparation in consultation with C-DAC, implementation, Integration with GIS Platform, Integration of solutions with Command and Control Center, KPI Development. SOP needs to be approved by Delhi Police.
- r. Information Security Policy, Backup Policies
- s. Portal to monitor project activities.
- t. Training to Police Officials
- u. Testing Phase
 - Unit & Integration Testing
 - End to End Testing
 - Regression Benchmarking Testing
 - User Acceptance Testing
- v. UAT and Phase Wise Go-Live
- w. Final Acceptance Test & GO Live
- x. Submission of System Documents, User Documents
 - Project Commencement Documentation
 - Equipment Manual
 - Training Manual
 - Installation Manual
 - User Manual
 - System Manual
 - Standard Operational Procedure (SOP) Manual
- y. Testing Phase
 - Unit & Integration Testing
 - End to End Testing
 - User Acceptance Testing
 - Roll Out
- z. Facilitating UAT and conducting the prelaunch security audit of applications.
- aa. Integration of the various services & solution with ICCC platform Develop provisions for a scalable system



- bb. MSI shall furnish a progress report periodically (monthly) of project activities etc. indicating date of start, date of completion and progress made till the date of report (approximate percentage of work done).
- cc. MSI will ensure that safety code, as per applicable laws, including health and sanitary arrangement for the deployed staff/personnel, has been complied with.
- dd. MSI shall maintain a site order book and inspection book containing the details of orders issued at site and their compliance. The same shall be opened for checking by TSP or any agency authorized by Delhi Police or Delhi Police itself.
- ee. Any other, meeting the RFP requirement.
- ff. Responsibility towards ISP work handshake:
 - Marking of the final pole locations at the junctions
 - Power availability & MCB 16amp on junction box for ISP's network devices
 - Power meter & power cable availability
 - Providing Multiple switch strip inside the junction Box
 - Outdoor IP65/66/67 junction box with 5 years warranty and support
 - Making of platform for the pole and pole installation
 - Approval of designs from customer and civic bodies
 - Space inside the junction box with the gap of 1U between the devices.
 - Hot air exhaust and cooling system inside the junction box
 - MSI should design the junction box to block the dust & External Particles
 - Regular preventive maintenance of the junction boxes which involves maintenance of basic hygiene
 - Chemical earthing availability and maintenance
 - UPS power with 1 hour battery backup for all installed devices
 - Connectivity between camera and switch
 - Connectivity between switch & MUX/router
 - Providing High security lock system in junction boxes to ensure the safety and security of the devices
 - Installing Junction boxes at a minimum height of 6 feet above the ground
 - Ladder to install the mux in junction box
 - Lightning arrester with GI strip
 - Providing access for the ISP team at each junction/pole & DC/DR location
 - Supporting and coordinating with the ISP in facilitating ROW/Digging and network extension
 - permissions from different authorities



- CPE device configuration
- Warning signboards at each junction point
- Acrylic Board mentioning this area in surveillance
- Cross connect availability in DC & DR locations and other if applicable
- Integration of CE and ISP devices
- Providing safety & security at the junction locations
- Ensuring no access to trespasser or any other than the authorized person at the junction
- locations
- Providing cable conduit with in junction box
- First Level Troubleshooting needs to be done by the MSI engineer
- Electrician if required at all locations must be arranged by the MSI.

4.5.2. Post Implementation (Operation & Maintenance)

- a. Deploying manpower Security of ICCV premises Annual technical support
- b. Preventive, repair maintenance and replacement of hardware and software components
- c. Provide a centralized Help Desk and Incident Management Support till the end of contractual period Recurring refresher trainings for the users and Change Management activities
- d. Provide required access and information for Audits
- e. Preventive, repair maintenance and replacement of non-ICT components
- f. Overall maintenance of the ICCV facility and continuity of operations as per SLAs.
- g. Monitoring of Network Connectivity (provided by service provider) as per service level and report the non- compliance.
- h. Submit Quarterly Reports
- i. Adhere to defined SLAs
- j. Any other, meeting the RFP requirement.
- k. Setting up the Help Desk for O&M
- l. Manpower Deployment for O&M Phase
- m. Preparing the Document and Reporting Mechanism
- n. Completing the documentation of Warranty, License & Agreement
- o. Pent scanning & Network Dressing & Internal Audit
- p. Third Party Administrator (TPA)
- q. Security & Network Audit - Format & SOPs



- r. Helpdesk Management
- s. Reporting & Dashboards
- t. SLA Management - ISP & MSI
- u. Setting up Governance Team
- v. Exit Management
- w. Closure of the contract

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

- **Support and warranty:**

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

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

- **Standards of Performance**

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

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

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



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

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

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

Key Personnel shift to Scope of Requirement

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

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

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

b. Evaluations of Personnel

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

c. Replacement

In case any proposed resource resigns, then the Bidder has to inform C-DAC within one week of such resignation.

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

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

- a resume, curriculum vitae and any other information about the candidate that is reasonably requested by C-DAC; and
- An opportunity to interview the candidate.

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



If C-DAC objects to the appointment, Bidder shall not assign the individual to that position and shall seek an alternative candidate in accordance with the resource requirements of this RFP.

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

d. High Attrition causing adverse impacts to Project flow

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

- e. Provide C-DAC with a reasonably detailed explanation as to the reasons for such change, including, where applicable and permitted, notes from any exit interviews conducted by Bidder with any departing member of the Key Personnel; and
- f. If such change to Key Personnel has or is likely to have any material adverse impact on the provision of the Services or any substantial part thereof, undertake, at its own costs, such remediation acts as are reasonably necessary in order to improve the retention of the Key Personnel including making reasonable changes to the human resources policies and procedures applicable to the Key Personnel (including those related to compensation, benefits and other conditions so that they are competitive with the market) as may be necessary to ensure that such policies and procedures comply with Good Industry Practice.

- **Compliance with labour regulations**

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

- **Operation Power charges**

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



- **Important milestones**

- a. Planning & Implementation

The MSI is responsible for the entire execution of the project as per the defined terms, conditions, Scope of Work in the RFP.

- b. Commissioning (phase-wise)

The implementation will be conducted and executed in a phase-wise manner as per the aforementioned clause. Henceforth, it is pertinent to note that every phase has to be commissioned progressively till the completion of the entire scope of implementation. The MSI is purely responsible to adhere to the timelines in fulfilling the purposeful phased approach. All the co-ordinations with the stakeholders, civic agencies, ISP, Project Management Consultant, etc. has to be established effectively so as to drive the time bound commissioning as a key and responsible stakeholder of the project portfolio.

- c. Go-Live

The cumulative and collective commissioning of the phases along with the successful final User Acceptance and Final Level Testing done by the end customer, will mark the project as live and operation for public services, as envisaged. This stage will be called as Go-live milestone of the project.

- d. Operations & Maintenance

The selected MSI shall be responsible to operate and maintain the provided solution for the envisaged requirement of Delhi Police. The detailed responsibilities of MSI towards O&M activity are given at para 2.2.28 chapter-2 of this document.

During the O&M phase, MSI has to deploy following key personnel for fulfilling the essential requirement of minimum Technical Manpower in working shifts:

- a. Manager - DC, C4I, C3I and C2I- 1 No.
- b. C4I Expert- 2 No.
- c. System Administrator- 6 No.
- d. Network and Security Manager along with Field Network Technician- 10 No.
- e. Storage Administrator- 4 No.
- f. Enterprise & Asset Manager- 2 No.
- g. Database Administrator- 1 No.

4.6. Physical Layouts of Civil Infrastructure Areas with essential components as envisaged

The below mentioned details are the essential parameters to help visualize the envisaged outcome. The details of the estimated and required quantities to execute the work can be seen in the SoR chapter 3 of the RFP.



4.6.1. C4i (Integrated Command, Control, Communication & Compute) at PHQ

C4i at PHQ 6th and 7th Floor (with DC)

- i. C4i will act as Central Viewing station from where around 10% of 10000 cameras can be monitored by 21 Operators and 1 supervisor sequentially. The operators will view and analyses the alerts, Also, C4i will have two Emergency Operation Centers where these alerts will be managed and controlled by Police Officers.
- ii. The Video wall will comprise of 70" DLP Laser 4K technology
- iii. 16 Workstations are also installed for viewing cameras sequentially at Video wall. Applications from Data Center like VMS client, GIS, ICCC client, video wall controller software, Edge gateway integration, Unified Platform etc. will be deployed on workstations which will be placed behind Video wall, one workstation will be having 3 outputs (VGA/HDMI/DVI) which will connect to 3 inputs of video wall controller. Accordingly, there will be 16 number of workstations with 3 outputs each. So, total 48 outputs of workstations will connect to 48 inputs (VGA/HDMI/DVI) of video wall controller inputs and can be centrally managed by operator at C4i.
- iv. There will be 4 TV installed with stand; The TV will be placed in pair next to Video-wall at both the sides to view news.
- v. The array pattern of the modules will be 3 sets adjacent to each other as depicted in the enclosed layout of C4i. Hence, total DLP modules to be installed will be 48 no.
- vi. 04 Video Wall Controllers will be used, One Controller for 15 nos. 70" display units/modules.
- vii. 2 sets of LED Monitor- 55" cubes in a 1 X 2 arrangement to be installed Conference Rooms on 06th floor and 7th floor
- viii. 21 Workstations with 3 nos. 24" UHD Touch Monitors for C4I application will be used, – on 6th Floor
- ix. All Enterprise hardware, software and analytics applications will be deployed at C4i and agents will be running at DHQ, Police Stations, Prakhari Vans & MCCV. Apart from this, we also have provisioned to integrate 32 Datasets of different existing applications of Delhi Police. Databases will be integrated at PHQ through open standard API / SDK based approach. We also have provisioned integration of Community Surveillance system on need basis and other CCTV projects of Delhi Police.
- x. C4i will be designed on an acoustic framework with State-of Art facilities.
- xi. It will be equipped with essential audio and voice recording and communication mediums like IP phones, wireless, Rex Phones, automatic voice loggers with SMS gateway services, etc.

- xii. The ceiling fire door and floor drawings of C4i arena at 6th and 7th floors with DC (at 7th floor) will be shared post the signing of the Non- Disclosure agreement with MSI.
- xiii. C4i Design and Standards with the compliance sheet are detailed in section 4.8.15 of Chapter 4 of this RFP.
- xiv. The details of the location and coordinates of the sites will be shared post the signing of the Non- Disclosure agreement with MSI.
- xv. Video-wall for Integrated Command & Control Operations at C4i in PHQ.



Figure: Indicative Video Wall Layout at PHQ (C4I)- 4*4 array (3 No.)

4.6.2. C3i for DHQs (at 16 locations)

There will be District Command & Control Centers located at 16 different locations across Delhi covering all Districts:

- i. The C3i will comprise of 55" LED monitor screen that will be arranged in 1*3 array pattern along with Workstations to Display LED Monitor Wall inputs.
- ii. 16 locations of C3i will have workstations each with 3 Nos. of Monitors (24") for C4i application as per the requirement to ensure 10% viewing at a moment. The total quantity of Workstations and LED screen is indicated as follows:



Phase	NAME OF DISTRICT	LED TV at C3i	Workstation for LED TV at C3i	WS at C3i- (Keeping the monitoring of Police Station approach, WS are considered at C3i level)
Phase I	East	3	1	4
	North	3	1	2
	North-West	3	1	4
	South	3	1	5
	South West	3	1	4
	West	3	1	5
Phase II	New Delhi	3	1	1
	Rohini	3	1	4
	Dwarka	3	1	4
	South East	3	1	5
Phase III	North-East	3	1	4
	Outer	3	1	4
	Outer North	3	1	3
	Railway	3	1	1
	Shahdara	3	1	4
	Central	3	1	3
Total		48	16	57

- iii. 16 number of SD-WAN router, 1 at each DHQ for Load balancing, Traffic prioritization, ease of manageability, better monitoring and troubleshooting of all the locations.
- iv. 10 KVA UPS with 30 Mins. Battery backup at 80% load, 2 AC's of 1.5/ 2-ton capacity in HA (round and robin) at each C3i etc.
- v. Each C3i DHQ will be provided with 1 Network Colour Laser Printer.
- vi. C3i Electrical and Lighting fixtures' layouts will be shared post the signing of the Non- Disclosure agreement with MSI.

vii. Video Wall at DHQs (uniform- illustration):



Figure: Video Wall & Work Station- Depiction at DHQ

4.6.3. C2i (182 locations- Police Stations)

Police Station located at 182 different locations (as given in Table 3):

- i. 182 locations of C2i will have respective workstations with set of 3 nos. 24" UHD Monitors for C4I application, workstations at each C2I (Police Station). Total of 258 workstations are spread across all Police Stations based upon the quantity of camera feeds per Station.
- ii. The following table shows the number of work stations and display screen (55") at Police Stations:

Sr. No.	Number of Police Stations	Workstations Required	No of Workstation Required
A	With 30% Viewing (Uniform View)		
1.	137 Police Station	1 Workstation	137 Nos
2.	37 Police Station	2 Workstations	74 Nos
3.	4 Police Stations	3 Workstations	12 Nos
4.	2 Police Station	4 Workstations	8 Nos
5.	1 Police Station	6 Workstation	6 Nos
B	With 100% Viewing		

1.	Kamala market Police station	3 Workstations	3 Nos
2.	Total Workstation		240

70 out of 182 Police Stations will be equipped with 55" LED screen (59 PS with 1 LED screen and 11 PS with 2 LED screen). The screens will be allocated to the Police Stations depending upon the no. of cameras (less than 50- no LED screen, equal and greater than 50 till 99- 1 LED screen, equal and more than 100- 2 LED screens) at the respective station as mentioned in the above table.

- 182 number of SD-WAN router for Load balancing, Traffic prioritization, routing, ease of manageability, better monitoring and troubleshooting of all the locations.
- SD-WAN router considering Minimum 500 Mbps throughput with scalability etc.
- 3KVA UPS (174 Nos) and 10 KVA UPS (08 Nos) with 30 min battery backup at 80% load, 1 AC of 1.5/2 ton capacity at each C2i
- Each Police Station will be provided with 1 Network Black & White Printer.
- The Police station is monitoring old/existing CCTV's as well as new CCTV's and the future viewing shall be adequately provisioned in scalable and modular fashion. Existing/Proposed project viewing will be available on need basis.
- Workstations layout at 182 police stations (C2i)

4.7. System Functional Requirements and Key Performance Indicators

4.7.1. Essential System Functional Requirements at various layers:

With a view of enabling varied and respective stakeholders to operate specified Safe City Project Components, it is proposed to create multiple Viewing Centers for various surveillance cameras installed across the city which will cater City Surveillance and Helpdesk in an integrated manner. The architecture of the complete network of smart elements is as follows:



Figure: Control Room C2I – Single Seating Workstation



- i. **Street IT Infrastructure Layer** –The sensor layer will help Delhi Police to gather information about events and incidents happening in Delhi or capture information from the edge level devices i.e. cameras.
- ii. **Network Layer** –The secured network layer will serve as the backbone for the project and provide connectivity to gather data from cameras and communicate video feeds to viewing centers as well as Data Center for further analytics.
- iii. **Data Center Layer** – The Data Center layer will house centralized computing power required to store, process and analyse the data to decipher actionable information. This layer includes servers, storage, ancillary network equipment elements, security devices and corresponding management tools. A disaster recovery site, which includes minimal capacity of servers, storage, network equipment and security management systems will be used to store all flagged data. If Data Center stopped functioning for some reason in that case flagged data will be safe and can be recovered at any moment.
- iv. **Application Layer**- The applications layer will include applications like Integrated Command & Control Center software, Video Management Software etc. that will be used to view camera feeds at viewing centers using secured mechanism and alerts can be generated and communicated to all the Command & Control centers through Data Center, ICCC application / enterprise management system to monitor and manage all IT infrastructure and field devices deployed in Delhi.
- v. **Integration Layer** –While aspects of ambient and monochrome conditions within the Delhi will be gathered through various cameras deployed as a part of the solution, some data will come from other government and non-government agencies. It is through the integration layer – that data will be exchanged to and from the underlying architecture components and other data from system developed by government (such as CCTNS, ITMS, Challan database, etc.) and non-government agencies.
- vi. **Command, Control, Center Layer** – The command center will enable citizens and administrators alike to get a holistic view of city conditions, and make informed decisions.
- vii. **Security Layer** –As ambient conditions, all field devices are now connected through a network, security of the entire system becomes of paramount significance and the system integrator will have to provide: Infrastructure security, Network security, Identity and Access Management, and Application security.

4.7.2. Essential & Key Performance Indicators of the envisaged system

Key performance indicators for safe cities. This deliverable also explores the issues, challenges and developments of key performance indicators (KPIs) for safe cities. From the existing sets of city indicators present in many standards and projects, indicators for evaluating safe city performance, building on the current ISO programmed, are proposed in this document.

The evaluation framework should contain quantifiable and measurable outcome indicators. There is a need to measure performance not only by cities themselves; Key Performance Indicators may be used by different stakeholders of the safe sustainable cities and communities such as:



- **No of additional CCTVs installed** – It will increase the number of alerts generated for specific cases
- **Uptime of surveillance system**– The implementation of CCTV cameras with UPS for 60 Mins backup and 128 Gb SD Card which will have 4-5 days backup of camera feeds will help to improve uptime and also it will increase the number of incidents reported at early stage and will reduce drastically later.
- **Integration with Location based Services with CCTV Feeds** – The response time will improve and using location-based services will help to reach and also to track the criminal or women in distress.
- **Integration with Crime & Criminal database**- This will be up & running which will help to find the criminal as the FIR details will be available online
- **Availability of real time Video Analytics, Audio & Video Feed integration** - This will help to watch the women and crime in real time as the alerts will be generated instantly.
- **Provision of Emergency Operation Centre** – Having Emergency Operation Centre in C4I will improve the responsiveness and enable them to take instant decision in case of crime and criminals spotted.
- **Integration with ERSS** – The entire database of ERSS, Dial 112, 1091, 1098 will be available online and also will be updated as per new alerts generated in safe city project; it will help to have consolidated database to have effective use of ERSS
- **Integration with Himmat Plus App, Predictive Analysis** – This will enhance the prediction capability to find out Criminals and Crime locations. It will also be updated with database and will be easy to track the incidents and location.
- **City residents and non-profit organizations** – enabling them to understand the development and progress of Safe Cities
- **Evaluation and ranking agencies, including academia** – supporting them in selection of relevant KPIs for assessing the contribution from ICT in the development.

Outcome indicators should measure result or progress towards it audit logs, henceforth, there should be a **standardized indicator framework**. It will allow Delhi Police for the benchmarking and learning from the other cities in a similar position and can give a more objective idea of areas for development. If measures are repeated for a certain time against the same indicators it allows a city to monitor its progress, and focus its future investment. If results are report publicly they can help a city be more transparent. ISO 37120 defines the benefits of standardized indicators as:

- Better Alert Generation in case of Women in Distress situation
- Improvement in reporting of women related issues
- Improved response in case of women related distress situation
- Enhancement in prediction capability
- International benchmarks and targets
- Local benchmarking and planning
- Informed decision-making for policy makers



- Learning across cities
- Leverage for funding by cities with senior levels of government
- Framework for sustainability planning

FY	Financial Outlay	Expenditure	Output Against outlay	Output Indicator To be tracked	Baseline	Target	Achievement	Data Source	Notes

F Y	Financial Outlay	Expenditure	Projected Medium Outlay	Outcome Indicator to tracked	Base-line	Target	Achievement	Medium Term Target	Medium Term Achievement	Data Source	Notes

Functional Architecture Framework for Delhi Safe City Project

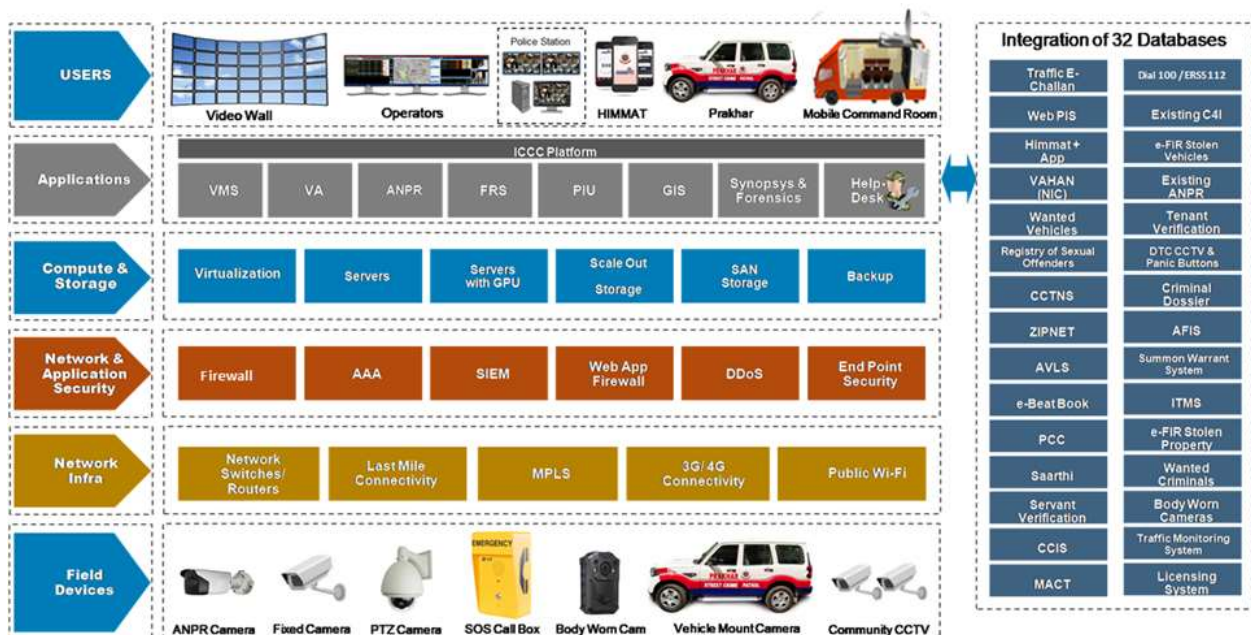


Figure: Essential Functional Components of Delhi Safe City Project



4.8. Component-wise Functional Requirements (with KPIs) and Technical Requirements

4.8.1. ICCP (Integrated Command & Control Center Platform) for C4i at PHQ

Functional Requirements of ICCP at C4i

- i. The Integrated Command & Control Center (ICCC) will be an enterprise class IP-enabled centralized application, will support the seamless unification of various Public Safety elements including Video Management System (VMS), Integrated Video Analytics System, Automatic Number Plate Recognition system (ANPR), Facial Detection & Recognition System (FRS), Picture Intelligence Unit, Incident management, Emergency Response System, Criminal tracking, Community Surveillance, Record management and integration with other Govt. databases on a single platform. The ICCP user interface (UI) applications shall present a unified security interface for the management, configuration, monitoring, co-relation, intelligence and reporting of various embedded systems and associated edge devices.
- ii. The ICCP platform must be a true unified management experience for critical infrastructure, simplifying control room operation and system integration, minimizing total cost of ownership, and increasing operational efficiency critical to rapid decision-making.
- iii. The ICCP Platform will maximize real-time monitoring and control efficiency from one workstation through the synchronized control of high-resolution blueprints, images, streaming camera data and system alerts which allows for interaction between all relevant data. There will be 20 Workstations for operators who render the services of ICCP Platform to showcase the video feeds (live streaming) along with the triggers and alerts generated by Analytical servers on the Video wall.
- iv. The ICCP will be open architecture based, highly scalable and able to integrate multiple disparate systems seamlessly on a common platform. The ICCP will provide a real time Common Operating Picture (COP) of the area involving all agencies using a simple Operator / User friendly interface.
- v. The ICCP platform will support various sensors like Cameras, GPS, Voice devices, Storage devices, Sensor inputs from other Utility applications/ systems. The ICCP platform will provide a dashboard functionality to manage workflows by integrating information from different agencies and systems to facilitate responsive decision making in City.
- vi. The ICCP platform will provide a cross-agency collaboration tool to support instant communication between various user groups and authorities. It will facilitate an Intelligent Fusion Center to conduct all Big Data Co-relation among various integrated datasets for interoperability.
- vii. The ICCP platform will be an IP enabled solution. All communication between the servers and other clients will be based on standard TCP/IP protocol and will use TLS encryption with digital certificates to secure the communication channel. The ICCP platform will protect against potential database server failure and continue to run through standard off-the-shelf solutions. The ICCP platform will support native and off-the-shelf failover options without any dependency on external application for both Hardware and Application level fail over.



KPI- Integrated Command & Control Center System

The following are the indicative functional requirements of ICCC required for safe city operations. MSI is expected to use all the functionalities of IOT platform/City Operations Platform for holistic management of Delhi Safe city applications and integrate applications within the scope of this RFP.

The required features of Integrated Command & Control Center for Safe city Delhi are as follows:

- a) Integrated Command and Control Center (ICCC) Platform.
- b) Integrated Dashboard – Provision for generating configurable reports through dashboard and also real time monitoring and Alert Systems.
- c) Video Wall & Controller System & Workstation for Operators
- d) Operator Workstation and Accessories Ex. Telephone, fax, inter-com etc.
- e) Alerting system service through SMS gateway, etc.
- f) Integration with 32 datasets of existing application of different projects of Delhi Police
- g) Helpdesk Service and Emergency Operation Centers on 24X7 basis.
- h) Necessary Civil, Electrical work including furniture, acoustics design including Air-conditioning for Data Center, fire safety, and Command & Control Center.
- i) Key functionalities of ICCC





**C4i platform (software)- Technical Requirements and Compliance Sheet
for MSI (to provide compliance report with the bid)**

S. No	Technical Specification	Compliance (Yes/No) with comments, if any
A	General	
1.	The Unified Command & Control Platform (UC&C) shall be an enterprise class IP-enabled Cloud ready application. The UC&C shall support the seamless unification of various Public Safety elements IP video management system (VMS), IP automatic number plate recognition system (ALPR), Incident management, Emergency response system. Criminal tracking, record management with future scalability to include Traffic management solutions also under a single platform. The UC&C user interface (UI) applications shall present a unified security interface for the management, configuration, monitoring, co - relation, intelligence and reporting of various embedded systems and associated edge devices.	
2.	The platform must be Cloud ready from day 1 and must have the ability to host either in total or some of the modules in a private cloud environment approved by Meity.	
3.	The platform must have native failover with no dependency on external virtualized or clustered applications. The failover must support both local & over geographical redundancy for all the modules outlined under the UC & C platform.	
4.	The UC&C platform must be a true unified management experience for critical infrastructure, simplifying control room operation and system integration, minimizing total cost of ownership, and increasing operational efficiency critical to rapid decision-making.	
5.	The UC&C Platform Shall Maximize real-time monitoring and control efficiency from one workstation through the synchronized control of high-resolution blueprints, images, streaming camera data, and system alerts which allows for interaction between all relevant data	
6.	Allows simple and accessible Integration with other independent control systems through a single Unification point with consistent user interface and better operational efficiency.	
7.	UC&C shall be open architecture based, highly scalable and able to integrate multiple disparate systems seamlessly on a common platform	
8.	UC&C system shall provide a real time Common Operating Picture (UC&C) of the area involving all agencies using a simple Operator / User friendly interface.	
9.	The system shall support various sensors like Cameras, GPS, Voice devices, Storage devices, Sensor inputs from other Utility applications/ systems	



10.	The UC&C platform shall provide a dashboard functionality to manage workflows by integrating information from different agencies and systems to facilitate responsive decision making in City.	
11.	The UC&C platform should provide a cross-agency collaboration tool to support instant communication between various user groups and authorities.	
12.	The ICCC software should have biometric authentication facility for operators using the software.	
B	UC&C Architecture:	
	The Application shall be an IP enabled solution. All communication between the servers and other clients shall be based on standard TCP/IP protocol and shall use TLS encryption with digital certificates to secure the communication channel.	
2	The Application shall protect against potential database server failure and continue to run through standard off-the-shelf solutions.	
3	The Application shall support up to one thousand instances of Clients connected at the same time. However, an unrestricted number of Clients can be installed at any time	
4	The Application shall support an unrestricted number of logs and historical transactions (events and alarms) with the maximum allowed being limited by the amount of hard disk space available.	
5	The UC&C Application shall support native and off-the-shelf failover options without any dependency on external application for both Hardware and Application level fail over.	
C	Native Map module (Both GIS and Offline Maps):	
1	The GIS MAP shall support the following file format PDF, JPG, PNG Web Map Service (WMS) defined by the Open Geospatial Consortium (OGC).	
2	It shall be possible to configure a mixed set of maps made of GIS, online providers and private imported files and link them together.	
3	The UC&C shall provide a map centric interface with the ability to Command & Control all the system capabilities from a full screen map interface.	
4	It shall be possible to span the map over all screens of the UC&C client station. In the scenario where the map is spanned over all the screens of the UC&C client station it shall be possible to navigate the map including pan and zoom, and the map's moves shall be synchronized between all screens. Spanning the map over multiple screens must provide the same Command & Control capabilities than in a single screen display.	
5	The GIS MAP shall provide the ability to display layer of information in Keyhole Mark-up Language (KML) format.	
6	It shall be possible to monitor the state of entities on the map. It shall be possible to customize the icons of any entities represented on the map.	



7	The GIS MAP shall offer a smart selection tool to access the video. By clicking the location, the user wants to see, the GIS MAP will automatically select the cameras that can see this location and move the PTZ towards that location. This smart selection tool shall take obstacles into consideration and not display cameras that cannot see the location because of a wall.	
8	It shall be possible to select a location by drawing a zone of interest on the GIS MAP, and to display all the entities that are part of that zone of interest at once.	
9	The user shall be able to select and display the content of multiple UC&C entities on the map in popup windows.	
10	The GIS MAP shall provide the following search capabilities:	
11	Search within the map by entity name, street name, or point of interest.	
12	Drag and drop entities from the UC&C to the map to center their location.	
13	Map to support event-based response actions for decision making in case of any emergency / critical situation	
15	CCTV feeds to be viewed on the Map in case of any event triggers	
D	Alarm management:	
1	The UC&C shall support the following Alarm Management functionality:	
2	Create and modify user-defined alarms. An unrestricted number of user-defined alarms shall be supported.	
3	Assign a time schedule or a coverage period to an alarm. An alarm shall be triggered only if it is a valid alarm for the current period.	
4	Set the priority level of an alarm and its reactivation threshold.	
5	Define whether to display live or recorded video, still frames or a mix once the alarm is triggered.	
6	Provide the ability to display live and recorded video within the same video tile using picture-in-picture (PiP) mode.	
7	Provide the ability to group alarms by source and by type.	
8	Define the recipients of an alarm. Alarm notifications shall be routed to one or more recipients. Recipients shall be assigned a priority level that prioritizes the order of reception of an alarm.	
9	The workflows to create, modify, add instructions and procedures, and acknowledge an alarm shall be consistent for various systems.	
10	The UC&C shall also support alarm notification to an email address or any device using the SMTP protocol.	
11	The ability to create alarm-related instructions shall be supported through the display of one or more HTML pages following an alarm event. The HTML pages shall be user-defined and can be interlinked.	
12	The user shall can acknowledge alarms, create an incident upon alarm acknowledgement, and put an alarm to snooze.	



13	The user shall be able to spontaneously trigger alarms based on something he or she sees in the UC&C system Dashboard.	
14	UC&C platform should generate Notification, Alert and Alarm messages as per the incidences / events that are received, that should be visible within the Dashboard and the Field Responder Mobile App or web services/portal if required	
15	1. All system messages (notifications, alerts and alarms) should always be available from the Notifications View, which provides controls that operator can use to sort and filter the messages that it displays	
16	2. ICCP platform should support to deliver message to a set of subscribers. The Notification service should support min two types of notification methods: a. Email notification b. Short Messaging Service (SMS) notification	
E	Incident management (IM) module:	
1	The IM MODULE shall be seamlessly embedded and must be a native module in the UC&C Platform.	
2	The UC&C and IM MODULE shall be forward compatible so upgrade of one does not prevent from using the other.	
3	The IM MODULE shall be seamlessly compatible with the UC&C and any of its components including VMS, ALPR, Big Data Co relation tool and external SDK integrations with 3 rd party systems.	
4	The IM MODULE shall offer the following native operational tools: a. Incident management b. Document management c. Rules Engine d. Workflow automation e. Standard operating procedures f. Incident monitoring operator interface g. Incident reports	
5	The IM MODULE shall provide situational intelligence to the operator with a map-centric approach and detailed overview of incident data, combining incident history, operator comments, workflow and operator action logs, standard operating procedures, relevant live and playback video, and an aggregated events sequence of the incident.	
6	The IM MODULE shall log all configuration changes in an audit trail with before and after configurations.	
7	The IM MODULE shall log all the user activities that are executed during the time that an incident is active.	
8	The IM MODULE shall provide the ability to configure incidents in a test mode that would allow user with the appropriate privilege to validate different parameters before activating the incident configuration.	



9	The IM MODULE shall be the interface that displays all situations as incidents.	
10	The IM MODULE Incident management shall provide the ability to trigger incidents manually or automatically, based on a correlation of events.	
11	An incident shall be the holistic description of the situation and support the following attributes: Visual: • Colour • Icon. Incident management shall provide the ability to customize incident types using a set of imported icons. Sound Incident category. Incident category shall allow an operator to organize incident types in a logical tree The location can be an entity (camera, door, zone, area) or a geographical coordinate. A priority level A description States Standard operating procedures. History of activities. Attach Entities. Entities related to the source of events triggering the incident shall be automatically associated to the incident. Attached documents. Documents and URLs providing more information or guidance on the incident and its management.	
12	The Incident management shall provide management of incident ownership. It shall be possible to explicitly request or release the ownership of an incident. Ownership of an incident shall be provided immediately to an operator who starts working on an incident.	
13	A supervisor shall be able to view all incidents that are under his supervision and see the ownership of each incident. In the same view, the supervisor shall also be provided with real-time information about who is currently monitoring an incident.	
14	The IM MODULE shall notify the supervisor when an operator skips a step in the standard operating procedure (SOP).	
15	For each incident, it shall be possible to open the incident details. The incident details will open on a configurable screen and provide, based on the incident type configuration, the following information: 1. A layout of all live and playback video related to the incident, including the camera associated to the source and location of the incident, as well as the local map centered on the incident location. 2. History of the incident including: a. All events related to the incident	



	b. System workflow activities c. Operator actions for the incident d. Comments about the incident	
16	Operators shall be able to perform the following actions: 1. Change the incident state. 2. Forward the incident. 3. Transfer the incident. 4. Edit the incident: a. Change the description b. Change the priority level c. Release the ownership 5. Attach additional entities to the incident. 6. Link related incidents. 7. Attach a document as a URL link to the incident. 8. Link the flagged incident data.	
17	The IM MODULE shall provide the ability to dispatch an incident to a user or group of users. Dispatching an incident to a restricted number of users will secure the access to information.	
18	The IM MODULE shall allow the distribution of specific tasks (managed as sub- incidents) that are associated to a unique incident, to different teams. Procedures can be performed in parallel.	
19	Incident supervisors shall be able to see all sub-incidents associated with a main incident.	
20	The IM MODULE shall offer a task to manage and generate reports. The ability to run a report is a user privilege.	
21	It shall be possible to query the incident history filtering by: a. Incident type b. Incident state c. Location d. Priority e. Trigger time range f. Incident owner d. Description	
22	The result of a report query shall provide a list of incidents as well as a visual of these incident locations on the map. When more than one incident is reported at the location, the GUI will cluster these incidents on the map.	
23	For closed incidents, the incident shall be in read-only mode with the exception of adding links to related incidents.	
24	The Report task shall also report the user activity log of the UC&C for the time in which the operator was owner of the incident and was monitoring it, in order to provide a view of all actions taken towards the resolution of this incident.	
25	The IM MODULE shall offer all reports in a visual presentation format (such as pie charts, lines, columns, and rows) native within the	



	platform with no necessary for additional external tools or software modules.	
26	The IM MODULE shall support the following report formats: a. HTML b. PDF c. XML d. Custom format	
27	The IM must have native document management tool and UC&C platform shall provide the ability to dynamically index documents to an incident in order to improve the efficiency of access to information for an operator.	
28	A document shall be automatically attached to an incident if the document properties match the incident properties. The following properties shall be available: a. Incident type b. Schedule c. Location. Location can be an entity or an area. d. User or user group of the operator monitoring the incident.	
29	The IM MODULE shall offer the ability to automatically link a document to a step in a standard operating procedure.	
30	Document Management shall provide a file system to store all documents as well as the document URLs for the use of third-party file systems.	
31	The Incident Management module should have facility to configure a sequence of events using logical AND /OR /NOT operators to trigger and incident.	
32	Configuring the Rules Engine shall be graphical without need for a script.	
33	It shall be possible to configure a complex sequence of rules by applying the occurrence, the interval, and event filtering.	
34	It shall also be possible to script the rules in advance and import them into the system later.	
35	The IM Module shall provide a native Workflow Engine to automate the response to an incident type.	
36	The IM Module shall provide a graphical workflow designer. No scripting competence shall be required to implement a workflow.	
37	It shall be possible to define a workflow for each incident type. The workflow shall be a series of activities that are sequentially executed.	
38	The IM Workflow Engine tool shall provide a framework to create custom activities that allow integration into a global business process.	
39	The IM Module shall provide guidance for operators in the form of a standard operating procedure (SOP) for the response to an incident type.	
40	The SOP shall be interactive and offer an operator-acknowledgement-audit for each	



	SOP step.	
41	The SOP shall be dynamic and provide the ability to adapt the next steps in a procedure based on the responses to previous steps in the procedure.	
42	The IM Module shall provide the ability to skip a step of the SOP and request a justification for skipping the step.	
43	Each step shall be optionally associated to a document in the form of a URL, or a document in a supported format (such as Word, PDF, or HTML).	
44	The tool shall track the elapsed time for each step of the SOP, as well as the total elapsed time from the initial response to resolution and enable the authorities to determine the steps which are getting delayed and plan the training needs for the crime analysts and UC & C operators.	
45	The IM MODULE shall provide the ability to configure standard options when defining dynamic steps of the SOP.	
46	A maximum delay shall be allowed for a user to initiate the procedure. Automated actions associated with this time to response threshold shall be configurable.	
47	A minimum time shall be allocated for a user to complete the procedure. Closing the incident before passing this time to resolution threshold shall trigger automated actions.	
48	A visual indicator shall be displayed when maximum time to response or the maximum time to resolution for the incident is exceeded.	
F	Big Data and Co Relation Tool (BDCR)	
1	The UC & C platform either native or through external module must have the below big data mining and Co Relation tools	
2	The BDCR must have a native Correlation engine which can assesses both temporal and geospatial data from multiple data sets like CCTNS, Court management, Dial 112 / emergency call system, Video Analytics, VMS, ANPR systems, GIS, Vehicle location systems, FRS and any other public safety or crime intelligence tools.	
3	The crime analyst or the operator in the Command Center through the UC & C module should be able to query data specific to incidents and gather all the meaningful information related to incident from discreet data sets through the native Correlation tool.	
4	The tool must generate correlation data for specific incident based on specific Query or Geospatial location-based analysis.	
5	The tool must provide relevant information during any incident Based on geospatial and temporal criteria, by detecting and displaying all relevant information from cameras, people, vehicles, and events that would be interest to specific incident or crime and also needs immediate attention.	
6	The tool must support native following Crime analytics and Insights module for proactive policing, Authority may want to activate this	



	module on need basis when the needed technology platforms like centralized data lake etc. are available – Prediction can happen for the following entities (indicative) a. Crimes - Using historical crime data, determining when certain areas will be more vulnerable, identifying geographical features. b. Offenders - Criminal groups, Criminal profiles, juvenile offenders likely to become major criminals. c. Perpetrator identities - Patterns in crimes done by the offender, profiling the kind of weaponry he keeps d. Point in time Analysis on areas like resource invested Vs Crimes going down in specific areas / Districts. e. Crime victims - Identifying groups likely to be hurt (religious targets), people at risk of domestic violence, etc. f. Time and Geography - Patterns in the area which is likely to experience unrest and time of the day, week or year within which a particular geography should be kept in check.	
G	Reporting:	
1	The UC&C shall support report generation (database reporting) for various systems Unified into the platform access control, ALPR, video, and intrusion.	
2	The workflows to create, modify, and run a report shall be consistent for all systems.	
3	The UC&C shall support the following types of reports:	
4	Alarm reports.	
5	Video-specific reports (archive, bookmark, motion, and more).	
6	Configuration reports	
7	ALPR-specific reports (mobile ALPR playback, hits, plate reads, reads/hits per day, reads/hits per ALPR zone, and more).	
8	System Health activity and health statistics reports for proactive maintenance.	
9	Generic Reports, Custom Reports and Report Templates	
10	The user shall be able to customize the predefined reports and save them as new report templates. There shall be no need for an external reporting tool to create custom reports and report templates. Customization options shall include setting filters, report lengths, and timeout period. The user shall also be able to set which columns shall be visible in a report. The sorting of reported data shall be available by clicking on the appropriate column and selecting a sort order (ascending or descending).	
11	The UC&C shall support comprehensive data filtering for most reports based on entity type, event type, event timestamp, custom fields, and more.	
12	The user shall be able to click on an entity within an existing report to generate additional reports from the Monitoring UI.	



13	The UC&C shall support the following actions on a report: print report, export report to a PDF/Microsoft Excel/CSV file, and automatically email a report based on a schedule and a list of one or more recipients.	
14	Reporting function is part of Command & Control dashboard visualization tool. It shall provide information about status of the Command & Control on managing the security incidents across the locations. Reporting function should enable operator to create reports in either graphical format or flat tabular format. Reports shall be created automatically or manually by operator whenever required. The reports should be generated and exported as a Microsoft word excel format or an acrobat format by operator.	
15	It shall be possible to generate a report from UC & C interface based on the profiles defined for the Incident management and associated tools defined with in IM Module. a. The profile report shall be exportable and printable. b. Profile reports shall allow filtering on profile identifier, initiators, recipient, and modification time. c. Columns for the profile reports shall be configurable.	
G	Real Time Dashboard:	
1	Real time dashboard should provide the real-time information about the security situation so called Situational Awareness for the Authorities and senior officials in a single go.	
2	The Monitoring UI shall dynamically adapt to what the operator is doing. This shall be accomplished through the concept of widgets that are grouped in the Monitoring UI dashboard.	
3	Widgets shall be mini-applications or mini-groupings in the Monitoring UI dashboard that let the operator perform common tasks and provide them with fast access to information and actions. ICCC software should have drag and drop facility for all widgets for user to move the required alerts and other windows on priority basis.	
4	Analysts / Operators shall be allowed to view dashboards if they are granted the appropriate privilege. Modification to the dashboards should also be allowed to users granted the appropriate privilege.	
5	Dashboard widget types shall be: Image: provides the ability to display an image (JPG, PNG, GIF, and BMP) on a dashboard. Text: provides the ability to display a text on a dashboard. The text style shall be configurable, so font, size, colour, and alignment can be specified by the user. Tile: provides the ability to display any entity of the USP inside of a tile. Web page: provides the ability to display a URL on a dashboard. Entity Count: provides the ability to display the total number of a specific entity type in the UC&C.	



	f. Reports: provides the ability to display the results of any saved reports in the system. The results shall be displayed either by showing the total number of results in the report, a set of top results from the report, or a visual graph from the data returned by the report.	
6	It shall be possible to extend the widgets of a dashboard using the SDK. This will provide the ability to develop custom widgets to the system.	
G	Threat Level Indication:	
1	UC&C should display the threat level based on the number of alerts and criticality of the alerts using color coded display. It should also follow a pre-defined system to alert different users on different hierarchy based on the criticality of alerts. It should be possible to activate various threat situations from Web / Mobile client application for those users with appropriate privileges.	
H	Incident Management & Reporting:	
1	The UC&C shall support the configuration and management of events. A user shall be able to add, delete, or modify an action tied to an event if he has the appropriate privileges.	
2	The UC&C shall receive all incoming events from one or more Unified Systems. The UC&C shall take the appropriate actions based on user-define event/action relationships.	
3	Incident reports shall allow the security operator to create reports on incidents that occurred during a shift. Both video-related and other Unified Systems related incident reports shall be supported.	
4	The operator shall be able to create standalone incident reports or incident reports tied to alarms.	
5	The operator shall be able to link multiple video sequences to an incident, access them in an incident report.	
6	It shall be possible to create a list of Incident categories, tag a category to an incident, and filter the search with the category as a parameter.	
7	Incident reports shall allow the creation of a custom form on which to input information on an incident.	
8	Incident reports shall allow entities, events, and alarms to be added to support at the report's conclusions.	
9	Incidents reports shall have facility for generating escalation matrix for alerts and incidents.	
H	Configuration User Interface:	
1	The Configuration UI application shall allow the administrator or users with appropriate privileges to change the system configuration.	
2	The configuration of all embedded systems shall be accessible via the Configuration UI.	
3	The Configuration UI shall have a home page with single-click access to various tasks.	



4	The Configuration UI shall include a variety of tools such as troubleshooting utilities, import tools, and a unit discover tool, amongst many more.	
5	The Configuration UI shall include a static reporting interface to: View historical events based on entity activity. The user shall be able to perform such actions as printing a report and troubleshooting a specific access event from the reporting view. View audit trails that show a history of user/administrator changes to an entity.	
6	Common entities such as users, schedules, alarms and many more, can be reused by all embedded systems in platform.	
7	The application must have single user unified interface for configurations of all the systems of Video, ANPR and Emergency response.	
8	There should not be any limitation on the number of end client licenses for the UC & C application.	
I	Smartphone and Tablet App General Requirements:	
1	The UC&C shall support mobile apps for various off-the-shelf smartphones and tablets. The mobile apps shall communicate with the Mobile Server of the UC&C over any WIFI or mobile network connection.	
2	All the communication between the mobile apps and UC&C platform will be on HTTP and by adding TLS encryption on https.	
J	Mobile app Functionalities:	
1	Ability to logon/logoff the UPS using an authorized use profile of the system. Ability to change the picture or the password of the user of the mobile app. Ability to view the current Threat Level of the system. Ability to change the current Threat Level of the system. Ability to execute hot actions configured in the user profile. Ability to view below minimum edge devices Unified with the UC&C platform: Cameras ii. ALPR cameras GIS and Offline Maps Iv. Ability to navigate the system hierarchical view of the edge devices & entities with ability to search entities in the system.	
2	It shall be possible to download the mobile apps from the Central application store (Apple iTunes App Store, Google Play, Windows Store).	
K	System Health Monitor:	



1	The UC&C shall monitor the health of the system, log health-related events, and calculate statistics.	
2	Detailed system care statistics will be available through a web-based dashboard providing health metrics of UC&C entities and roles, including Uptime and mean-time-between-failures.	
3	Health events shall be accessible via the SDK (can be used to create SNMP traps with external EMS / NMS systems).	
L	UC&C Audit and User Activity Trails:	
1	The UC&C shall support the generation of audit trails. Audit trails shall consist of logs of operator/administrator additions, deletions, and modifications.	
2	Audit trails shall be generated as reports. They shall be able to track changes made within specific time periods. Querying on specific users, changes, affected entities, and time periods shall also be possible.	
3	For entity configuration changes, the audit trail report shall include detailed information of the value before and after the changes.	
4	The UC&C shall support the generation of user activity trails. User activity trails shall consist of logs of operator activity on the UC&C such as login, camera viewed, badge printing, video export, and more.	
5	The UC & C shall support the following actions on an audit and activity trail report: print report and export report to a PDF/ Microsoft Excel/CSV file.	
M	Third Party System Unification:	
1	Directory service like MS – AD or Similar integration shall permit the central user management of the UC&C users, user groups and other Access control groups.	
2	The UC&C shall support multiple approaches to integrating third party systems and other Safe City application. These shall include: Software Development Kits (SDKs), Driver Development Kits (DDKs), REST-based Web Service SDK and RTSP Service SDKs.	
3	A UC&C SDK shall be available to support custom development for the platform.	
4	The SDK shall enable end-users to develop new functionality (user interface, standalone applications, or services) to link the UC&C to third party business systems and applications such as Badging Systems, Human Resources Management Systems (HRMS), and Enterprise Resource Planning (ERP) systems.	
5	The SDK shall provide an extensive list of programming functions to view and/or configure core entities such as: users and user groups, alarms, custom events, and schedules, and more.	
N	Cyber Security Requirements:	
1	The UC&C Application shall be an IP enabled solution. All communication between the Servers, Clients and external systems shall be based on standard TCP/IP protocol and shall use TLS	



	encryption with digital certificates to secure the communication channel.	
2	The Application shall limit the IP ports in use and shall provide the Administrator with the ability to configure these ports.	
3	The VMS system Unified with the UC&C application shall support only secured media stream requests, unless explicitly configured otherwise. Secured media stream requests shall be secured with strong certificate-based authentication leveraging RTSPS (aka RTSP over TLS). Client authentication for media stream requests is claims-based and may use a limited lifetime security token.	
4	All other needed best practices for best Cyber Security Standards must be followed and adopted in the development, deployment and adoption phases of the project.	
5	The OEM of UC&C application shall have an online or offline Cyber Security emergency response center to update on latest vulnerabilities and provide needed assistance during any cyber-attacks on the system. Details of response center must be available on the OEM global website.	
6	All other needed best practices for best Cyber Security Standards must be followed and adopted in the development, deployment and adoption phases of the project.	

4.8.2. Video Management System Functional Requirements of VMS

- i. The proposed Video Management System (VMS) shall provide a complete end-to-end solution for security & surveillance application. The VMS shall be an enterprise class IP based application with Server-client architecture. The VMS shall support cameras using the industry standards ONVIF Profile S, and Profile G. The VMS shall have Management Servers, Recording Servers and Client Interface as integral part of the solution.
- ii. The VMS will be accompanied with the stack of recording servers is capable to record the live streaming flow of HD videos with appropriate codec and certifications in place. The recording servers under the supervision of VMS will render SDK services through media gateway upon the unicast stream of video per camera entered in DC in order to provide dedicated encrypted stream to the analytical servers, FRS servers and ANPR servers.
- iii. The Analytical platform will revert back the derived outcomes to the VMS which will be forwarded to the VMS clients located in the user workstations at C4i, Police Station and District Offices as per the defined jurisdictions. Also, the MCCV will be equipped with one of the VMS client of the central VMS platform to receive triggers for necessary and immediate field actions.
- iv. The VMS and C4i servers will conduct Out-of-Band Management (OOBM) Operations with the Analytical platform to enable users to be facilitated with triggered based structured outcomes at the video wall.



- v. The Surveillance System shall not have any limit on the number of cameras to be connected for Surveillance, Monitoring and Recording. Any increase in the no. of cameras shall be possible by augmentation of Hardware components.
- vi. Police personnel/ operators shall have following access to the video feeds of the cameras according to the role-based access assigned to them:
 - Viewing of the live Camera Video Streams (Approx. 10% of 10000 Camera) based on access rights
 - Viewing rights to the stored feeds, stored on Primary / Secondary Storage
 - Viewing of video feeds from collaborative public CCTV surveillance system
 - Viewing of video feeds basis upon the Alerts / Exceptions / Triggers raised by Video Analytics, FRS, ANPR and PIU system
 - Trail Report on specific person / object / vehicle for a specific period / location
 - Personalized Dashboard (depending upon role-based access level defined to the police personnel/ operators, detailed requirement finalization will be done during Pre-Implementation stage)
 - Provide search of recorded video. Advanced search should be possible based on various filters like alarm / event, area, camera, etc.
 - Export rights of video / other critical incident data based on appropriate rights and privileges
 - Ability to back up data stored in DC to Near DR on demand/ schedule based

KPI- VMS performance requirements

- i. The Police Stations, District Offices, PHQ will be provided with Video Management System (clients) in policy based association with the central VMS server at Data Center, with necessary computing and controllers to manage all the raw data feeds coming from the cameras of the respective territories for viewing under jurisdiction through multi-cast enabled MPLS network.
- ii. The Video Management System at Police Head Quarters will be equipped with C4i computing with all media servers regulated with central management server aligned with Database servers and adequate storage requirement. The envisaged multi-cast cameras will be equipped with in-built Network Video Storage (edge level storage) which will serve for continual storage pattern in case of failure or downtime with respect to any server as a part of this essential architecture.
- iii. There will be a provision of the single master server at C4i that will handle 10,000 new cameras, recording servers and unlimited users to access data. The Master Server will have manual and automatic mode for assigning cameras to the available recorder servers as per District or PHQ requirements. In automatic mode, the cameras will be assigned based on the compute capability of the recorder server. In manual mode, the system will allow the operator to assign the cameras. In both cases it will be possible to utilize all the recorder servers including the redundant one.
- iv. The Video Analytic and Artificial Intelligence tools will be capable to conduct real time analyses of the video feed and post data analyses of the triggered or tagged data from the big data pool. The Post Data Analyses will be provisioned with video summarization tool and methodologies by reducing timeframe of actual video substantially. This video synoptic



and summarization methodology will support Police Personal in investigation studies with minimal time consumption based on customized search facility. In order to keep the real time streaming and recording uninterrupted with possible downtime during Post Data Analyses when multiple users access same feed, a streaming server will be provisioned to route the accessibility without hampering the real time input efficiency.

- v. VMS will be camera agnostic. The IP details of each camera linked with the VMS so that the segregation of the real time streaming from respective cameras will be maintained and facilitate to store the continuous data feeds in the logical units of pre-defined virtualizations in the servers. Subsequently, the storage will also be linked with the same pattern indexing which will be helpful while retrieval during post analyses.
- vi. The viewing of the feeds will cater up to 10% of 10,000 cameras at a given point of time. This will enable the optimum and efficient use of provisioned bandwidth to minimize the recurring bandwidth expenditure. The VMS will periodically check the gaps in live recording of the cameras based on broken time periods of continuous feeds and will check with the on-board storage of the camera. In case of a gap, the VMS will synchronize the video recording on the on-board storage with the VMS storage through ONVIF Profile G standards.
- vii. The VMS will support multi-site deployments with centralized monitoring of the videos, video analytics and system health alerts.
 - Support matrix view at full frame rate
 - Support digital zoom of the cameras from central site.
 - Control PTZ cameras from central monitoring client application
 - Ability to pick and choose the selected cameras from remote sites.
 - Ability to search and retrieve the archived video from the remote site with intelligent motion-based search
 - Download multiple video segments from multiple sites efficiently
 - Multi-layer maps support
 - System health dashboard for all connected systems. The VMS will ensure performance checks of all cameras to alert upon the deficiency in flow of camera feeds, if any.
 - User and rights management with audit trail and logs
 - The VMS will ensure calibration of the camera feed to show case on the video wall or monitor displays.

Video Management Server for Camera feeds

- i. The Video Management Server will provide centralized management of all IP cameras in the city. The database will support more than 20000 cameras / IP end points in a single server. The Management Server will provide with 1:1 redundancy. The Fail over and Fall-back Management Server will be on hot standby, ready to take over during the primary Management Server fails. No manual action from the user will be required. The fail over time will not be beyond 1 Min and there should not be any loss in the Live and Recorded Videos of the connected cameras.
- ii. The Video Management Servers shall be capable to be running in virtualisation / Physical server environment in the DC. The Standby VMS server will support data recovery scenarios where a server can be in another building and only take over if Primary server become offline. Both Primary and Secondary must be based on a single instance Active – Active architecture. The Standby Server will support real-time synchronization of the configuration databases for high reliability.



Video Recording Server(s) for Camera feeds

- i. In the centralized scheme of solution, the Video Recording Servers will be running centrally in the best possible efficient environment in DC. Each Video Recording Server Host will be able to handle at least 960 Mbps of Video bandwidth in virtualized or physical environment to meet the project requirement.
- ii. The recording Servers will have N:1 redundancy. The Fail over and Fall-back Recording Server will be on hot standby, ready to take over during the primary Recording Server fails. No manual action from the user will be required. There should not be any loss in the Live and Recorded Videos of the connected cameras due to failover.
- iii. There will be 10% additional servers to handle the interim storage / database /failover requirements.

Storage requirement for Camera Video Streams

- i. In the centralized scheme of solution, there will be centralized storage for all cameras at DC. The centralised storage has been planned at DC to store all camera feeds for 30 days 24/7 at 4MP resolution or at the highest resolution available from the camera at 25 FPS with H.265 video compression.
- ii. The recordings of all cameras will happen at DC. In Case DC goes down, data of 5% critical camera location will travel to near DR, which has provision of scalability. 5% of Analytics and ANPR feeds and 100% storage of Tagged Data will be stored in active-active mode at near Data Recovery Centre. DC & nDR will have storage capacity of 30 days and 7 days respectively.
- iii. Additional storage capacity for the flagged data at DC which will be replicated to DR. The video feeds related to incidents and important in nature and which may be required for evidence purposes will be flagged by the operator. The flagged video feeds will be archived in the storage for at least 90 days or as defined SOP by the police officials. A pool of mixed drive to form a tier to keep video data for 24/48 hours on SSDs for better response during playback is required.

CCTV Monitoring requirement at C4i, C3i and C2i

- i. The VMS and its associated clients shall support Direct Multicast of video streams from the Cameras. The application shall redirect video streams to active viewing clients on the network using multicast UDP directly from cameras and the architecture shall not use multicast streaming via recording servers or any other servers. This will achieve bandwidth usage optimization in the city-wide network and increase the overall compute capacity of recording servers.
- ii. The VMS client workstations must support GPU based decoding for open standard video compression like H.265 etc.
- iii. The failover for VMS client workstations between the management servers hosted at DC must be seamless during any of the Management server of ICCV or VMS goes down.
- iv. At C4i, 10% of 10,000 cameras that is approx. 1000 cameras to be monitored live. Considering 16 cameras in one 70" screen, 48 screens will be displaying 768 cameras live on the video wall and 20 Operators and 01 supervisors will be able to view 320 cameras, sequentially. Operators will be able to swap or switch any camera from operator desk to video wall.
- v. At C3I, 10% of the cameras of that district, max approx. 100 cameras to be monitored live sequentially. C3I will have 1x3 matrix of 55" monitor displays along with operator workstations with 3 nos. 24" monitors each (57 WS across all 16 C3i).



- vi. At C2I, the operators will be able to monitor up to 30% cameras on operator workstation(s) per police station, The C2i where the number of reporting cameras are equal or more than 50 no. will be equipped with LED screen for magnified viewing of the camera feed in case of alert generation. Two LED screens are provisioned for the C2i where reporting cameras are equal or more than 100 no.

Edge Community Surveillance / SWAT teams Gateway

- a. 50 edge gateway devices will be procured as an integral part of the Project Solution. It will be used for connecting the feeds of existing cameras reporting to Police Stations/ Police District offices/ NDMC Control Room. The Edge Gateway appliances will connect the external set of cameras that will be used as per need basis.
- b. The primary purpose of the gateway is to provide critical situational awareness solution by accessing live video camera feeds during any crisis operations or in the community surveillance solution requirements.
- c. The gateway with embedded software will have the ability to connect with 3rd party VMS software / NVR systems deployed in the private and public institutions and act as a gateway to get the live cameras feeds in to ICCV VMS application.
- d. The gateway will have an ability to stream at least 200 cameras from each of the deployment site live into the Command centers or any other locations where the C4i / VMS application is made available.
- e. Live video feed streaming should not have any dependency in any format on the 3rd party VMS or NVR solutions deployed in the private or public institutions where such gateways would be deployed.
- f. The communication between Edge gateway and VMS / C4i application at command center or any other location will be secured and encrypted.
- g. The gateway will have the native intelligence to stream live video with dependency only on the network infrastructure of the 3rd party system and under no circumstances the solution should depend / intervene on the 3rd party solution deployed except accessing the live video feeds from the CCTV cameras deployed at sites.
- h. The device / software will be Cyber securely hardened.
- i. The requirement of 50 Edge- Gateways will be increased as per the requirement.

Page 236 of 656



VMS and Recording Software- Technical Requirements and Compliance Sheet for MSI (to provide compliance report with the bid)

S. No	Technical Specification	Compliance (Yes/ No) with comments, if any
A	VMS General Requirements	
1	Licenses: 10,000 camera licenses + 1000 (floating licensing for integration of 15000 Existing cameras of Delhi Police	
2	The VMS application must seamlessly Integrate with the ICCC platform including the sub modules like Incident management and Big data tools for all the functionalities outlined.	
3	The VMS shall be based on a true open enterprise architecture that shall allow the use of non-proprietary workstation and server hardware, non-proprietary network infrastructure and non-proprietary storage. The VMS application provider must support at least 50 + brands of Cameras and the list of integrations must be listed on the global web site of the application provider.	
4	The VMS shall integrate cameras using dedicated driver or using the industry standards ONVIF Profile S and Profile G. The same must be listed on the ONVIF website.	
5	The Security application shall offer a complete and scalable video surveillance solution which allows cameras to be added on a unit-by-unit basis. The database shall support more than 50000 cameras / IP end points in a single Hardware machine.	
6	The Proposed VMS Solution Shall support native Fail over with in application with no dependency on any external application for both hardware and application redundancy. The native fail over architecture must be for both management and recording servers.	
7	The Fail over and Fall-back management and recording Server shall be on hot standby, ready to take over during the primary management server fails. No manual action from the user shall be required. The fail over time should not be beyond 1 Min and there should not be any loss in the Live video and recorded video.	
8	The Standby VMS server shall support disaster recovery scenarios where a server can be in another geographic area (or building) and only take over if Primary server become offline. Both Primary DC and Secondary DC must be based on a single instance Active – Active architecture.	
9	The Standby Server shall support real-time synchronization of the configuration databases for high reliability.	
10	The Application shall offer a plug and play type hardware discovery service with the following functionalities:	
11	Automatically discover Video surveillance units as they are attached to the network.	



12	Discover Surveillance units on different network segments, including the Internet, and across routers with or without network address translation (NAT) capabilities.	
13	The Application shall have the capacity to configure the key frame interval (I-frame) in seconds or number of frames.	
14	The Application shall allow for multiple recording schedules to be assigned to a single camera.	
15	The Application shall support Direct Multicast from Camera. For network topologies that restrict the Application from sending multicast UDP streams, the application shall redirect audio/video streams to active viewing clients on the network using multicast UDP directly from cameras and the architecture should not use Multicast streaming via recording servers or any other servers and increase the overall compute capacity of Recording servers.	
16	The Application shall allow important video sequences to be protected against normal disk clean-up routines.	
17	The application shall have the following options when protecting a video sequence: Until a specified date, for a specified number of days, indefinitely (until the protection is explicitly removed for evidence).	
18	The application shall support edge recording capabilities with ability to playback the video recorded at different speeds and ability to offload the video recorded on the application server on schedule, on event, or manually to store it on the recording server.	
19	The proposed software shall be scalable to support live viewing and automatic transfer of video recorded to the cloud on demand basis from UC&C user interface, based on the age of the video for future scalability and the hosted Cloud Platform must be among the approved vendors as per the MeitY approved GI Cloud initiative from Govt of India. The proposed application must provide a single interface to monitor, collaborate and action for both on premises and cloud devices like cameras, ANPR devices etc.	
20	The Application shall be capable to handle both IP v4 and IP v6 Unicast and Multicast traffic with both PIM - SM and PIM - DM support.	
21	The application management server should not have any limitation on the no of recording servers added on one single management / fail over server. Any limitations must be clearly specified by the bidder.	
22	There should not be any dependency on the end point MAC address for licensing for ease of operations.	
23	VMS Software must be capable and certified to run on Physical or Virtualized Environment	
24	The VMS Platform must have the capability to real time and scheduled backup video/ Flagged and critical data to Near DR Servers/Storage	
25	The VMS platform must have the flexibility to deploy rules for storing and avoiding data deletion of the flagged data, critical data, & Incident reports based on the criticality of the data.	



B	Client Interface	
1	The Monitoring UI shall support the role of a Unified Security Interface that can monitor various Video, ALPR, and other system events and alarms, as well as view live and recorded video.	
2	VMS shall enable seamless integration with video analytics systems like face recognition, intrusion detection, crowd monitoring; Automated Number Plate Recognition (ANPR) system, other traffic management applications; and other typical video analytics applications	
3	The system shall have a single API interface for sending Analytics event alerts and other Maintenance Alerts over HTTP protocol to external systems such as Command & Control Application, Incident Management System, etc.	
4	The Client Viewer shall allow digital zooming on live view as well as on replay view on Fixed as well as PTZ Cameras.	
5	The Client Viewer shall support the use of standard PTZ controller or 3-axis USB joysticks for control of pan, tilt, zoom and auxiliary camera functions.	
6	The Client Viewer shall have the capability to receive multicast streams if a pre-set number of clients are requesting the same live view camera. The system shall have the capability to detect if the network becomes unreliable and to automatically switch to unicast to ensure that the operator is able to receive video.	
C	User workspace customization:	
1	The user shall have full control over the user workspace through a variety of user-selectable customization options. Administrators shall also be able to limit what users and operators can modify in their workspace through privileges.	
2	Once customized, the user shall be able to save his or her workspace.	
3	The user workspace shall be accessible by a specific user from any client application on the network.	
4	Display tile patterns shall be customizable.	
5	Event or alarm lists shall span anywhere from a portion of the screen up to the entire screen and shall be resizable by the user. The length of event or alarm lists shall be user-defined. Scroll bars shall enable the user to navigate through lengthy lists of events and alarms.	
6	The Monitoring UI shall support multiple display tile patterns (e.g. 1 display tile (1x1 matrix), 16 tiles (8x8 matrix), and multiple additional variations).	
7	Additional customization options include: show/hide window panes, show/hide menus/toolbars, show/hide overlaid information on video, resize different window panes, and choice of tile display pattern on a per task basis.	
8	The Monitoring UI shall provide an interface to support the following tasks and activities common to Various systems	



9	Monitoring the events from a live security system	
10	Generating reports, including custom reports.	
11	Monitoring and acknowledging alarms.	
12	Creating and editing incidents and generating incident reports.	
13	Displaying dynamic graphical maps and floor plans as well as executing actions from dynamic graphical maps and floor plans Unified with UC&C.	
14	The live video viewing capabilities of the Monitoring UI shall include:	
15	The ability to display all cameras attached to the system both Public, Collaborative monitoring and Cloud based entities.	
16	The ability to drag and drop a camera into a display tile for live viewing.	
17	The ability to drag and drop a camera from a map into a display tile for live viewing.	
18	Support for digital zoom on live camera video streams.	
19	The ability for audio communication with video units with audio input and output.	
20	The ability to control pan-tilt-zoom, iris, focus, and Presets.	
21	The ability to bookmark important events for later retrieval on any archiving camera and to uniquely name each bookmark in order to facilitate future searches.	
22	The ability to start/stop recording on any camera in the system that is configured to allow manual recording by clicking on a single button.	
23	The ability to activate or de-activate viewing of all system events as they occur.	
24	The ability to switch to instant replay of the video for any archiving camera with the simple click of button.	
25	The ability to take snapshots of live video and be able to save or print the snapshots.	
26	The ability to browse through a list of all bookmarks created on the system and select any bookmarked event for viewing.	
27	Tools for exporting video and a self-contained video player on various media such as USB keys, CD/DVD-ROM and Proposed Evidence management and Collaboration system. This video player shall be easy to use without training and shall still support reviewing video metadata.	
28	Tools for exporting video sequences in standard video formats, such as ASF, MP4	
29	The ability to encrypt exported video files with industry standard encryption.	
30	A tool building and exporting a set of videos into a single container. This tool shall allow the operator to build sequences of video to create a storyboard and allow the export of synchronous cameras.	
D	Cyber Security Requirements:	



1	The VMS shall support only secured media stream requests, unless explicitly configured otherwise. Secured media stream requests shall be secured with strong certificate-based authentication leveraging RTSPS (aka RTSP over TLS). Client authentication for media stream requests is claims-based and may use a limited lifetime security token.	
2	The VMS shall offer the ability to encrypt the media stream, including video, audio, and metadata with authenticated encryption. Media stream encryption shall be done at rest and in transit and be a certificate-based AES 128-bit encryption.	
3	The VMS shall allow encryption to be set on a per camera basis for all or some of the cameras.	
4	Provide up to 20 different certificates for different groups of users who have been granted access to decrypted streams.	
5	Use Secure RTP (SRTP) to encrypt the payload of a media stream in transit and allow multicast and unicast of the encrypted stream.	
6	Use a random encryption key and change periodically.	
7	Allow encrypted streams to be exported.	
8	The VMS shall support end to end encrypted streams with cameras supporting Secure RTP (SRTP) both in unicast and multicast from the camera.	
9	The Application shall support digitally sign recorded video using 2048-bit RSA public/private key cryptography.	
10	The Application shall protect archived audio/video files and the system database against network access and non-administrative user access.	
11	Media encryption shall support with latest industry standards - AES-128.	
12	The application must support encryptions at the rest and not only on the exported videos footage	
13	The proposed VMS platform must have international recognized certifications to prove the Cybersecurity standards adaption. Bidders to submit the certifications along with the technical bid.	
E	User Authentication support:	
1	The system shall support logon using the user name and password credentials shall allow distributed viewing of multiple cameras on the system on any monitor.	
2	System shall be integrated with dual factor authentication using LDAP/ AD and fingerprint based biometric devices for User authentication.	
3	The system shall include flexible access rights and allow each user to be assigned several roles where each shall define access rights to cameras.	
4	The System shall provide a feature-rich administration client for system configuration and day to- day administration of the system.	



5	The VMS shall support mobile apps for various off-the-shelf devices. The mobile apps shall communicate with the Mobile Server of the VMS over any Wi-Fi or cellular network connection.	
6	All communication between the mobile apps and central server shall be based on standard TCP/IP protocol and shall use the TLS encryption with digital certificates to secure the communication channel.	
F	Other essential Functionalities:	
1	Core The mobile app should a COTS based app from the VMS provider being made available from the day 1 and must be easily be downloadable from IOS and Android stores online. Ability to display a geographic map with VMS entities geo-located on the map. Ability to view any camera configured on the map. Ability to search cameras or location on the map. Ability to view live and recorded video from the cameras of the central recording server. Ability to display live and recorded video side-by-side for a specific camera. Ability to perform digital zoom on cameras. Ability to perform actions on cameras such as add a bookmark, control a PTZ, control the iris/focus function, save a snapshot, start/stop recording. Ability to use the camera of the smartphone and stream a live video feed to a video recorder in the system. Ability to locate the mobile app user on map and provisioning to message and collaborate in real time with the central command center or field staff.	
2	It shall be possible to extend to the widgets of a dashboard using the SDK. This will provide the ability to develop custom widgets to the system.	
3	The VMS shall support the following actions on a dashboard: print dashboard, export dashboard to PNG file, and automatically email a report based on a schedule and a list of one or more recipients.	
4	The VMS shall support the following operations: Adding an IP device Updating an IP device Updating basic device parameters Adding/removing channels Adding/removing output signals Updating an IP channel Removing an IP device Enabling/disabling an IP channel	



	Refreshing an IP device (in case of firmware upgrade) Multicast at multiple aggregation points	
G	Community Surveillance Module:	
1	Architecture overview: The feeds city wide Surveillance system and feeds from Community surveillance (Invested by Public property owners in the premises) shall also be viewed at the Command & Control Center through the UC&C platform. It is envisaged that about 10,000 cameras from community surveillance feeds would be extended from various district police stations across the city of Delhi. The feeds from Community surveillance cameras could be fed into city UC & C platform through below 3 means and the solution must be ready to consume all the format of feeds and provide native intelligence within the UC & C platform – Through LAN / WAN from each community operator or a set of community operators to the nearest police station of each district and further federated to the Command & Control UC & C platform. The solution must be capable of viewing the streams both at the local police station levels or Viewing centers or other District police stations and Command centers. Community surveillance camera connected via Public cloud network and further connected to the Command center UC & C platform and VMS module. An Edge based intelligent IoT gateway solution with ability to sniff the CCTV feeds, which can be installed by community owners and streamed in to the District police stations or directly to the Command Center UC & C and VMS module. Such gateways streaming to either local District police stations or Central command center would be based on the availability of LAN / WAN connectivity and the architecture must be flexible enough to support both design possibilities.	
2	The UC & C and VMS module must be flexible to adapt all the possible architectures outlined above and the operators must get a unified view of the CCTV feeds irrespective of the architecture through which the community camera feeds are extended to Police network.	

4.8.3. Video Analytics

The Video Analytics shall offer a suite of analytics rules with Artificial Intelligence to provide automatic detection of a range of motion and non-motion behavior of persons, objects and vehicles.

There shall be a provision of Analytics and Artificial Intelligence through Machine and Deep learning solutions on video feeds received from at least 2500 cameras out of total envisaged number of cameras. There should be provision of 2 used cases (minimum) per camera.



4.8.4. Functional Requirements and KPIs- AI based Video Analytics process flow

- i. Each of the video analytics use case shall be able to run on a unified video intelligence platform of the system. Where the platform shall have the capability to support several multi-vendor/OEM video analytics applications that can be deployed on any camera or video-feed seamlessly.
- ii. Each of the video analytics use-case shall be structured as an independent module through dedicated SoP that can be deployed on any camera feed using a simple user interface utility, providing a complete visibility of the use cases and which cameras they are running on. The platform should have utility of scheduling each use case on individual camera.
- iii. The user should be able to easily select the camera by tag, groups or locations and schedule applications on any camera.
- iv. System will ingest Petabytes of Data in Storage Repository–
 - Intelligence inputs from field officers
 - Internet Data
 - Interrogation Reports
 - Criminal Records
 - Videos and Images from CCTV cameras, Satellites etc.
- v. Custom Predictive Models trained on client's training set (AI and ML Models) –
 - Similar criminal profiles
 - Similar events clusters
 - Alerts for specific crimes
 - Identify themes and trends
 - Track hotspots and dangerous areas
 - Force deployment
 - Sensitive Locations
- vi. Visual and Analytical platform to carry out analytics (Analysis) –
 - Track the complete profile of an individual
 - Track compromised assets
 - Track events and main suspects
 - Track organizations and their actions
 - Identify linkages between events and individuals
 - Identify chronology of an event
 - Charts and Reports to identify upcoming trends
- vii. Performance Indicators for the Video Analytics:



- Detection Rate (> 99%)
 - True Positive Rate + True Negative Rate (>95%)
 - False Positive Rate (<5%)
 - False Negative Rate (<5%)
- viii. All the scalability measures in terms of increase in no. of cameras or use-cases will be under the MSI responsibility.

KPI- Video Analytics (Use-Cases)

Video Analytics will be performed on metadata fields on a data lake of the envisaged system. The data will also be gathered from different datasets to be integrated. Big Data solution with its built Artificial Intelligence (AI) and Machine Learning (ML) algorithms will be capable of assisting Police Officials to work in tandem and collaborative manner in all three following scenarios:

- Retrospective (Post Incident),
- Preventive
- Predictive measures.

The various Analytic solutions as envisaged as an effective outcome of the system includes:

People detection

- The most important priority of city surveillance systems is on the people themselves focusing upon the prime objective of this project i.e. safety of Women and Children. The objective is to keep people safe and prevent accidents or criminal activities. Not all activities are easy to detect. For example, it is very difficult to detect if two people are fighting as this can take many different forms. However, many associated behaviors can be detected.
- For instance, if a person enters in any restricted area or any unattended baggage or kept beyond some threshold time etc. If crowds gather suddenly, this could be a symptom of some unusual activity as well. Having a system that can monitor various types of human behavior can help the city's officials ensure the safety of their citizens. The following can be the people driven use-cases:

a. Crowd Detection & Headcount

- The analytic should have the capability of detection of a crowd within the Field of View of the camera. It should be possible for the operator to define the number of persons including gender identification within the crowd scenario.
- The analytic should generate the crowd formation alert with estimate of the number of persons in the crowd based on the headcount.
- Based on the trend evaluations for the defined area on the criminal and suspicious activities, predictive analyses should be performed for effective forecasting towards possible threat bearing activities towards Women and Children.

b. Person Falling Detection

The analytic should detect the person falling all of a sudden in the field of view of the camera and does not get up within the pre-configured duration of time. The analytic should be able to detect one or more persons falling simultaneously.



c. Protection and security towards women in isolation

The analytics will ensure suspicious behavior activity for women in isolation/ deserted area or possibly when traced surrounded by men in such identified places.

Also, the women raising and waving hand in such aforementioned situations will be tracked and alert will be generated at ICCV Platform for immediate extension of SoS help.

Vehicular analytics

a. Automatic Number Plate Recognition (ANPR- Vehicle Surveillance)

Through the inputs received from ANPR cameras, the system should capture the number plate of two-wheeler and four-wheeler vehicles. The analytic should be able to:

- Read and convert the license plate number into a text string of the vehicle with 95% detection accuracy.
- Store the JPEG image of the license plate in the database with other metadata such as time stamp, location, camera, etc.
- Classify the vehicles in categories such as four-wheeler light and heavy motor vehicles, three wheelers, auto rickshaws and two wheelers
- Detect colour of the vehicle (in day time)
- Set separate recording duration for event information (number plate as text), media clips (pre and post event recording) and ANPR- VEHICLE SURVEILLANCE picture snapshot.
- Software should also raise an alert in case of any vehicle not having any number plate.

b. Suspect Vehicle Detection

It should be possible to store the number plates of the vehicles under various lists such as stolen, suspicious, blacklisted, etc. The analytic should detect such vehicles in the field of view of the cameras in real time by matching the number plate.

c. Vehicle Search

The analytic should provide the feature to search the vehicles based on the attributes that includes number plate (partial or full), class of the vehicle (four-wheeler light and heavy motor vehicles, three wheelers, auto rickshaws and two wheelers, etc.), color of the vehicle and location.

d. Missing Number Plate Detection

- The system should be able to detect if there is any vehicle in the camera view without a properly installed number plate or no number plate at all.
- The system should have capability to let the user search for all such vehicles through a UI based filtering system.



- The user should be able to search and track any such vehicle using various vehicle as mentioned above.

Health monitoring of Field Cameras and Network

There will be a policy defined management at the central level (Data Center) for continuous health monitoring of field level devices and the network layer of the architecture.

- **Camera Status:** The Camera Health Monitoring application should be able to monitor the status of the camera and report an alert in case the camera is not functional or tampered with intentionally or unintentionally.
- **View Obstruction:** It should detect and raise an alert if the camera view is obstructed by any foreign object. The user should be able to adjust the threshold parameters of extent of obstruction in terms of percentage of camera view
- **Bright Light Shown:** The app should be able to detect and raise an alert if the camera view is tampered with bright lights. The system should specifically identify it as a camera tampering event with light shining.
- **Camera View Changed:** It should raise an alert if the camera view is changed/moved suddenly.
- **Illumination Too Low:** It should raise an alert if the camera scenes gets too dark below a threshold.
- **Camera Connectivity:** It should raise an alert if the camera is turned off or connectivity is lost.
- The proposed solution must automatically discover manageable elements connected to the network and map the connectivity between them. The Network Fault Management consoles must provide the topology map view from a single central console.
- The proposed solution must automatically discover manageable elements connected to the network and map the connectivity between them. The Network Fault Management consoles must provide the topology map view from a single central console.
- The proposed system must support multiple types of discovery including IP range discovery, Seed router-based discovery & Trap-Based Discovery
- The system should provide discovery & inventory of heterogeneous physical network devices like Layer-2 & Layer-3 switches, Routers and other IP devices and do mapping of LAN & WAN connectivity with granular visibility up to individual ports level.
- The system must be able to support mapping and modelling of the infrastructure grouped by network connectivity, physical location of equipment and user groups



Analytics for Police Investigation Support

a. Investigation Scene Rebuilding

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.

b. Smart Archived Video Search

- The investigation feature should provide the feature to select a region within the field of view of the camera to show only the frames pertaining to the motion detected in the selected region.
- It should also have a feature to search the archived video based on the image thumbnails.

Predictive Analytics through Media Platforms

- It is envisaged to have a unique state-of-art multi-dimensional analytics solution for women and child safety in Delhi. The solution combines, Telecom CDRs, videos & facial images from surveillance cameras, social media data points, enterprise search from varied range of datasets including RTO, ITMS data, etc.
- With regards to the location details of a target or a person under threat needing help, these multi-dimensional data points will be processed and analysed in real time on Big Data Analytics platform at the C4i.
- The following cross domain analytics will bring down the response time drastically, thereby increasing the probability of aversion of crime against women, children, old-aged and differently-abled people.

a. Call Detail Record (CDR)- On request Basis: This will cover the following features:

- Analyses date, time and location of voice calls made & received, nos. which went silent after incident, location trail of suspects, and link analysis of calls made and received by victims and suspects.
- Analysis of call dumps of a particular Telecom tower or group of towers in the vicinity of incident location.
- The suspect nos. from this solution can be fed to Video Analytics to check for visuals and near real time location trail and vice versa.
- This will be catered through ERSS/ Dial 112 application.

b. Enterprise Search

It enables Police Personnel to carry out unified intelligent search across multiple data silos and disparate databases to check for criminal or questionable background across different State and central records, modus operandi, FIRs, jail records, immigration entries, hospital treatments, RTO records, etc. Alerts can be generated and sent across the mapped hierarchies of officials to take time bound decisions and actions.



VA- Technical Requirements and Compliance Sheet for MSI (to provide compliance report with the bid)

AI based Video Analytics - Overall System Specifications			
S No.	Key	Description	Compliance (Yes/ No) with comments, if any
1	Unified Video Intelligence platform	Each of the video analytics use case shall be able to run on a unified video intelligence platform. Where the system shall have the capability to support several multi-vendor/OEM video analytics applications that can be deployed on any camera or video-feed seamlessly.	
2	Dynamic Deployment	Each of the video analytics use-case shall be structured as an independent module that can be deployed on any camera using a simple user interface utility, providing a complete visibility of the use cases and which cameras they are running on. The platform should have utility of scheduling each use case on individual camera. The user should be able to easily select the camera by tag, groups or locations and schedule applications on any camera.	
3	Advanced AI compatible	The Video Analytics system shall be compatible with the latest technological advancements in the domain of computer vision and AI. Hence, it shall be able to quickly adapt to newer libraries and AI advancements. All the analytics and use-cases shall be based on advanced AI technology, and shall not depend on traditional algorithms.	
4	Libraries and frameworks	The system shall be fully compatible with popular Computer Vision and Artificial Intelligence frameworks including but not limited to such as OpenCV, OpenVINO, Tensorflow, Caffe, Pytorch, MXNet, TensorRT, Keras and Darknet. from day one	
5	Training models new	The system shall allow seamless training by labelling any objects within the images and providing them suitable attributes of multiple types such as class, subclass, color, type etc. The	



		system shall allow training to happen continuously, on demand or on periodic intervals, which shall be configurable.	
6	Annotation	The system shall have an inbuilt annotation tool that allows a user to label the images with relevant information using both rectangle and polygon drawing facilities. The annotation should allow labeling of images or drawn objects with different class names. In case of persons, it should also support labeling of various attributes such as color of clothing, type of clothing, age, gender etc. as well. The annotation tool should have a comprehensive project management feature, including assigning annotation jobs on a set of images to individual users. The system should also have support for higher privileged users who can approve/disapprove the annotations done by the annotators. The user should be able to train new deep-learning models from the annotated data using the Annotation UI itself. The user-interface should allow to plug-in the trained model in any of the relevant Video Analytics use-cases dynamically at each camera. The system should allow the user to plug newly trained AI models at runtime by simply selecting the models in the per-camera configuration page	
7	Model Comparison	The System shall have a library of standardized AI models developed by the OEM of the Video Analytics System, academic institutions and members of the developer community. These models shall be used for comparing and benchmarking the performance of newly developed models. The system shall allow for both qualitative and quantitative comparison of models, i.e. it shall allow the end user to compare individual parameters of the model (such as learning rate) as well as the overall performance of the model on any given dataset when compared to a standardized model.	



8	Monitoring and analytics	Autonomously objective metrics shall be available to be evaluated and Insights into the performance of each algorithm, model and their versions shall be made available to key stakeholders or users as defined. Visual map of composition, workflow, usage analytics, resource utilization, failure points etc. would be made available to provide complete control of A.I. workload.	
9	Unsupervised deep learning methods	The system shall be able to use algorithms and unsupervised deep learning methods to provide alerts and useful actionable insights from live streaming video feed data. System shall have capability to automatically analyze hours of video data for defining own rule.	
10	Self-learning Capabilities	The system shall be capable of fully self-learning with no initial programming input by the end user. The solution shall learn what normal behavior is for people, vehicles, machines, etc. and the environment based on its own observation of patterns of various characteristics such as size, speed, reflectivity, color, grouping, vertical or horizontal orientation and so forth.	
11	Key UI View and functionalities	The System shall provide the following key results from the use case	
		Event Notifications: The result of each of the use case shall be in the form of events that contain the screenshot with other metadata describing the event, such as detected objects, timestamp, camera/video that generated the event and all other metadata representing the event from different use cases. The User Interface shall have a grid and list view with all the events from different use cases, cameras etc. These features should be supported through a mobile application to be utilized by various field users. The system should support customization of alerts, video feeds, and priority-based alerts for individual users from day one.	
		Resource Management View: The User interface shall provide a list of all the resources available in the system such as computing servers and cameras. The status of each of the devices, whether	



		they are online/offline shall also be available at all times.	
		AI Training Tool: The User interface shall have a training tool to annotate and label images from the events to train new AI models and update the existing ones. The training tools shall also contain a list of all the models available in the system, which can be plugged into any AI use case easily.	
		Use case deployment matrix: The user interface shall have a matrix to assign, start, stop and schedule any use case on any camera. The status of active and non-active use cases shall be clearly visible with color coded information. All the licenses should be able to operate in floating mode for all cameras.	
		Data Analytics Dashboard: The user interface shall also have an analytics dashboard listing all the patterns of events from different cameras with a heat-map of number of events on an hourly basis.	
		Picture Intelligence Unit – UI Interface and Functional requirements: Video Intelligence platform should have inbuilt intelligence capabilities to deliver the analytics requirement of the PIU. This is envisaged to be a video forensic unit/ R&D Setup for Video Content Analysis. It will use live camera feeds, criminal and crime scene photographs/ videos etc. as evidence. It will ensure video analytics, continuous time stamp and non-tampering of electronic evidence as per laws.	
		Video Synopsys UI- The Video Intelligence shall provide an intuitive UI for Vide Synopsys. Able to analyze all the recorded video files and provide the operator with synopsis video for quick review and investigation thereby reducing viewing time considerably. The video files from all the 3rd Party Video Management Software (VMS) shall be supported.	
12	Common UI for all the use-cases	The user interface shall be a unified dashboard that shows events from all the Video Analytics use-cases and all the cameras in a common UI, and	



		which gets populated in real time from event notifications.	
13	Web Interface based	The User interface of the system shall be a web interface that can be accessed from any system in the local area network with login credentials. It shall allow multiple users to log in at the same time, and receive real-time alerts and notifications.	
14	Live Video Interface	The User interface shall allow a user to view the live video stream from any camera with overlaid information of regions, objects, people and vehicles based on each of the use-case	
15	Configuration per-use-case per-camera level	The system shall allow each use-case to be uniquely configured for every individual camera stream, with parameters for camera calibration, image quality improvement, night/day settings etc.	
		Each use-case shall be able to run on different cameras with different settings (e.g., different Zones for Intrusion, different lines for line crossing detection, etc.) at different hours of the day.	
		The configuration page shall allow a user to choose any of the available AI models to detect and classify objects within the image. The description of the models shall clearly specify performance and hardware requirements of each of the model.	
16	Camera Calibration Tool	The Video Analytics system UI should have an in-build camera-calibration tool that can take user inputs such as reference-heights, reference depths and floor landmarks to calibrate the camera. The calibration tool should have an option to use the GPS coordinates of the camera location. Once the camera is calibrated, each detected object should also be assigned real-world coordinates with respect to the Camera GPS coordinates. This functionality should be available for each camera added in the VA system The OEM should ensure that there should not be any geometric distortions on the deployed cameras.	
17		The use case on each camera shall allow setting up configuration of multiple detections zones such as	



	Key configuration parameters	lines and regions that can be used to define perimeters, regions of interest.	
		The configuration user interface shall allow adjusting various sensitivity and confidence parameters to adjust each video-analytics use-case's performance with respect to the physical deployment of the camera.	
18	Filtering and Retrieval	The system shall allow a user to filter and retrieve all the events based on any combination of the following parameters: - Time of the event - Objects in the event - Type of the use-case - Camera Location etc.	
19	Transparent and Open Architecture	The architecture shall clearly demonstrate the technology stack with layers of the core platform, data governance and interface to different software applications.	
20	Highly parallel and distributed	The algorithms powering the video intelligence system shall possess capability to operate parallel and distributed manner across a cluster of machines. Both training of AI algorithms and inference shall be distributed.	
21	User Management	The system shall support user with a hierarchical access level, with different access level for different users demarcated with respect to cameras, locations and the data. The user access control system shall allow setting of SOP's like CRUD (Create, Read, Update and Delete) operations for each user.	
22	Deployment of use-case across any camera	The system shall allow deployment of any use case on any camera without any MAC level or IP level locking. Ideally any use case shall be deployable and redeploy able on any camera or video source as far as the camera view supports such use cases to be deployed.	
23	Video Compatibility	The System shall be a real-time video analytics engine that utilizes advanced image processing algorithms to turn video into actionable intelligence. The AI based Video Analytics system shall consist of video-processing & analytics engine	



		that works seamlessly both on saved videos or camera streams in real-time and provide events to the user based on the use-case basis. The system shall be compatible with all ONVIF compliant IP cameras with H.264/H.265 video decoding.	
24	Centralized Deployment Support	All the video streams shall be processed centrally at the Data Center with one or more servers for video processing. The user shall be able to log in to the system through the central dashboard to access all the data from all the servers. The processing of videos as well as alert generation shall be done on premise. At no point in time shall the data from the site be shared over the internet or sent over to the cloud. The System UI shall only be accessible using workstations and terminals available on premises.	
25	Support for third-party use-cases	The AI system shall also support third-party developed algorithms and use-cases that can provide the user with a large base of use-cases to choose from.	
		If a new use-case needs to be developed based on Video Intelligence, the system shall provide a developer Software Development Kit (SDK) for this purpose. The SDK shall be provided along with detailed documentation for building end-to-end use-cases on the system.	
		The system shall also allow the user to plug different AI models in the individual running of the video analytics use-case.	
26	Flexible Technology Stack	The technology stack shall be modular and scalable based on containerized micro services. Each use-case shall be orchestrated as a stand-alone micro service, which communicates with a central server for exchanging of the data.	
		A.I. micro services components shall be agnostic to language used in technology stack. It shall work with any language, framework, and library of choice without any impact on the rest of the architecture. This type of flexibility will ensure lower friction for collaboration and deployment of AI.	



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



		The analytics events shall be stored in the database. In case the events are purged, the purged events stored to external files for later reference.	
		For Vehicular and ANPR Analytics, it is possible to deploy the analytics in centralized architecture where all the feeds from the cameras are available in the Data Center and analyzed centrally.	
		The system shall have a single client application for setting analytics, live viewing, archived viewing and the administrator functions.	
28	VA Accuracy Parameter	Accuracy may be evaluated using following KPIs: a. Detection Rate (> 99%) b. True Positive Rate + True Negative Rate (>95%) c. False Positive Rate (<5%) d. False Negative Rate (<5%)	
		There should have feature to improve the accuracy overtime with further continuous learning and also based on the input received from the field officer's incident reports (captured by the system and matrix generated through the system rather than the manual exercise) and improvement of AI models. The OEM should take this feedback and upgrade the algorithm to show accuracy improvement quarterly basis.	

Video Analytics Use Case Specifications: -			
A. AI based Crowd Estimation and Management			
S. No.	Key	Description	Compliance (Yes/ No) with comments, if any
1	Introduction	Crowd Estimation and Management (CEM) Video Intelligence system shall allow estimation of crowd density within the camera view. This is an important tool for understanding the crowd movement and management for the security and facilities management agencies. System shall raise an alert if the crowd density within a camera view is above a certain threshold.	
2	Deployment	The CEM System shall be a purely computer vision and artificial intelligence-based system that be deployed on all	



		the existing and new CCTV cameras, including box cameras and PTZ cameras.	
3	Camera compatibility	The system shall be completely independent of the make/model of the cameras and be compatible with ONVIF compliant cameras. The CEM system shall support H264, H264+, H265 and MJPEG video streaming from cameras.	
4	Accuracy on datasets	The CEM system shall have 85% average accuracy in estimation of crowd on public databases and/or real time situation to be given during proof of concept time	
5	Ability to define regions	The CEM system shall have an ability to annotate multiple regions within the camera view and the user shall be able to specify crowd thresholds for each of the regions separately. If within any region the crowd density estimation is above the user defined threshold, the system shall raise an alert.	
6	Alerts	The system shall raise alerts in case of the following: - The CEM system shall raise an alert if the density of crowd is above a user-defined threshold. - The system shall raise an alert in case of erratic movement detected within the crowd - The system shall raise an alert if there is any chance of stampede or overcrowding due to increase in flow rate and erratic movement - The system shall trigger alarm if more than desired density is observed near specified regions of interest.	
7	Crowd flow estimation data	The CEM system shall also provide a data of crowd flow from one user-defined region to the other, in case of two regions selected by the user.	
8	Data representation	The CEM system shall have an MIS system with a detailed report and dashboard on crowding events and data at a minimum of hourly granularity. - The system shall report Crowd Density and direction to load-balance various gates. - The system shall provide detailed counts of total visitors in hourly/daily/weekly/monthly and overall. - The system shall also provide IN and OUT counters for all the visitors	
9	Heat Maps	The CEM system shall have an option of generating real time heat maps of crowd density.	



B. AI Based Camera Health Monitoring			
S. No.	Key	Description	Compliance (Yes/ No) with comments, if any
1	Camera Status	The Camera Health Monitoring app should be able to monitor the status of the camera and report an alert in case the camera is not functional or tampered with intentionally or unintentionally.	
2	View Obstruction	It should detect and raise an alert if the camera view is obstructed by any foreign object. The user should be able to adjust the threshold parameters of extent of obstruction in terms of percentage of camera view	
3	Bright Light Shown	The app should be able to detect and raise an alert if the camera view is tampered with bright lights. The system should specifically identify it as a camera tampering event with light shining.	
4	Camera View Changed	It should raise an alert if the camera view is changed/moved suddenly.	
5	Illumination Too Low	It should raise an alert if the camera scenes gets too dark below a threshold.	
6	Camera Connectivity	It should raise an alert if the camera is turned off or connectivity is lost.	
7	Notification with Health Type	The health monitoring app should notify the user with the type of camera health issue, namely: View Obstruction, Bright Light Shown, Camera View Changed, Low Illumination and loss of connectivity	
8	Sensitivity Management	It should have provision to adjust the sensitivity of detection on each camera	
C. App Specification - Abandoned Object			
S. No.	Key	Description	Compliance (Yes/ No) with comments, if any
1	Detections	The system shall be capable of detecting left objects that have remained stationary for a period of time that is considered suspicious by the user.	
2		The system shall be capable of performing the left object detection despite drastic light changes and the casting of shadows in front of the left objects.	



3	Multiple object detection	The system shall have the ability to detect multiple objects that are left stationary in a scene.	
4		The system shall be able to detect multiple objects each with its own timer as per the defined detection time. If multiple objects are abandoned in the scene one after the other and alarm shall be raised for each object (one after the other) once that object has been left in the scene for longer than the detection time.	
5	Configuration of detection time	The user shall have the ability to configure the detection time to suit the environment.	
6	Event Review	The system shall be able to immediately review the event (with a click of a single jump- to-event button) to recognize the person who has left the object.	
D. App Specification – Person Collapsing			
S. No.	Key	Description	Compliance (Yes/ No) with comments, if any
1	App detection	The app should detect if a person walking upright has collapsed or fallen on the ground.	
2	Configurable parameters	The user should be able to configure the amount of time beyond which if the person is on the ground, the system should raise an alert.	
3	App Reporting	This app should raise an alert if any pedestrian is Jay walking. The app should provide zone wise data of both the pedestrian movements at zebra crossings and jay walking with a minimum of hourly granularity.	

4.8.5. Video summarization and Analysis Functional Requirements & KPIs:

- Artificial Intelligence based video analytics are crucial to increase efficiency of proposed Integrated Command & Control Center being built as part of Delhi Safe City Project. These live video feeds and responses to incidents reported needs to be analysed for better policing. Artificial Intelligence (AI) based analytics that can handle “Active Surveillance”. This specific section covers the technical use case aspects of “AI-based Video Review & Investigation System”
- The proposed solution should help in making Video Searchable, Quantifiable and Actionable, reviewing long duration of video in short time; quantitatively analyse video to derive actionable insights for data driven safety, security and operational



decision making. The proposed system should be state of the art image processing technology essentially creating condensed summaries of original, full length video recordings, while preserving all objects and events of interest. These should be presented either simultaneously or in rapid succession, regardless of the time point and sequence in which they occurred, effectively providing operators with a clear view of activities and enabling them to rapidly review and home in on events of interest.

- iii. While keeping human operators "in the loop" the system should provide operators, what they need to quickly scan through video data to find suspicious, out of the ordinary or potentially criminal aspects. After detecting an object of interest, the user shall be able to select to see the object in its original form in the original video which can then be exported.
- iv. Video Summarization tool based on attributes and meta data field will facilitate to reach to relevant and meaningful content for the defined search meeting the requirements for effective post investigation analyses within shorter time span.

Video Summarization- Technical Requirements and Compliance Sheet for MSI (to provide compliance report with the bid)

Sr. No.	Specification	Compliance (Yes/No) with comments, if any
1.	System shall be able to analyze all the recorded video files and provide the operator with Summarization video for quick review and investigation thereby reducing viewing time considerably. The video files from all the 3rd Party Video Management Software (VMS) shall be supported.	
2.	System shall support: - Investigation case management Video summarization (extraction and superimposition of video objects over original scenes to allow simultaneous display of events that occurred at different times) Multi-camera search, enabling the pinpointing of objects of interest via appearance similarity as well as a broad range of filter Presets.	
3.	Multi-camera search, enabling the pinpointing of objects of interest via appearance similarity as well as a broad range of filter Pre-sets.	
4.	Shall support Video File exports from all kind of 3rd Party VMS and even the video files recorded from a Mobile Or any other kind of Analog Camera.	
5.	System shall be able to enhance safety and security with quick rapid human response to critical events recorded on video	
6.	Shall support Video File exports from all kind of 3rd Party VMS and even the video files recorded from a Mobile Or any other kind of Analog Camera.	



7.	Shall automatically extracts objects from the original video and efficiently reconstructs and superimposes them back in the original scene, simultaneously displaying events that have occurred at different times.	
8.	System shall rapidly pinpoint people and vehicles of interest, using an extensive range of appearance and movement filters, across multiple video sources from different cameras installed in the premises.	
9.	Shall Instantly locate people, vehicles, and items of interest by searching for similar looking objects.	
10.	System shall display time-stamps for various objects in the video continuously, while the summarization is played.	
11.	Shall provide a web-browser (Preferably Google Chrome) interface to upload the video files, generate the Summarization & for the management of multiple investigation cases	
12.	System shall provide density control while replaying the Summarization video. Density refers to the number of events shown concurrently when playing a Summarization. The density control shall increase or decrease the number of events shown at once also changing the event density shall alter the run time duration of the video Summarization thereby enabling quick review time.	
13.	Time Range - Limit the search criteria to specific time ranges	
14.	Source - Limit objects to specific cameras or files	
15.	Class - Video Summarization shall be shown based on People, Two-Wheeled Vehicles, Other Vehicles and Animals - People Class: Man, Woman and child. - Two-Wheeled Vehicle Class: Bicycle and Motorcycle - Other Vehicles Class: Car, Pickup, Van, Truck, Bus, Train, Airplane, and Boat	
16.	attributes - Shall be able to select the attributes within a class to refine the search - Bags: Backpacks, Hand-held Bags - Hats: Hats, No Hats - Upper Wear: Short/No Sleeves, Long Sleeves - Lower Wear: Long, Short	
17.	Colour - Identify objects according to any combination of Brown, Red, Orange, Yellow, Green, Lime, Cyan, Purple, Pink, White, Grey and Black	
18.	Size - Select objects based on their actual (real-life) size from a histogram of sizes relevant to a specific case	
19.	Speed - Select objects based on their actual speed from a histogram of speeds relevant to a specific case	



20.	Dwell - Select objects dwelling for longer than a certain period in a scene	
21.	Area - Identify objects included or excluded within one or more user-defined 3- or 4-sided polygon areas. The user shall be able to set the minimum duration the object spends inside the area.	
22.	Path - Identify objects traveling along one or more user-defined paths. The user shall be able to set the minimum duration the object spends inside the area.	
23.	Appearance similarity – System shall be able to do filter and display only the objects matching similar-looking people (People Similarity) or Vehicles (Vehicle Similarity).	
24.	Supported Video Resolution – Minimum CIF and Maximum 4K	
25.	Visual Layers – System shall provide statistical visual analysis of object activity & dwell areas and popular event paths in a Summarization.	
26.	Supported Frame Rate – 8-30 FPS	
27.	Shall support video file formats like .AVI, .MKV, .MPEG4, MOV, WMV, DVR, ASF, RT4, DIVX, .264, .H264, .H265, .GE5, .TS, .3GP	

4.8.6. Facial Recognition System

Functional Requirements:

- i. The FRS application shall install for the cameras positioned at the entry/ exits of public places/ city, High Security Areas, Places of Worship, etc.
- ii. There will be 370 cameras across all the cameras identified for FRS application at any point of time. The licenses/ channels acquired for FRS application will be used to randomly select any camera out of 6121 cameras (for Video Analytics) to run FRS limited to 2 cameras per Police Station (370 Nos.) cameras simultaneously.
- iii. **Analyses on Video and Facial Images:** This will cover the following features:
 - It analyses facial images to match with suspects/targets and victims and raise alerts in the event of match. The solution will be capable of capturing facial images at distance 15 to 20 ft. and even at tilted angles of incidence unlike other solution requiring direct facing incident images.
 - The solution will have many built in algorithms like detecting crowd movement in a particular direction, presence or absence in a frame alert, tracking movement of target/suspect or victim across multiple camera locations and raising alert.
 - Alone female /child present in a frame. Identified suspects or victim's identity can be searched through Enterprise search, and fed to social media analytics/CDR analytics for cross domain analytics.
- iv. The height of the camera from Ground / Floor shall be 8-10 feet.
- v. Capture zone to be channelized to capture Frontal Face of the people. Although, one caught, the application should have the capability to make minimum 15 iterations with different illumination levels and varied angles.



- vi. As a precautionary measure the camera should not be placed/ pointed directly to strong light sources like sunlight, headlight or spotlight.
- vii. Face Recognition System shall work on real time and offline mode.
- viii. The system shall have the best suited technology employed for 1:1 (one to one) and 1: N (one to many) matching applications for various purposes.

KPI- Facial Recognition System

- i. The areas for which the camera feed will be used as input for FRS module will be identified considering:
 - Highly prone area for criminal activities against women, child, elderly people as per criminal records;
 - Public places with substantial walking head-counts
 - High Security zones and a few Government Offices under critical surveillance
 - Accuracy in bad lightening and weather conditions may be evaluated using following KPIs:
 - Detection Rate (> 70-80%)
 - True Positive Rate + True Negative Rate (>75%)
 - False Positive Rate (<25%)
 - False Negative Rate (<25%)
- ii. FRS should be able to
 - integrate with CCTNS & other databases,
 - generate Alerts based on predefined parameters
 - integrate with watch list
 - search on-line and off-line in video and images
 - Generate Reports and Manage data
- iii. Other essential KPIs:

Sr No	Aspect
1	Measuring following KPI (Key Performance Indicators) 1. Detection Rate 2. Number of True Positives 3. Number of False Positives 4. Number of True Negatives 5. Number of False Negatives All vendors will be provided with a recorded video to ensure common ground along with suspects who can be enrolled. Above outcomes will be measured and compared among all vendors to check the accuracy.
2	Measuring following KPI (Key Performance Indicators) 1. Detection Rate 2. Number of True Positives 3. Number of False Positives 4. Number of True Negatives 5. Number of False Negatives



	All vendors will be provided with a live stream with similar Field of View to ensure common ground along with suspects who can be enrolled. Above outcomes will be measured and compared among all vendors to check the accuracy.
3	Simultaneous detection of multiple faces in crowd: All vendors will be provided with a crowded video and outcomes will be recorded.
4	Deep Learning based algorithm: All vendors will have to demonstrate learning capabilities within their algorithm.
5	Global Threshold, Camera wise threshold and watch list wise threshold
6	Real Time back search for newly enrolled subjects
7	Video & Image evidence of suspects
8	Easy Monitoring of System Health
9	Multiple detections to be collated using intuitive methods
10	Privacy as per GDPR compliance
11	Integration with leading VMS vendors
12	Integration with any sensor

FRS- Technical Requirements and Compliance Sheet for MSI (to provide compliance report with the bid)

S No.	Key	Description	Compliance (Yes/ No) with comments, if any
1.	Detection	Face Recognition System shall work on real time and offline mode for identifying or verifying a person from various kinds of inputs from digital image file and live video source from any IP video streaming sensor like IP Camera, Body Worn Cameras, Mobile handset cameras, UAV/Drones etc.	
2.	Deep Learning Technology	FRS must be a latest generation Convolutional Neural Networks based facial and person tracking technology with Real-time 1:1 (one to one), 1: N (one to many) and N:N (many to many) matching application for various purposes for non- voluntary face detection & recognition in the open crowded scenarios.	
3.	Live and Offline Mode	FRS shall be able to capture face images from live & pre-recorded CCTV feeds received and generate alerts if a blacklist (face from suspect list) match is found.	



S No.	Key	Description	Compliance (Yes/ No) with comments, if any
4.	Detections in crowd	The system shall be able work to detect more than 20 faces in crowd on moderate face rotation either horizontal or vertical. It should support a yaw angle of -40 to +40 degrees , a pitch angle of -30 to +30 degrees and a roll angle of -30 to +30 degrees.	
5.	Detection of partial faces	The FRS shall recognize partial faces with varying angles from multiple videos simultaneously from Video clips, Group Photographs and VMS Playback directly from FRS Client Interface. FRS shall be able to process uploaded pre-recorded video feeds with a speed of up to X20, depending on the proposed hosting hardware and the video quality	
6.	Ability to add reference Images	The system shall be able to add photographs obtained from law enforcement agencies to the criminals' repositories tagged for sex, age, scars, tattoos etc. for future searches.	
7.	Support for cameras/video formats	The system shall support diverse graphic & video formats as well as live cameras. FRS shall support day/night operation with ability to detect faces both in colour and in black/white mode by using any H.264, H.265 Fixed IP and PTZ Cameras with IR Illuminators without any special configurations required	
8.	User-management	FRS must support a user management module that enables different user level groups to support various permission levels.	
		FRS client shall have ability to share recognition data like images & videos with multiple users and operators for better reference, alarm & incident management.	
9.	Image Enhancement Capabilities	FRS system must have capability to enroll whatever images fed in the system with image enhancement and ability to verify the quality of the enrolled images with different colour indicator for low quality images enrolled in watch list/database.	
10.	Image Format support	The system shall be able to utilize any of the file formats like JPEG, PNG, BMP, TIFF etc. format for enrolment.	



S No.	Key	Description	Compliance (Yes/ No) with comments, if any
11.	De-duplication	FRS shall be able to check if new enrolled face is already enrolled in the database before registering the new enrolled face in the system. Also, the system shall be able to find a previous detection of a POI (person of interest) upon enrolment to watch list (retrospective search) in less than 2 sec.	
12.	Enrolment of faces	The system shall have option to automatically enroll face images from CCTV cameras/video source. This functionality should also be provided through the Video Intelligence platform in addition to the FRS application. The system should also have an option for Bulk Enrollment either from file system or a 3rd party databases such as UID, SAARTHI, IT, NCRB, EPIC etc.	
13.	Categories of database faces	The system shall have capacity to create different categories of people with option to customize the matching threshold for different categories.	
14.	Full HD Support	The system shall be able to work on full HD Camera video with maximum performance.	
15.	Implementation	The system shall be able to be implemented on IT hardware like Server or Workstation.	
16.	OS Support	The FRS algorithm should be able to use proven open source tools and technologies like Linux to bring down the total cost of ownership of the solution. FRS running on any other OS should be supplied with Pre-Licensed Server based latest version OS like Microsoft Server 2016 and Microsoft SQL as needed by the application	
17.	Database Support	The system shall employ database system like MS SQL/ MYQL/ Leading Open Source Database/Sybase/ Mongo DB/ Postgres/Oracle etc. The FRS system should natively integrate with Video Intelligence platform and use a common database of the platform, so that common queries can be made on the common database for faces detection and other events.	



S No.	Key	Description	Compliance (Yes/ No) with comments, if any
18.	Algorithm Benchmarking	The Vendor should have any performance benchmarking certificate. NIST certificate will be preferred.	
19.	Performance	The system must perform a full 1: N search of the probe image in under 5 seconds against a database of up to 50 mn face records.	
20.	Mobile Application Support	FRS Software vendor shall have mobile application of the same FRS software to support iOS and android based smart field devices. Mobile application shall be capturing the face of suspect in field and sending back to the FRS server for matching. Matching result shall be shown on the mobile application screen with matching score. There shall be provision in mobile application to stream mobile device camera as video streamer.	
21.	Detection robustness	System shall be able to detect the faces across the multiple CCTV video sources for online (real-time) and offline modes regardless of following conditions:	
		a. Changes in Facial expression	
		b. Changes in facial hair or hairstyle	
		c. Changes by moderate aging (up to 15 years)	
		d. Partially hidden faces or occluded faces like wearing dark glasses mask etc.	
		e. Changes in lighting conditions	
22.	Search Capabilities	Simple Search UI that facilitates quick and easy access to the collection of events recorded by the system without the constant monitoring by operators and must perform a full 1: N search of the probe image in under 2 seconds against a database of up to 5-8 Million POIs. It shall support following	
		a. Search previous events by images from previous detections	
		b. Search previous events by images uploaded by operator	
		c. Search previous events by enrolled names	
		d. Search previous events by date and time	
		e. Search previous events by watch list group	
		f. Search in Watch list by image	



S No.	Key	Description	Compliance (Yes/ No) with comments, if any
23.	Retrospective Search	FRS shall have capability of Search backwards for previous detections and/or recognitions (events) of the detected person without enrolment from live CCTV & other forensic videos / offline videos	
24.	Up to 5 nearest matches support	FRS shall have ranking features to show next 5 closest & similar subjects in the Watch list with nearest score to the detection. This option enables you to review POIs that are potential matches for this detection for efficient system performance.	
25.	OEM owned algorithm	The FRS OEM should have ownership of Face Recognition Engine /Algorithm for any custom specific development as required by client	
26.	Map feature	FRS must allow tracking of person on maps to be uploaded in the system for cameras connected to FRS and shall highlight the camera location on the map for each detection/alert.	
27.	SDK/API for integration	FRS shall provide an SDK/API for integration with any third-party software like C4I (Command, Control Communication & Compute Center). API must be available with a full set of documentation of each method with accompanying sample code. All FRS function shall be fully accessible via API.	
28.	Video Alert	FRS shall be able to play a short video clip of the moment of face detection without dependency on VMS which can be downloaded/exported/saved for evidence proof	
29.	Timeline of detections	FRS shall provide timeline sequence of all detections of subject with date, time & location.	



S No.	Key	Description	Compliance (Yes/ No) with comments, if any
30.	Email Integration	FRS shall support email Alerts via Gmail, Outlook or via an Exchange SMTP service. Different recipients can be defined for different Camera Groups. User shall be able to define how frequently recognition/detection emails are sent, the email subject and the email sender (among other things). The email itself includes the timestamp of the detection, the score, the description, the reference image (defined in the Watch list) and the detected image.	
31.	Minimum hardware support	FRS Application Engine must be able to run a minimum of 20 FRS Camera Channels per Server. (Server with 128 GB RAM, 3 NVIDIA Tesla T4 card with 40 cores.) Other optimized and better sizing shall be accepted.	
32.	Use of AI accelerator hardware	FRS shall use extensive AI Technology and perform video processing on GPUs like NVIDIA; INTEL or similar as per design & sizing vetted by AI FRS Algorithm OEM. The number of servers to be supplied, shall be based on the number of camera channels on which the FRS needs to be performed.	

4.8.7. Automatic Number Plate Recognition (ANPR) S/W - Vehicle Surveillance Functional Requirements & KPIs

The System shall automatically detect a vehicle in the camera view using video detection and activate license plate recognition.

The System shall automatically detect the license plate in the captured video feed in real-time.

The system shall perform OCR (optical character recognition) on characters of the license plate (English alpha-numeric characters in standard fonts).

The ANPR system should work on 95% accuracy parameters for capturing and 90% accuracy of OCR on the standard fonts.

The System shall store JPEG image of vehicle and license plate and enter the license plate number into PostgreSQL database along with date time stamp and site location details.

System shall be able to detect and recognize the English alpha numeric License plate in standard fonts and formats of all vehicles including cars, HCV, and LCV.

The system shall be able to process and read number plates of vehicles with speed up to 120 km/hr. or above.



The system shall be robust to variation in License Plates in terms of font, size, contrast and color and shall work with good accuracy.

The system shall support Black list / White list configuration: The system shall have option to input certain license plates according to the hot listed categories like “Wanted”, “Suspicious”, “Stolen”, etc. by authorized personnel

The system shall be able to generate automatic alarms to alert the control room personnel for further action, in the event of detection of any vehicle falling in the hot listed categories.

A single compressed stream shall also be sent to server for recording and general video analytics purpose

The system shall have capability to integrate with Computer Aided Dispatch (CAD) system via API

The system shall have capability to queue all pending incidents (of detection of blacklisted vehicles) so that CAD operators can attend them one by one

ANPR- Technical Requirements and Compliance Sheet for MSI (to provide compliance report with the bid)

S No.	Description	Compliance (Yes/ No) with comments, if any
1	The ANPR Platform shall be an enterprise class IP-enabled security and safety software solution.	
2	The ANPR Platform shall support the seamless Integrate with the proposed C4i platform.	
3	The automatic number plate recognition Software will be part of the supplied system, Success rate of ANPR will be taken as 95% or better for both day and night time.	
4	The ANPR Platform shall allow the user to Protect a Read or Hit from deletion for a configurable period of time.	
5	The ANPR Platform shall allow the user to correct a Plate Read manually.	
6	The ANPR Platform shall present the user with a Simple Wizard for Hotlist creation.	
7	The ANPR Platform shall allow the user to create a Hotlist without the need for any attribute information other than license plate number.	
8	The ANPR Platform shall allow the user to search the configured hotlists for any data in any of the specified fields.	
9	The ANPR Platform shall allow the user to generate a read report specifically targeted to those reads that generated a hit.	
10	The ANPR Platform shall allow for map-based viewing of real-time read monitoring.	



11	The ANPR Platform shall allow the user to search for full or partial license plate numbers.	
12	The ANPR Platform shall allow the user to search for a license plate by using wildcards.	
13	The ANPR Platform shall allow the user to automate downloading Hotlists from a FTP/SFTP or HTTP/HTTPS server using username/password/certificate authentication.	
14	The ANPR Platform shall allow the user to customize the format of the Reports displayed on-screen.	
15	Reporting, including creating custom report templates and incident reports.	
16	The ANPR Platform shall be an IP enabled solution. All communication between the SSM and ANPR Platform shall be based on standard TCP/IP protocol and shall use TLS encryption with digital certificates to secure the communication channel.	
17	The ANPR Platform shall protect against potential database server failure and continue to run through standard off-the-shelf solutions.	
18	The ANPR Platform shall manage the central database that contains all the system information and component configuration of the ANPR Platform.	
19	The ANPR Platform shall authenticate users and give access to the ANPR Platform based on predefined user access rights or privileges, and security partition settings.	
20	The ANPR Platform shall support the configuration/management of the following components specific to ANPR: • ALPR units and cameras. • Hotlists and Wanted vehicles • It shall be possible to view video associated to ALPR events when viewing a report. • Pattern of vehicle number plates if found new to be incorporated and given to OCR additions.	
21	The ANPR Platform shall support the following types of reports: ALPR-specific reports (mobile ALPR playback, hits, plate reads, reads/hits per day, reads/hits per ALPR zone, and more).	
22	The ANPR Platform shall support the configuration and management of users and user groups. A user shall be able to add, delete, or modify a user or user group if he or she has the appropriate privileges.	



23	The ANPR Platform shall support the generation of audit trails. Audit trails shall consist of logs of operator/administrator additions, deletions, and modifications.	
24	Audit trails shall be generated as reports. They shall be able to track changes made within specific time periods. Querying on specific users, changes, affected entities, and time periods shall also be possible.	
25	For entity configuration changes, the audit trail report shall include detailed information of the value before and after the changes.	
26	The ANPR Platform shall support the generation of user activity trails. User activity trails shall consist of logs of operator activity on the ANPR Platform such as login, ALPR event viewed, hotlist edits, camera viewed, badge printing, video export, and more.	
27	The ANPR Platform shall be an IP enabled solution. All communication between the SSM and ANPR Platform shall be based on standard TCP/IP protocol and shall use TLS encryption with digital certificates to secure the communication channel.	
28	The ANPR Platform shall monitor the health of the system, log health-related events, and calculate statistics.	
29	Calculates availability for clients, servers and ALPR/access/video units for efficient SLA management	
30	A web-based, centralized health dashboard shall be available to remotely view unit and role and status of the ANPR devices.	
31	Detailed system care statistics will be available through a web-based dashboard providing health metrics of ANPR Platform including Uptime and mean-time-between-failures.	
32	ANPR Platform should integrate with Vaahan Database via C4I.	
33	ANPR should have at least 1 Deployment in India in any Law Enforcement Project. Necessary Document evidence to be provided	
34	Vehicle Search: Shall have an option to search vehicles by a. vehicle colour b. vehicle colour +license plate c. vehicle make and type d. date & time e. location f. type of Vehicle	



35	Number plate missing detection: a. The system should be able to detect if there is any vehicle in the camera view without a properly installed number plate or no number plate at all. b. The system should have capability to let the user search for all such vehicle through a UI based filtering system c. The user should be able to search and track any such vehicle using various vehicle search criteria as mentioned in the point above.	

4.8.8. Picture Intelligence Unit (PIU)/ P-IRIS Functional Requirements & KPIs

Picture Intelligence Unit (PIU) will maintain all Audit Trails and logs of all instances, triggers and incidental data derived out of VA platform, FRS Engine, ANPR Engine and the activities governed by the VMS. PIU will not replicate the incidental data however, will keep the track record of all such activities as a common directory which provide convenience during post investigation analyses.

Picture Intelligence Unit (PIU) shall be given access to the databases of Passport, CCTNS, Prisons, AMBIS or open source databases or any similar database available with the State Government and Central Government. It shall also create a repository of photographs obtained from various police sources like Newspapers, Photos during raids, Photos sent by people, etc. Such photographs would be tagged for sex, age, scars, tattoos, etc. so that these become searchable. Some of the approaches to be used by the Picture Intelligence Unit for implementation of Facial Recognition System would be as follows:

- a. Match a suspect/criminal photograph with these databases.
- b. Search photographs from the database meeting certain suspect features.
- c. Match a suspected Criminal face with Video Feeds of specific camera locations or with the feed received from private or other public organization's video feeds.
- d. Whenever there is a requirement at any of the Police team to check the identity of an individual, Police Station would make such a request to PIU, who in turn would search the databases available with it to match the individual. Such databases would either be accessed through web services or in a downloaded manner. Full audit trail of reports and data provided will be maintained.
- e. PIU would also try to access information from third parties — for example, banks, telecom companies, credit companies, etc. PIU shall also liaison with other institutes & agencies doing R&D work on Facial Recognition & related technologies. It is expected that the Systems Integrator look at this Picture Intelligence Unit as a Research & Development Center to test the best and latest technologies and ensure its continuous enhancement. MSI is required to analyse the futuristic requirements for the effective functioning of PIU and propose tools like Data mining (application of statistical techniques and programmatic algorithms to discover previously unnoticed relationships within the data).
- f. Using the Key UI and integration capabilities of the Video intelligence platform, PIU shall oversee the integration of ANPR with the other relevant databases
- g. Picture Intelligence Recording and Investigation System (P-IRIS) is a video forensic unit for Video Content Analysis. It will use live camera feeds, criminal and crime scene photographs/ videos etc. as evidence in investigation of crime



- h. P-IRIS shall be set up at the PHQ level
- i. P-IRIS shall be given access to the databases of CCTNS, Visitor image database or any similar database available with State Government and Central Government
- j. It shall also create a repository of photographs obtained from various police sources like Newspapers, Photos during raids, Photos sent by people, etc. Such photographs shall be tagged for sex, age, scars, tattoos, etc., so as to create a data repository of photographs.
- k. P-IRIS Facial Recognition System shall be as follows:
 - Match a suspect/criminal photograph with these databases
 - Search photographs from the database meeting certain suspect features.
 - Match a suspected criminal face with video feeds of specific camera locations or with the video feed received from private or other public organization
 - Whenever there is a requirement at any of the Police Station to check the identity an individual, Police Station would make such a request to P-IRIS, who in turn would search these databases to match the individual. Such databases would either be accessed through web services or in offline manner.
- l. P-IRIS shall oversee the integration of ANPR System with other relevant datasets like eVAAHAN, eSAARTHI, RTO, etc. as a feature of video forensic unit. P-IRIS shall oversee the integration of ANPR with the other relevant databases like VAHAN.
- m. The PIU/ P-IRIS will act as data exchange for within Data Centre applications as envisaged in the system and the data exchange bi-directionally with any external dataset.
- n. The PIU/ P-IRIS server will index all data exchange bidirectional among all datasets and all the alarms with structured data in the system. This will facilitate a comprehensive data-lake search module.
- o. PIU/ P-IRIS system must have capability to enroll whatever images fed in the system with image enhancement and ability to verify the quality of the enrolled images with different colour indicator for low quality images enrolled in watchlist/database.
- p. Further, it shall also evaluate the use of various emerging applications and also customize these applications for effective deployments. Such applications shall include:
 - **Unidentified object detection**

The left-out object detection application automatically identifies any foreign physical object for example bags, boxes or any object kept/left un-attended in the user defined region of interest or in the field of view of a surveillance camera. Alert for the Object detected in an area of interest that has been left more than specified time span.
 - **Motion / intrusion detection**

Motion / intrusion detection can be used to detect unauthorized entry, for example, if a member of staff leaves by an unapproved exit.
Specific areas of interest can be defined in a scene and searched automatically through a recording to identify and view any significant motion that occurred during the recording.



This is useful when searching for motion in a quiet area throughout a long period of recorded video.

It can be tuned using parameters such as object size and sensitivity.

- **Noise level detection (gunshot, explosion, shattering of glass etc.)**

Gunshot detection application shall be provisioned in order to capture the instances severe crimes related to bullet fire. The system shall be capable enough to capture the Gun shot sound in the noisy conditions of roads in Delhi. It is to be considered that the Gun-shot application would be operated for the camera locations where the Police Administration has firm trends of such probable crimes only, considering the low accuracy of the solution in the current demographics of Delhi NCT.

- **Camera Vandalism and tamper detection**

In a city surveillance scenario, it can become harder to understand whether cameras are still functioning as initially intended or viewing the scenes for which they were configured. Changes in camera view may arise as a result of natural causes such as dirt build up over time or through malicious interference from people who would prefer that their actions are not recorded. Camera Tamper Detection can be applied to cameras individually, as required. Each condition listed above can be enabled or disabled and tuned per camera so that it suits the environment and scene being monitored.

Digital Video Manager (DVM) includes the ability to detect whether a camera has been tampered with under the following conditions:

- **Changed Field of View (FOV):** It can be very hard for an operator monitoring many cameras to realize quickly, that a camera is no longer observing the scene originally intended. This could be because the camera was bumped or intentionally moved to avoid detection. Either way, the changed FOV algorithm will detect and alarm this change.
- **Camera Blurred:** Camera vision may blur over time due to dust build up or through intentional defocus by someone wishing to avoid detection or hoping to degrade recorded evidence to avoid identification. The algorithm provides a means of detecting when the scene is blurred and thus assists in maintaining the integrity of the system though detection of malicious tampering or timely servicing.
- **Camera Calibration:** The Video Analytics system UI should have an in-built camera-calibration tool that can take user inputs such as reference-heights, reference depths and floor landmarks to calibrate the camera. The calibration tool should have an option to use the GPS coordinates of the camera location.
- **Camera Blinded:** This algorithm detects whether a camera has either been blinded by a bright light source or had the lens covered. Both scenarios may involve an attempt to avoid detection or identification from recorded video. DVM is now able to detect and alarm when this occurs.

- **People / Mass movement**

Crowd formation detection: System estimates the density of people in a scene and generates an alert as soon as the density in any defined area crosses a certain limit.



Crowd estimation: Once a crowd is formed, it statistically estimates the location of the crowd, number of individuals in the scene, their distribution, and statistics of their location in a zone (particularly suitable in a game field environment).

Crowd dispersion detection: Detects sudden random movement of a crowd in the scene to alert a potential safety and security threat.

During processions etc. as the crowd starts gathering and Detection reaches certain level, these cameras should automatically popup along with alarm and start monitoring from ICCV by dragging these cameras on video wall.

- **Image extraction**

System will have ability to extract image from video recording

- **Search camera feeds for person/ vehicle**

The search module of P-IRIS shall be designed with integration of above mentioned databases like crime and traffic related databases such as CCTNS, Criminal Dossier, CCIS, ZIPNET, Automated Fingerprint Identification System, e-challan, VAHAAN, SAARTHI, e-FIR Stolen Vehicles, Wanted Vehicles in Robber etc. which have the capability to perform forensic data analytics and cyber threat intelligence to analyze and anticipate the likely threats which would, increase the readiness.

q. P-IRIS shall have following types of searches:

- **Person search:** Search a person by the conditions of time period, camera, and structured information. System shall have the ability to do single attribute and combined attribute search on a person's features or clothing, such as baldness, hat, glasses, sun glasses, hair color, skin tone, texture, etc.
- **Face Search:**
 - It shall be able to search/match a suspect/criminal photograph with database created using photograph images available with Criminal Dossier, CCTNS, ZIPNET, Automated Fingerprint Identification System or any other image database of criminal available with Delhi police
 - Compare and search the face picture uploaded from the local PC, into the captured library, or in the blacklist library and get the face pictures matching the similarity
 - Search by structural information (age, gender, wearing glasses).
 - View the search results: original pictures, picture details, and video playback. Export the face picture and structural information.
 - Sort the search result from high similarity to low similarity
 - Compare the similarity between one or more specified pictures and the one in the blacklist library
 - Export the face picture and structural information



- **Vehicle Search:**

- Search for a particular vehicle based on its registration no. (the last four digit) from the database
- The system shall allow the advance search with different set of criteria while conducting post incident analysis/investigations.
- The System shall allow the user to search for appearance of any particular vehicle given its License plate number.
- The system shall allow the user to search for vehicles based on its color.
- If a vehicle is involved in theft, the cameras shall capture the picture of its driver and number plate of the vehicle which will help to nab the thieves

P-IRIS/ PIU- Technical Requirements and Compliance Sheet for MSI (to provide compliance report with the bid)

S No.	Specification	Compliance (Yes/ No) with comments, if any
A	Picture Intelligence Unit	
1	This is envisaged to be a video forensic unit/ R&D Setup for Video Content Analysis. It will use live camera feeds, criminal and crime scene photographs/ videos etc. as evidence. It will ensure video analytics, continuous time stamp and non-tampering of electronic evidence as per laws.	
2	Picture Intelligence Unit (PIU) shall be given access to the databases of Passport, CCTNS, Prisons, AMBIS or any similar database available with the State Government and Central Government. It shall also create a repository of photographs obtained from various police sources like Newspapers, Photos during raids, Photos sent by people, etc. Such photographs would be tagged for sex, age, scars, tattoos, etc. so that these become searchable. Some of the approaches to be used by the Picture Intelligence Unit for implementation of Facial Recognition System would be as follows:	
3	PIU system must have capability to enroll whatever images fed in the system with image enhancement and ability to verify the quality of the enrolled images with different colour indicator for low quality images enrolled in watch list/database.	
4	Match a suspect/criminal photograph with these databases.	
5	Search photographs from the database meeting certain suspect features.	



6	Match a suspected Criminal face with Video Feeds of specific camera locations or with the feed received from private or other public organization's video feeds.	
7	Whenever there is a requirement at any of the Police team to check the identity of an individual, Police Station would make such a request to PIU, who in turn would search the databases available with it to match the individual. Such databases would either be accessed through web services or in a downloaded manner. Full audit trail of reports and data provided will be maintained.	
8	PIU would also try to access information from third parties — for example, banks, telecom companies, credit companies, etc. PIU shall also liaison with other institutes & agencies doing R&D work on Facial Recognition & related technologies. It is expected that the Systems Integrator look at this Picture Intelligence Unit as a Research & Development Center to test the best and latest technologies and ensure its continuous enhancement. SI is required to analyze the futuristic requirements for the effective functioning of PIU and propose tools like Data mining (application of statistical techniques and programmatic algorithms to discover previously unnoticed relationships within the data). SI needs to propose one of the most advanced (+ tried & tested) Facial Recognition System.	
9	Uptime SLA would be applicable to this application, but no performance SLA is fixed since the technology is still under R&D. MSI needs to customize the application to the local conditions & carry out continuous enhancements during operational phase.	
10	PIU shall oversee the integration of ANPR with the other relevant databases. Further the PIU shall also evaluate the use of various emerging technologies and their features such as Video Analysis Module.	
B	Experts in PIU Team	
1	MSI has to provide adequate team to operationalize PIU and train the Police Personnel to make optimum utilization of the same. Minimum requirement of the team to be proposed by SI for PIU is as follows:	
2	01 Facial Recognition Analyst (with min. 1 year of relevant experience)	
3	01 video Analytic Analyst (with min. 1 year of experience in video analytics (other than facial recognition))	



4	01 IT Forensic Expert (with min. 2 years of experience in IT Forensic). Forensic Experts shall be responsible for preparing the incriminating video clips and shall also certify its integrity & chain of custody.	
5	The above experts would be deployed for a period of 2 years, from the starting of PIU of the project. It may also be required from time to time for these experts to depose in the court of law. These experts will analyze the incriminating video footage and certify its integrity & chain of custody. These experts shall oversee the integration of ANPR with the other relevant databases and also undertake R&D to evaluate and analyze various analytics-related technologies and their implementation during the project period. All the necessary software, tools required for undertaking this activity should be provided by the bidder.	
C	Publishing of Guideline Documents by PIU	
1	PIU shall be responsible for preparing various guideline documents/manuals for the appropriate use of video data and for uniform operationalization of Surveillance systems across the city at different private/public institutions. An indicative list of such guideline documents / manuals to be prepared by the PIU is given below:	
2	Guideline document/manual to standardize file Formats, compression types, interfaces, to be used by various agencies (such as Fire Dept., Ambulance Dept., Other Public Institutions, Pvt. Institutions, etc.) concerned with video / photograph recording & storage.	
3	Guidelines for video data handling for submission of the video data to judiciary as legal evidence.	
4	Guideline document / manual for setting up of Video Surveillance System by Private and Public institutions within the city.	

4.8.9. Geographical Information System (GIS) Functional Requirements & KPIs

It is envisaged that as part of the Safe City Project, integration of the CCTV Surveillance System with the Geographical Information System (GIS) will be carried out, so that physical location of cameras, GPS fitted police vehicles, Prakhari Vans, MCCV, equipment, etc. are brought out on the GIS map. It will be a seamless integration to ensure ease of use of GIS in Command & Control Center's, Police Stations & by higher management. Delhi Police holds maps nevertheless, it is recommended that the maps should be at a minimum 0.6-meter resolutions or better with all CCTV surveillance cameras located on the map apart from the updated map of all buildings, utilities and roads. The GIS maps will be provided by C-DAC being used by team of ERSS 112 project. Different Layers for Camera Pole & Heights and other parameters



need to be added as per safe city requirement in current updation. Different layers, which are proposed to be covered under GIS are as follows:

- a. CCTV Cameras
- b. Movement/Location of Prakhari Vans and MCCV
- c. Buildings / Structures
- d. Police Stations, Transport Hubs
- e. Important Government / Public Buildings, schools, colleges, hospitals etc.
- f. Public Places like Gardens, Grounds, Markets, etc.
- g. Roads, Bus Stands. - Bridges, Flyovers - Footpaths - Women Hostels, Paying-Guest accommodations.
- h. Halting points of Emergency Response Vehicles.
- i. Counselling Center's for victims of crime against women.
- j. Optical Fiber Cable network.
- k. Metro high tension wire, BSES, NDPL electrical wire
- l. Gas pipeline

Web based GIS application features

- a. It shall provide complete view of CCTV, facilities, and alarms in an easy-to-use and intuitive GIS-enabled graphical interface with a powerful workflow and business logic engine.
- b. The map will define the boundaries of the jurisdiction limits of respective police Stations and District Headquarters.
- c. MAPs shall be Open Geospatial compliant (OGC) compliant
- d. Panoramic images: Application shall allow display and navigation of 360-degree panoramic images synced with map.
- e. The system shall integrate with GIS and map information and be able to dynamically update information on the GIS maps to show status of resources.
- f. Shall allow all resources, CCTV & others on the map to be georeferenced such that they have a real-world coordinate.
- g. Shall visually display a camera sensor with related camera orientation, camera range and camera field of view angle (wherever this information of CCTV is available).
- h. Shall visually differentiate CCTV on map through different color and icon identifiers based on their type and working condition.
- i. Shall immediately view alarm details (including description, video, etc.) and investigate the alarm from the map based on the API provided through Video analytic engine.
- j. Shall allow user to choose camera from map to view live video and the data
- k. It shall be possible to selectively display the objects according to type of object and event type in order to avoid information overload through pre-defined filter settings that automatically apply during event handling
- l. Identification and display of Road and surrounding assets on geo-referenced panoramic images with attribute information display
- m. Selection of an object on the map and interactively display the corresponding panoramic image with related attributes.



- n. Shall facilitate navigation around 360° views of panoramic images
- o. User will be able to view panorama images for the identified locations on map.
- p. User can press the zoom in and zoom out button to perform zoom operation on panorama.
- q. Navigate to 360° view by panning around panorama.
- r. Move to next panorama.
- s. Jump to the desired location to view Panoramic images
- t. Geo-spatial analysis: Search to find the features around and along a particular location or features.
- u. Map Navigation: The application shall have a seamless navigation over the digitalized map
- v. Feature identification: The user shall be able to view attribute information of map features.
- w. Measurement: The user shall able to measure the area and distance.
- x. Layers: Being GIS application, application shall have different published layers on the base map e.g. roads, POI, CCTV etc.
- y. Allow one box search to locate the CCTV, locations and other assets on the map as well as on panoramic images.
- z. Thematic view: Application shall have the thematic presentation on the map layers/features.
- aa. Multiple User Access – Allows multiple users to access the system with their unique user ids and passwords.
- bb. Provision to define access rights by administrator to different users / groups.
- cc. Integration of GIS web application with other application through API or database
- dd. Shall allow show/hide different layers on GIS map as per need. i.e. If user wants to see only camera layer and hospital layer on base google map to see nearest hospital where incident happen.

GIS- Technical Requirements and Compliance Sheet for MSI (to provide compliance report with the bid)

Enterprise GIS Software

S. No	Technical Specification	Compliance (Yes/ No) with comments, if any
1	Should be capable of maintaining data history, version management and conflict detection.	
2	Should support database check in – check out / replication functionalities hence maintaining the parent child relationship of Master Database.	
3	Software should have inbuilt utility for checking availability of server software updates/patches	
4	Software should support Geo-data service and Geometry service	



5	Software should support Cloud Environments like Amazon Web Services (AWS) or Microsoft Azure	
6	Software should support deployment on-premises on physical hardware, in a private cloud using VMware or other virtualization technologies, or in the cloud using an Infrastructure as a Service provider (IaaS) such as e.g. Amazon Web Services, Microsoft Azure, IBM Soft Layer, etc.	
7	The software should support feature data (Point, line, polygon) as input data type and tabular data	
8	GIS system should be capable to manage maps, satellite images, GIS data of various point of interest information, infrastructure and assets etc.	
9	It should provide access to free Online 2D, 3D, Street, Base map, imagery Services for location reference.	
10	GIS system should have a portal for administration that lets administrators to add, update, manage and maintain city GIS data and user management, Content Sharing and capability to build various GIS applications	
11	Software should have the feature to create web sites using template or wizard. It should support adding widgets which can easily be configured minimizing customization.	
12	The application should provide an out-of-the-box, configurable mobile application that allows dynamic query and update server data remotely. The mobile application should be able to integrate with GPS devices.	
13	The software should be able to seamlessly visualize and share data, maps, apps, 3D scenes with other members in organization	
14	The software should be able to share map and layer packages to be used in desktop GIS application.	
15	The software should provide a map viewer to create, save, share maps and provide analysis tools for clustering, aggregation, proximity analysis, data enrichment, etc.	
16	The software should record various usage statistics for items, users and groups, and reports this in activity dashboards and access / usage reports to administrators and or select users.	
17	The software should provide an embedded interactive app for designing and building web responsive applications with no requirement of programming.	
18	The software should support user-friendly applications for map centric field data collection, form-based surveys and maintaining field crew workforce, etc.	
19	Should be capable of Content Management (like, Manages content locations and marks relevant content as Authoritative) and Organization User Management (e.g. User can manage all aspects of inviting and managing User, including adding to groups and resetting	



	passwords) for Managing content for different projects and role based-access management.	
20	Software allows Users to sign in with built-in accounts and accounts managed in multiple SAML-compliant identity providers configured to trust one another to manage users that may reside within or outside your organization	
21	The GIS server should be highly scalable	
22	Software should support deployment in clustered environments: Active-Active, Active-Passive.	
23	The software should provide open API to visualize the published Services	
24	Should support multiple number of Editing and viewing by desktop, web browser and mobile clients.	
25	Server application should record various service statistics, such as total requests, average response time, and timeouts, and reports this information in Manager console for better monitoring and performance optimization of services	
26	Should have Web Editing Application Functionalities like simultaneous Feature editing, isolated editing in separate versions, Undo/Redo operations, snapping by layer, snapping to new geometry, settable snapping, modify, merge, split operations, specify an Exact X,Y location, modify and create attribute values, maintain attribute values through defined rules (Domain) etc.	
27	Should support server-side Geo-processing tasks	
28	The software should provide open API to visualize the published Services	
29	The software should provide open API to visualize the published Services	
30	Should support multiple number of Editing and viewing by desktop, web browser and mobile clients.	
31	Server application should record various service statistics, such as total requests, average response time, and timeouts, and reports this information in Manager console for better monitoring and performance optimization of services	
32	Should have Web Editing Application Functionalities like simultaneous Feature editing, isolated editing in separate versions, Undo/Redo operations, snapping by layer, snapping to new geometry, settable snapping, modify, merge, split operations, specify an Exact X,Y location, modify and create attribute values, maintain attribute values through defined rules (Domain) etc.	
33	Should support server-side Geo-processing tasks	
34	The software should provide open API to visualize the published Services	
35	Should support multiple number of Editing and viewing by desktop, web browser and mobile clients.	



36	The Server software should support Replication across multiple commercial databases in connected and disconnected environments	
37	Server should be able to support read-only site mode. (This is intended to disable publishing new services and blocks most administrative operations during production.)	
38	Software should support a Service Oriented Architecture (SOA) (GIS on the enterprise service bus).	
39	It should have ready to use apps for Field, Office, and community and Application developers.	
40	The software should provide SDKs to build and deploy native applications on a variety of popular platforms and devices including Android, IOS, Java, .NET, QT etc.	
41	The application server and database servers must be supported on both Windows & Linux platform.	
42	Should support standard Web server / application server like IIS, Apache, Tomcat, Web Sphere, Web logic etc.	
43	Server based GIS Software should offer server-based analysis and Geo-processing. This should include vector, scripts, and tools; and synchronous processing.	
44	Server Software should run as a native 64-bit application and should support Windows 64-bit and Linux operating systems 64-bit.	
45	Should support Open Geospatial Consortium (OGC) and open web services: including Map, WMS, WFS, WCS, KML and Geo-JSON	
46	Should have out of the box Web Application Functionalities like pan, zoom, identifying features on a map, measure distance, interactive north arrow, magnification window, overview window, find place, query attribute, search attribute, editing, geo-processing tasks, adding base maps etc.	
47	Should support browser-based access for viewing, editing and analyzing of Geo-Spatial Data	
48	Software should allow character-by-character auto-complete suggestions to be generated as a user types an address in a client application for Geocoding of addresses	
49	Server Software should support rapid encoding and decoding for any pixel type for image service caches.	
50	Server administrator should be able to prevent unauthorized users from accessing cached pages by disabling of caching of service-related information by the web browser	
51	Software should allow to export data from the feature service to a file geo spatial database or SQLite database using custom clients.	
52	software should support to automatically generate diagrams and manage physical and logical network, Access, create, update, and edit Schematic Diagrams	
53	System tools can analyze patterns and aggregate data in the context of both space and time -Space-time (spatiotemporal) analysis	



54	Server Software should support Dynamic map service	
55	Server Software should support Cached service – Map, Image	
56	Server Software should support print and Schematic services	
57	Server Software should support Geocoding service	
58	Server Software should support Geo-processing service and run custom Geo-processing models	
59	Support for geo spatial databases and Query layers – Amazon RDS for Microsoft SQL Server or Amazon RDS for PostgreSQL IBM DB2 or Informix Microsoft Azure SQL Database or Microsoft SQL Server Oracle PostgreSQL	
60	Server Software should support Big Data File Shares like Apache Hadoop HDFS, Apache Hive, Local File Shares (CSV, Shape file)	
61	Server Software should support Raster File Share like - AWS S3, Microsoft Azure Storage, Local File Shares	
62	Server Software should support for Query Layers: ALTIBASE, Dameng, IBM Netezza, SAP HANA, SQLite and Teradata	
63	Software should support simple scripting syntax to control feature rendering, label text etc. that can be used across the platform	
64	Software should support Token model authentication and the built-in User Store	
65	Should have built in user management along with Active Directory and LDAP	
66	Should support Web-tier authentication by the web server such as Integrated Windows Authentication or even leverage an organization's existing Public Key Infrastructure (PKI)	
67	Should support the option to use Enterprise Logins -	
68	Integrate with a SAML 2.0 Identity Provider (IdP) to provide Web Single Sign On	
69	Software should support to encrypt data-in-transit by enabling HTTPS	
70	Log events of interest such as who is publishing services for the Logging and Auditing purposes. should support to enable spatial database in SAP HANA	
71	Server Software should be capable of running advanced Geo-processing tools	
72	Should have an inbuilt web gateway option to be configured and option to use different gateways like HTTP load balancer and network router devices	
73	Should have Geo-processing framework, Geo-processing tools, core analysis functionalities	



4.8.10. Other Essential Functional and Technical requirements for C4i operations

Enterprise Management System including SLA Management, Network Management, Asset Management, Incident & Work Flow Management, Privilege & Identity Management.

Functional Specifications

Sr No	Description
1	EMS including other essential featured systems like Dash-boarding, SLA Management, Network Management, Asset Management, Incident & Work Flow Management, Privilege & Identity Management, etc. will be implemented as an approach of collaborative framework by OEMs.
2	For effective operations and management of IT Operations, there is a need for an industry-standard Enterprise Management System (EMS). Given the expanse and scope of the project, EMS becomes very critical for IT Operations and SLA Measurement. Some of the critical aspects that need to be considered for operations of IT setup of are: • Network Fault Management • Network Performance Management • Server Performance Monitoring • Centralized Log Management • Centralized and Unified Dashboard • Centralized and Customizable Service Level Reporting • Help Desk for Incident Management
3	The Monitoring Solution should provide Unified Architectural design offering seamless common functions including but not limited to: • Event and Alarm management, • Auto-discovery of the IT environment, • availability and Performance monitoring • Correlation and root cause analysis • Service Level Management, notifications • Reporting and analytics • Automation and Customization
	The proposed solution must be featured in Gartner/IDC reports. Documentary proof must be provided at the time of submission.
4	There should be a tight integration between infrastructure metrics and logs to have the single consolidated console of Infrastructure & security events.
5	Consolidate IT event management activities into a single operations bridge that allows operator quickly identify the cause of the IT incident, reduces duplication of effort and decreases the time it takes to rectify IT issues.



6	The Operator should be able to pull up security events related to a given Configuration Item, from a single console which also has NOC events, and use the security events to triage the problem. This way the Operator gets consolidated system/network event details and security events (current and historical) from the same console and save time in troubleshooting / isolating the issue.
7	The operator should be able to build correlation rules in a simple GUI based environment where the Operator should be able to correlate cross domain events
8	The solution shall provide future scalability of the whole system without major architectural changes.
9	The Solution shall be distributed, scalable, and multi-platform and open to third party integration such as Cloud, Virtualization, Database, Web Server, Application Server platforms etc.
10	All the required modules should be from same OEM and should be tightly integrated for single pane of glass view of enterprise monitoring
11	The solution must provide single integrated dashboard to provide line of business views and drill down capabilities to navigate technical operators right from services to last infrastructure components
12	Consolidated dashboard of the proposed EMS solution must be able to do dynamic service modelling of all business-critical production services & use near-real time Service Model for efficient cross domain event correlation.
13	The proposed solution must provide SDK/Rest API for North bound and South Bound Integrations E.g. Forwarding specific metric data to third party database, Notifications to third party systems such as Jira, AutoDesk, Slack
14	Proposed NMS solution must have deployment reference of monitoring & managing 10,000+ network nodes in at least 3 deployments across Govt./PSU/Large Enterprise.
15	The Solution should provide all the modules as a single monitoring engine to correlate events in real-time from Networks, Servers and Applications
	The solution should be virtual appliance and deployable on Linux operating systems to reduce the overall TCO
16	The solution should run without any propriety database license for datastore - Datastore must be bundled within EMS (E.g. popular time-series, no-sql, hbase based monitoring systems) to reduce the TCO
17	The solution should provide High Availability (HA) at datacenter site
18	The solution should have inbuilt role-based access module to enable multiple users with different groups to create dashboards specific to their department
19	The Solution should have way to control and define permission such as read/write for set of devices rather than all the devices for the ease of use.
20	Calculates availability for clients, servers and ANPR/access/video units for efficient SLA management
21	Detailed system care statistics will be available through a web-based dashboard providing health metrics of ANPR Platform including Uptime and mean-time-between-failures.



EMS package- Technical Requirements and Compliance Sheet for MSI (to provide compliance report with the bid)

S No.	Description	Compliance (Yes/No) with comments, if any
Consolidated Dashboard		
1	The platform must provide complete cross-domain visibility of IT infrastructure issues	
2	The platform must consolidate monitoring events from across layers such as Network, Server, Application, Database etc.	
3	The solution should support single console for automated discovery of enterprise network components e.g. network device, servers, virtualization, cloud, application and databases	
4	The solution must support custom dashboards for different role users such as Management, admin and report users	
5	The solution must allow creating custom data widget to visualize data with user preferences e.g. Refresh time, time span, background colour, unit conversion	
6	The solution must support multiple visualization methods such as gauge, grid, charts, Top N etc.	
7	The solution should provide superior view of infrastructure health across system, networks, application and other IT Infrastructure components into a consolidated, central console	
8	There should be only one dashboard/interface to collected network/server/application/log data after correlation and consolidation across the IT landscape to reduce/correlate number of metrics/alarms	
Element & Network Performance Management (EMS/ NMS/ NTA)		
1	The proposed solution platform shall provide a single integrated solution for comprehensive management of the wired/wireless access, and rich visibility into connectivity and performance assurance issues.	
2	The EMS must conduct Performance Monitoring, Performance Management Control, and Performance Analysis of every network element into the system.	
3	There will be a policy driven protocol (management) to check the health of edge devices.	
4	The EMS should conduct the monitoring and management of the coordinated configuration of multiple devices	
5	The EMS must ensure FCAPS compliance: coordinated Fault Management, Configuration Management, Accounting Management, Performance Management and Security Management across the associated elements in the network.	



6	The design functionality shall facilitate creation of templates used for monitoring key network resources, devices, and attributes. Default templates and best practice designs are provided for quick out-of-the-box implementation automating the work required to use OEM validated designs and best practices.	
7	The proposed solution must provide comprehensive and integrated management of IT infrastructure components to maximize the availability of IT services and SLA performance.	
8	The proposed solution must provide the complete view of the Topology and network elements. The NMS shall have the ability to include the network elements and the links in the visual/graphical map of the department. The visual maps shall display the elements in different colour depending upon the status of the element. It is preferable that green color for healthy and amber/yellow color for degraded condition and red for unhealthy condition is used.	
9	The proposed solution must have suitable system level backup mechanism for taking backup of NMS data manually as well as automatically	
10	The proposed solution must keep historical data at raw level without averaging for minimum of six month	
11	The proposed solution must provide the visual presentation of the Network Element's status and the alarms. It shall also present the complete map of the network domain with suitable icons and in suitable color like green for healthy, red for non-operational, yellow for degraded mode of operation etc.	
12	The proposed solution must provide Health Monitoring reports of the network with settable periodicity -@24 Hrs, 1 week, 1 month.	
13	The proposed solution must provide the graphical layout of the network element with modules drawn using different colors to indicate their status	
14	The proposed solution must provide calendar view which allows the operator all the schedule activities such as Reports, Inventory scans etc. It shall also allow to define scheduled report for uptime, link status etc.	
15	The proposed solution should have multiple alerting features to get the notification via email, SMS and third-party systems	
16	The proposed solution must support listening to traps and syslog events from the network devices with retention period upto 6 months.	
17	The proposed solution must support defining the data retention period to control storage	
18	The solution must support custom device template to support Generic SNMP devices	



19	The solution must provide discovery & inventory of heterogeneous physical network devices like Layer-2 & Layer-3 switches, Routers and other IP devices and do mapping of LAN & WAN connectivity with granular visibility up to individual ports level.	
20	It shall provide Real time network monitoring and Measurement offend-to-end Network performance & availability to define service levels and further improve upon them.	
Fault Management		
1	The proposed solution must should provide out of the box root cause analysis with multiple root cause algorithms inbuilt for root cause analysis. It should also have a strong event correlation engine which can correlate the events on the basis of event pairing, event sequencing etc.	
2	The Platform must include an event correlation automatically fed with events originating from managed elements, monitoring tools or data sources external to the platform. This correlation must perform: • Event filtering • Event suppression • Event aggregation • Event annotation	
3	The proposed solution should provide out of the box root cause analysis with multiple root cause algorithms inbuilt for root cause analysis. It should also have a strong event correlation engine which can correlate the events on the basis of event pairing, event sequencing etc.	
4	Powerful correlation capabilities to reduce number of actionable events. Topology based and event stream-based correlation should be made available.	
5	The solution must offer relevant remedy tools, graphs in context of a selected fault alarm/event	
6	The proposed monitoring solution should have capability to configure actions-based rules for set of pre-defined alarms/alerts enabling automation of set tasks.	
7	The Platform must support Event or Alarm Correlation integrations with service desk to trigger automated creation of incidents, problems management	
8	The solution should classify events based on business impact and also allow defining custom severity levels and priority metrics such as Ok, Critical, Major, Down, Info etc. with color codes	
9	The solution should allow creation of correlation or analytics rules for administrators	
10	The proposed solution must provide default event dashboard to identify, accept and assign generated alarms	



Log Management		
1	The proposed solution must provide a common classification of event irrespective of the log format	
2	The proposed solution must provide the ability to store/ retain both normalized and the original raw format of the event log as for forensic purposes for the period of 3 months and allow to extend it to further with additional hardware without any disruption to the ongoing data collection	
3	The proposed solution should provide a minimum log compression of 8:1 for ensuring log compression to reduce overall log index storage space for the raw log format	
4	The log data generated should be stored in a centralized server. The period up to which the data must be available should be customizable.	
5	The proposed solution must support logs collected from commercial and proprietary applications. For assets not natively supported, the solution should provide the collection of events through customization of connectors or similar integration	
6	The proposed solution must support log collection for Directories (i.e. AD, LDAP), hosted applications such as database, web server, file integrity logs etc. using agents	
7	The Log receiver or log collection component must store the data locally if communication with centralized collector/receiver is unavailable.	
8	The proposed solution must support log collection from Network infrastructure (i.e. switches, routers, etc.). Please describe the level of support for this type of product.	
9	The system shall support the following log formats for log collection: Windows Event Log, Syslog, Access Log Data, Application Log data, Any Custom Log data, Text Log (flat file), JSON Data	
10	The solution should be able to collect raw logs in real-time to a Central log database from any IP device including: • Networking devices(router/switches/voice gateways) • Security devices (IDS/IPS, AV, Patch Mgmt, Firewall/DB Security solutions) • Operating systems(Windows 2003/2008,Unix,linux,AIX) • Virtualization Platforms(Microsoft HyperV, VMware Vcenter/VSphere 4.X, vDirector, Citrix) • Databases(Oracle/SQL/MYSQL/DB2)	
11	The collection devices should support collection of logs through Syslog, syslogNG and also provide native Windows Agents as well as Agentless (PowerShell) connectors	
12	The proposed solution must provide alerting based upon established policy	



13	The proposed solution must provide SDK and Rest API to write custom connectors and collectors to pull log and monitoring data from third party system	
14	The proposed solution must provide UI based wizard and capabilities to minimize false positives and deliver accurate results.	
15	The proposed solution must collect, index the log messages and support full-text searching for forensic investigation	
16	The proposed solution must support the ability to take action upon receiving an alert. For example, the solution should support the ability to initiate a script or send an email message.	
17	The solution must provide pre-defined log correlation rules to detect suspicious behavior	
18	The solution must support real-time and scheduled alerting time-line while creating a log policy to catch specific log pattern	
19	The solution should support applying regex pattern in real-time to extract vendor specific log data for reporting and alerting purpose	
20	The system shall have the capability to drag and drop building of custom search queries & reports	
21	The system shall be capable of operating at a sustained 5000 EPS per collection instance. The system shall provide the ability to scale to higher event rates by adding multiple collection instance	
Service Desk - Incident Management		
1	The proposed helpdesk system shall provide flexibility of logging, viewing, updating and closing incident manually via web interface	
2	The proposed helpdesk solution should have achieved Pink VERIFY certification on at least 6 available ITIL processes. Documentary proof must be provided at the time of submission.	
3	Each incident shall be able to associate multiple activity logs entries via manual update or automatic update from other enterprise management tools.	
4	The proposed helpdesk system shall be able to provide flexibility of incident assignment based on the workload, category, location etc.	
5	The proposed solution should automatically provide suggested knowledge base articles based on Incident properties with no programming	
6	The proposed solution should automatically suggest available technicians based on workload, average ticket closure time assigning tickets with no programming	
7	The proposed solution should tightly integrate with monitoring system to provide two-way integration - E.g. when system down alarm created, it should automatically create ticket and assign it to technician, in case system comes up before ticket is resolved by technician, it should automatically close the ticket to minimize human efforts	



8	The proposed system must not create more than one ticket for same recurring alarm to avoid ticket flooding from Monitoring system	
9	Each escalation policy shall allow easy definition on multiple escalation levels and notification to different personnel via web-based console with no programming	
10	The proposed helpdesk system shall be capable of assigning call requests to technical staff manually as well as automatically based on predefined rules, and shall support notification and escalation over email	
11	The proposed solution should allow administrator to define ticket dispatcher workflow which automatically assign incoming tickets based on rules defined in workflow. E.g. Network fault keyword tickets gets assigned to network technician automatically within NOC team	
12	The proposed helpdesk system shall provide grouping access on different security knowledge articles for different group of users.	
13	The proposed helpdesk system shall have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues	
14	The proposed solution should allow Technician to relate Incidents to Problem, Change and vice versa to have better context while working on any of ticket type	
15	The proposed helpdesk system shall support tracking of SLA (service level agreements) for call requests within the help desk through service types.	
16	The proposed helpdesk system shall integrate tightly with the Knowledge tools and CMDB and shall be accessible from the same login window	
Asset Inventory Management		
1	A configuration management database shall be established which stores unique information about each type Configuration Item CI or group of CIs.	
2	The proposed solution allows scheduling periodic report to check current software and hardware inventory	
3	The proposed solution must allow attaching CI record to generated service tickets	
4	The Proposed solution should provide end to end Asset Life Cycle Management: Makes it easier to handle the complete life cycle of an asset, that is, all stages/modules from procurement to disposal	
5	The Proposed solution should support maintaining AMC/Warranty Information with Alerting when about to expire also provide Asset Deletion capabilities enabled with workflow engine	



6	The Proposed solution should support Software License Metering: Helps to understand the software license compliance and the use of unauthorized software in the organization and helps to act proactively to curb illegal usage and problems associated with it.	
7	The proposed solution should provide Asset Dashboards/Reporting: Graphical representation all the assets based on Category, location, aging of the asset, customer, which can be further level down to the incident record ID	
8	The proposed solution should provide out of the box purchase and contract management modules to support end to end asset life cycle	
Service Level Reporting		
1	The solution should provide reports that can prove IT service quality levels, such as application response times and server resource consumption	
2	The system reports should be accessible via web browser and Reports can be published in PDF and csv format	
3	The solution must have an integrated dashboard, view of Contract Parties & current SLA delivery levels and view of Services & current SLA performance	
4	The solution must provide Reports that can be scheduled to publish automatically or they can be produced on demand	
5	The solution should be able to report in the context of the business services that the infrastructure elements support—clearly showing how the infrastructure impacts business service levels	
6	The solution should provide Business Service Management functionality to track Service quality by logically grouping Network, Server and Application components. The solution should provide correlation between Network, Server and Application to identify the business impact from the specific event or alarm	
7	The solution must provide way to define key performance indicators (KPIs) within the Service Quality report.	
8	The solution must provide SLA measurement to track service quality from both Availability and Performance perspective.	

Infrastructure cabling and connection monitoring

S No.	Parameters	Compliance (Yes/No) with comments, if any
1.	The solution should be capable of tracking device history for networked end devices including the following forensics details:	
2.	When device was first connected to the network	
3.	If and when it was removed from the network	
4.	If and when it was moved from one physical location to another	
5.	How long it has been active or inactive.	



6.	Asset, configuration and change management	
7.	The solution should be fully complying with ANSI/TIA 606-B (including B-1) and ISO/IEC 18598 standards.	
8.	The solution should deliver physical connectivity information to the management software.	
9.	The solution should be a complete Real Time Interconnect Solution and should provide alerts for:	
10.	Patch cord connections or disconnections from the patch panel.	
11.	Patch cord connections or disconnections from the switch.	
12.	Inter-changing of patch cords at the switch side.	
13.	Inter-changing of patch cords at the panel side.	
14.	There should use of DAC/ Multi-mode cables to ensure maximum possible reduction in latency parameters.	
15.	These alerts should be patching connection or disconnection alerts. These should show exact information about the panel port or switch port which got disconnected or connected and end to end link information.	
16.	The Physical Layer Management solution should be strictly based on the physical detection of patch cord connectivity.	
17.	The solution should provide the capability of electronically tagging any network equipment such as network printer, servers, IP Camera, desktop, switches, modems, etc.	
18.	The system should be robust and should report the patching connectivity information as complete ONLY when the two ends of the same patch cords are connected and should not get confused by any subsequent insertion of any other patch cord.	
19.	The solution should provide the technician an easy method of patching with- out imposing any specific sequence rules/order for the patching, thus allowing the technician to carry patching work orders as in the case of a non-intelligent solution.	
20.	Patch cord removal from Panel / Switch side should be monitored and alerts like email/SMS should be sent if any end of the patch cord is removed.	
21.	The solution should provide the capability to automatically connecting to a remote database sites as well as to a local database.	
22.	The solution shall be able to maintain a record of the rack capacity and utilization including:	
23.	Total rack space and occupied rack space	
24.	Total number of available intelligent panel ports	
25.	Total number of non-intelligent panel ports	
26.	Total number of switch ports and "switch utilization"	
27.	Total number of PDU power outlets (if installed at site)	
28.	Total number of environmental sensors (if installed at site)	



29.	The solution should be able to monitor on-line of patch cord removal from either side:	
30.	Between intelligent panels	
31.	Between intelligent panel to active device like Switch.	
32.	The solution should have the following visual indications:	
33.	LED above each port - indicating patching, patching work order pending and correcting bilking mode in case of patching mistake.	
34.	LED per each patching frame – indicating panel status.	
35.	Sound – in case of patching or removal of a cord between either intelligent panels or between intelligent panels to a switch.	
36.	All Changes of the telecommunications infrastructure facilities and networked devices should be maintained within the intelligent infrastructure management system to keep track of current activities and completed activities including:	
37.	Real time tracking of authorized and unauthorized patching activities	
38.	Generation of move, add, change work orders	
39.	Providing means for retrieval of work orders at racks with intelligent equipment using port LEDs, tablet, etc.	
40.	Automated tracking of work order completion	
41.	Scheduled work order and work order history	
42.	Monitoring and alerting on connected information	
43.	The Intelligent Physical Layer Management Solution should have guidance lights per port. The light guidance is mandatory for tracing the two ends of any patch cord, executing planned work orders and for remote management.	
44.	The lights per port on the panels should be powered from the scanning devices and should not require a separate power supply.	
45.	The intelligent panels should have the necessary intelligent hardware and light indicators integrated within the panels. Retrofits are not an option.	
46.	The panels should be passive and the panels should not require any power for operation of the intelligent management solution.	
47.	The Intelligent Physical Layer Management solution should be scalable and the design should enable maximum usage of its components e.g. scanning devices, by sharing of same components over multiple racks when required.	
48.	The solution should be simple, effective and as automated as possible requiring minimum human intervention. For e.g. for executing work orders the solution should depend on light guidance only without need for reading instructions from any media/display.	
49.	The solution should provide patching information based only on physical connectivity information and not thorough any other way.	
50.	The solution should be web based and not require any clients to be installed on end devices. All features should be available through this web explorer only.	



51.	All scanning devices monitoring the intelligent panels should be 1U only to allow maximum usage of rack space. Also they should have the capability to be shared among more racks.	
52.	The scanning devices should automatically detect the panel type; the scanning devices are connected to, and should also automatically detect the connectivity between the scanning devices. This is necessary for automatic & error free real time detection & installation of hardware components in the software.	
53.	The solution should offer flexibility to extend the panel scanning capability to distances more than 100 feet (one rack) in order to cover multiple racks.	
54.	Since all the upper & center units of the rack (critical real estate space in rack) will be required to mount panels or switches to provide a hassle free environment for their control and installation, the scanning devices would be mounted either at the top or bottom of the rack. Hence it is important that the scanning devices should carry a design such that they require minimum interaction during any work order execution and do not force any change in the rack design to enable their functioning.	
55.	The solution should be efficient and should not require use of multiple media for providing or verifying of the same information or carrying out a work order. Any work order execution should be achieved by means of lights without requiring any other interface. This is essential to ensure easy usage of the system.	
56.	The solution should provide an easy way for tracing panel port connectivity information even at the rack level without directly interacting with any panel port / software. This is important to provide information during network outage.	
57.	The implementation of the intelligent solution should not hamper or should not be hampered by the progress in the other cabling, patching & active installation. The solution should be capable to be installed at any time during the network installation and testing.	
58.	The solution should provide the capability of monitoring port availability status on network equipment including switches, patch panels and telecommunication outlets should be monitored in real time for the purpose of detecting unexpected or unauthorized activities.	
59.	The intelligent management software should use standard database so that the solution should be able to communicate and exchange data with other systems using standard protocols and database formats. This is to provide easy integration and customised reporting to other systems. Integration can be done via: SDK, SNMP traps, XML, database sharing and web services.	



60.	Server provisioning feature should be supported and built in the solution at the time of implementation. For this the solution should be ready and should not require to build integration module to integrate to IP power strips to get information of the power being consumed in the racks in real time.	
61.	The solution should be ready to connect to devices which control various parameters in the Datacenter / Hub room environment (temperature sensors, humidity sensors, door access sensors, etc.) and provide this information to the software in real time and help in server provisioning.	
62.	The system should provide Servers Health like the real time power being consumed by a server and information like ambient temperature inside the servers ,by an out of band access or network method without additional requirement of sensors or hardware.	
63.	The solution should offer as a built in feature the possibility to report any unauthorized MAC outside the white list of MACs allowed on the site.	
64.	The solution should be capable to block switch ports automatically on intrusion detection. This capability however should be selectable by the user depending on the critical nature of the location.	
65.	The solution should provide visual representation of the datacenter environment for:	
66.	Power consumption	
67.	Space availability	
68.	Temperature, humidity and other related environment sensor information.	
69.	The solution should have inbuilt dashboard. The solution should offer users to customize their own dashboard like switch utilization, panel utilization etc.	
70.	The solution should be provided with an unlimited user licenses. This is important to enable use by multiple users.	
71.	The single scanning hardware unit should be able to connect to panels in multiple Racks.	
72.	The work order execution should be achieved by LEDs on panel ports. No other interface should be required for execution of the work order.	
73.	The solution connectivity, between the different scanning appliances, should be based on standard RJ-45.	
74.	The solution should have built in reports for all physical layer monitoring, and also for Data Center operations like power consumption, temperatures, rack status and various other sensors information.	
75.	The intelligent solution must offer all copper and fiber options (RJ-45, LC, and MPO/MTP)	
76.	The solution should support tablet/smart phone in order to present the work orders.	



77.	It should have the ability to connect and provide datacenter environment reports like power consumption in racks in real time, temperatures within racks, rack door closures, water level sensing etc.	
78.	All Copper & Fiber components should be from the same OEM vendor.	
79.	All Components Passive and active Components should be RoHS (Restriction of Certain Hazardous Substances) complied.	
80.	Declaration –RoHS Compliant should clearly be mentioned on datasheets of each Passive Components (Copper & Fiber).	
81.	FRLS cables to be used for power related connections.	
82.	There should be 15-year performance warranty and Application Assurance	

Helpdesk Management

Functional requirements

MSI will be required to establish the help-desk and provide facilities management services to support the Police officials in performing their day to day functions related to this system. The helpdesk management system will be fully integrated with the enterprise monitoring (EMS) and network management system. The system will be accessed by the Police officials for raising their incidents and logging calls for support.

The key functionalities of the helpdesk would include the following:

1. Service help desk management with respect to all the trigger, alarms related to fault, and incident reported for anomaly and issues in operations of the hardware and software domains of the project architecture.
2. The service helpdesk will be primarily responsible for ensuring adhering to the SLA terms and bridge in-between the Enterprise Management System and the SLA compliance parameters.
3. There must be a handholding mechanism for Delhi Police Personnel in terms of regular operations considering all ticket closures, Incident management, Project Management to ensure uninterrupted support to Delhi Police. The system must be capable of:
 - a. Incident records can be created and changed through web interface, Event Management, NMS/EMS, CRMs, ERPs or any 3rd party system, Mobile App, Email etc.
 - b. Support for notification and escalation: System should support Incident Hierarchic Escalation; Hierarchic Escalation rules should support based on Severity or Priority. For Ex. Based on Incident Priority the Auto Escalation time to Higher Level should be different.
 - c. It should support tracking of SLA (service level agreements) for call requests within the helpdesk through service types. It should be able to attach multiple SLA profiles, Multiple SLA Metrics, should be able to adjust the SLA based on Authorized workflow



- d. Have a predefined out-of-the-box process for problem management that is compliant with best practice frameworks such as ITIL.
- e. The Helpdesk will ensure User manuals for all the Hardware and Operations at C4i, C3i and C2i with all the associated Standard Operating Procedures before Go-Live of phase I.

Technical Specifications

S No	Parameters	Compliance (Yes/ No) with comments, if any
1	The proposed helpdesk system shall provide flexibility of logging, viewing, updating and closing incident manually via web interface	
2	The proposed helpdesk solution should have achieved PinkVERIFY certification on at least 6 available ITIL processes. Documentary proof must be provided at the time of submission.	
3	Each incident shall be able to associate multiple activity logs entries via manual update or automatic update from other enterprise management tools.	
4	The proposed helpdesk system shall be able to provide flexibility of incident assignment based on the workload, category, location etc.	
5	The proposed solution should automatically provide suggested knowledge base articles based on Incident properties with no programming	
6	The proposed solution should automatically suggest available technicians based on workload, average ticket closure time assigning tickets with no programming	
7	The proposed solution should tightly integrate with monitoring system to provide two-way integration - E.g. when system down alarm created, it should automatically create ticket and assign it to technician, in case system comes up before ticket is resolved by technician, it should automatically close the ticket to minimize human efforts	
8	The proposed system must not create more than one ticket for same recurring alarm to avoid ticket flooding from Monitoring system	
9	Each escalation policy shall allow easy definition on multiple escalation levels and notification to different personnel via web-based console with no programming	
10	The proposed helpdesk system shall be capable of assigning call requests to technical staff manually as well as	



	automatically based on predefined rules, and shall support notification and escalation over email	
11	The proposed solution should allow administrator to define ticket dispatcher workflow which automatically assign incoming tickets based on rules defined in workflow. E.g. Network fault keyword tickets gets assigned to network technician automatically within NOC team	
12	The proposed helpdesk system shall provide grouping access on different security knowledge articles for different group of users.	
13	The proposed helpdesk system shall have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues	
14	The proposed solution should allow Technician to relate Incidents to Problem, Change and vice versa to have better context while working on any of ticket type	
15	The proposed helpdesk system shall support tracking of SLA (service level agreements) for call requests within the help desk through service types.	
16	The proposed helpdesk system shall integrate tightly with the Knowledge tools and CMDB and shall be accessible from the same login window	

Centralized- Field UPS Health

IP Power SE Standard UPS Centralized Health Monitoring & Network Management software.

S No.	Specification	Compliance (Yes/ No) with comments, if any
1	Software should Support multi-brand multi-UPS centralized monitoring and management	
2	Maintenance, monitoring and management of the wide distributed UPS power supply and its surrounding environment should become very easy and efficient. A variety of UPS brands and models should be monitored at the unified platform, making the management simple and convenient.	
3	It should Support all-day real-time UPS monitoring and management.	
4	It should support 365 days × 24-hour real-time continuous monitoring. UPS operating conditions should be easy to master and the quality and efficiency of the management should greatly enhance.	



5	Real-time detection of each network UPS's main power, battery, inverter work, bypass, self-test and other working conditions should be supported by software.	
6	Software should Display detailed and intuitive data and real-time image of UPS status, data and graphically intuitive and clearly showing each network UPS's voltage, frequency, load, battery and other parameters of the real-time status information to help users understand the current situation of electricity supply quality.	
7	Software should be Capable of remote control and maintenance of UPS power, and can set its regular automatic control, maintenance, preservation, such as the battery discharges and other conditions when there is no need for users to visit on-site, which means you can conduct regular operation and maintenance of the remote UPS, which greatly reduce the difficulty of the UPS management work, enhance the work efficiency, making the management of the UPS greatly improved and let the UPS battery acquire better maintenance and extend the battery life. Also, all control actions of the users have to be logged and it is easy to manage and trace.	
8	Real-time response to UPS's alarm information should be provided in software.	

Procurement of Licenses

The licenses of all the software domain features will be perpetual. They will be valid initially for phase 1 duration, followed by 3 years' validity based on the associated performance parameters of the system.

LDAP Software

It will be Windows / Linux Based Active Directory.

Audit trails and incident logs

The systems should have following features for logs and reports:

- Reports such as camera uptime availability, camera recording percentage, recording status, critical events, incident video, etc.
- Allow the operator to raise support ticket from the VMS client itself.
- Continuous log of Server Status Messages, Camera Connectivity, Storage Status, Recording ON/OFF, User Activity Logs, etc. which should be accessed from the workstations using different filters.
- Detailed listing of all active or incoming alarms with available filters for time period, alarm source, operator and alarm state.



- e. Ability to reassign alarms to other operators based on: change of state for one/multiple or all alarms, change of alarm priority, entering incident-specific log information and the suppression (snooze function) of alarms.
- f. Ability to preview, view live or playback recorded images.
- g. Automatically close an alarm based on a corresponding event.
- h. Generate audit trail reports by incident.
- i. Give full audit trail of the user activities in the system.
- j. The system log should be searchable by Level, Source and Event Type.
- k. The Audit Log should record remote user activity (searchable by User name, Audit ID, Source and Location)
- l. The Alert Log should record alerts triggered by rules (searchable by Alert type, Source and Event type)
- m. The Event Log should record event-related information (searchable by Service name, Source and Event type)
- n. 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)
- o. Bandwidth utilization logs.

4.8.11. Hardware equipment at C4i

Video Wall Solution- 70" cubes in a 4 X 4 arrangement - 3 Video Walls

S No.	Item	Specification	Compliance (Yes/No) with comments, if any
1.	Display Wall Individual Cube Size	70"±5%	
2.	Projection Technology	DLP Rear Projection with each cube having 4K-UHD resolution	
3.	Individual Video Wall Resolution	15360 x 8640	
4.	Cube Depth	Less than 600 mm	
5.	Light Source	Laser	
6.	Light Output of projection engine	2200 Lumens or more	
7.	Brightness Uniformity	95%	
8.	Dynamic Contrast ratio	100,000:1	
9.	Dust Proof	Projection Engine to be certified IP6X by a third-party laboratory to ensure prevention from ingress of dust ensuring long life of the video wall	



10.	Power Supply	Dual Redundant Power Supply Built in inside the cubes	
11.	Half Gain viewing angle	Horizontal $\pm 36^\circ$, Vertical $\pm 34^\circ$	
12.	Lifetime	Normal mode: 60 000h	
13.		Eco mode: 90,000 Hours	
14.	Inputs	1 x Display Port 1.2, 1 x HDMI 2.0	
15.	Power	100 - 240 VAC, 60 - 50Hz, (below values are for 230V; 110V +5%)	
16.	Normal mode	Less than 350 Watt	
17.	Normal mode	Less Than 1200 BTU/h	
18.	Operating conditions	5 Degrees to 35 Degrees C	
19.	Humidity	Up to 80% non-condensing	
20.	Temperature	10°C-40°C 50°F-105°F	
21.	Temperature	0°C-40°C 32°F-105°F	
22.	Video Wall and cube Control	Management through IP and handheld Remote Control for quick access	
23.	Screen Backing	3-layer screen with hard backing	
24.	Pixel clock	162 Mhz	
25.	Screen to Screen Gap	0.2 mm or lower at temperatures between 20~25 deg C.	
26.	Screen Half-gain Viewing	Hor: ± 36 degrees	
27.	Angle	Ver: ± 34 degrees	

Video Wall Controllers (For C4i)

S No.	Item	Specifications	Compliance (Yes/ No) with comments, if any
1.	Display controller	Each Controller to be able to control each PHQ video wall with a total resolution of 15360 x 8640	
2.	Redundancy in the controller	Power supply and HDD should be redundant in the controller	
3.	Platform	Windows 10 with processor with Quad core 3 Ghz or Core i7/Xeon	
4.	RAM	16 GB	
5.	Chassis Type	19" Rack mount industrial chassis	
6.	Network	2 Network Ports	
7.	Resolution Support for Outputs	16 outputs with 4K-UHD resolution per output	
8.	Inputs	Each of the two Controllers should be equipped with minimum 16 inputs of DP/HDMI supporting 4K-UHD resolution	



9.	Scalability	The system should be able to add additional inputs as required in the future using additional chassis/cards	
10.	Redundancy	Redundant Hot Swappable in RAID Configuration	
11.	Redundancy	Redundant Hot Swappable Power Supply	
12.	24 x 7 operation	The controller shall be designed for 24 x 7 operation	
13.	Others	The Video Wall and the Controller should be of the same make to ensure better performance and compatibility	
14.	OEM Certification	All features and functionality should be certified by the OEM. The Display Modules, Display Controller & Software should be from a single OEM.	
15.	Ticker	There should be a possibility in the controller to create user defined multiple tickers. It should also be possible to place these tickers anywhere on the wall	
16.	Control	The system should have the capabilities of interacting (Monitoring & Control) with various applications on different network through the single Operator Workstation. It shall be possible to launch layouts, change layouts in real time using Tablet	



Video Wall Software

S No.	Item	Specifications	Compliance (Yes/ No) with comments, if any
1.	Layouts	The software should be able to pre configure various display layouts and access them at any time with a simple mouse click or schedule/timer based.	
2.	Sources	The software should be able display multiple sources anywhere on video wall in any size.	
3.	Workspace Allocation	The video wall administrator should be able to allocate workspace to each operator	
4.	Software features	Video Wall Control Software shall allow commands on wall level or cube level or a selection of cubes:	
5.		• Switching the entire display wall on or off.	
6.		• Snap sensitivity to ensure quick and accurate aligning of sources	
7.		• Fine-tune colour of each cube	
8.	License	Should have a software license key to protect from unauthorized use	
9.	Authentication	Should offer 4 levels of authentication	
10.	Scaling	Each source should be capable of being scaled to required size	
11.	Display	The software should be able to create layouts and launch them as and when desired	
12.	Remote Control	The Display Wall should be controllable from Remote PC also.	
13.	Offline Layouts	Should be possible to create offline layouts	
14.	Layout Scheduler	All the Layouts can be scheduled as per user convince.	
15.	Layout Scheduler	Software should support auto launch of Layouts according to specified time event by user	
16.	Layout Management	It should be possible to create layouts comprising of screen scrapped content of Workstations, DVI inputs, URLs configured as sources.	
17.	Layouts Configuration	Can be pre-configured or changed in real time	
18.	Scheduling	It should be possible to schedule specific Layout based on time range	



19.	OEM Certification	All features and functionality should be certified by the OEM.	
20.		The Display Modules, Display Controller & Software should be from a single OEM.	

LED Monitor- 55" Display in a 1 X 2 arrangement

S. No.	Parameter	Specification	Compliance (Yes/No) with comments, if any
1.	Technology	LED Based	
2.	Screen Size	55 inches diagonally (± 0.4 inches)	
3.	Resolution	4k (3840 x 2160 at 60 Hz)	
4.	Viewing Angle	178° / 178°	
5.	Brightness	350 cd/m ² (typical)	
6.	Contrast Ratio	4000:1 (typical)	
7.	Aspect Ratio	16:9	
8.	Input	2 x HDMI 2.0 1 x Display Port 1 x VGA 2 x USB Ports	
9.	Remote Management	Asset1 x RJ45 1 x RS232	
10.	Duty Cycle	12/7	
11.	Certifications	UL/EN/CE/IEC/BIS certification for Safety and CE/FCC Certifications for EMC & Immunity.	
12.	Warranty	As mentioned in RFP	

Workstation for LED Monitors

Workstation:			
Sr. No	Parameters	Specifications	Compliance (Yes/ No) with comments, if any
1.	Form Factor	Tower	
2.	Processor	Intel Xeon Processor, 8 Cores, 16MB Cache, 3.8Ghz base frequency, 4.7Ghz Turbo frequency or higher processor	
3.	Operating System	Windows 10 Pro, 64bit or latest	
4.	Office	Microsoft office standard edition latest.	
5.	Chipset	Intel Workstation Chipset 400 Series or higher	



6.	Memory	32GB in combination of (4x8GB) DDR4 2666MHz Memory or higher	
7.	Hard Drive	256GB SSD	
8.	Graphic Card	Nvidia Quadro P2200 GPU or higher	
9.	Keyboard & Mouse	Wired Keyboard & Mouse (Same make as PC)	
10.	Monitor	Should be able to support min 3x 55" Led Monitor mentioned above	
11.	PSU	80PLUS Gold Certified Energy Star Compliant	
12.	Expansion Slots	Minimum "1" PCIe x16 Gen3; "2" PCIe x4/x8 Gen3 and "1" M.2 or more	
13.	Network Card	Dual Intel Ethernet Connection 10/100/1000 or better	
14.	I/O	4 - USB 3.1 1 - USB 3.1 Type C 1 - Audio Jack/ Microphone & Headphone 4 - DisplayPort 2 - RJ45 Network Connector	
15.	Warranty	As mentioned in RFP	

Workstations with 3 nos. 24" UHD Touch Monitors for C4I application at multiple rooms on 6th & 7th Floor (EoC) Mike + webcam +speaker along with operator workstation

Workstation:			
Sr. No	Parameters	Technical Specifications	Compliance (Yes/ No) with comments, if any
1.	Form Factor	Tower	
2.	Processor	Intel Xeon Processor, 8 Cores, 16MB Cache, 3.8Ghz base frequency, 4.7Ghz Turbo frequency or higher processor	
3.	Operating System	Windows 10 Pro, 64bit or latest	
4.	Office	Microsoft office standard edition latest.	
5.	Chipset	Intel Workstation Chipset 400 Series or higher	
6.	Memory	32GB in combination of (4x8GB) DDR4 2666MHz Memory or higher	
7.	Hard Drive	256GB SSD	
8.	Graphic Card	Nvidia Quadro P2200 GPU or higher	
9.	Keyboard & Mouse	Wired Keyboard & Mouse (Same make as PC)	



10.	Monitor	Should be able to support min 3x 24" Full HD Monitor (min 23.8" diagonal screen size). Monitor should be of same make as of workstation.	
11.	PSU	80PLUS Gold Certified Energy Star Compliant	
12.	Expansion Slots	Minimum "1" PCIe x16 Gen3; "2" PCIe x4/x8 Gen3 and "1" M.2 or more	
13.	Network Card	Dual Intel Ethernet Connection 10/100/1000 or better	
14.	I/O	4 - USB 3.1 1 - USB 3.1 Type C 1 - Audio Jack/ Microphone & Headphone 4 - DisplayPort 2 - RJ45 Network Connector	
15.	Warranty	As mentioned in RFP	
	Monitor		
S No.	Parameters	Technical Specifications	
1.	Size	23.8" / 24" LED Monitor	
2.	Resolution	1920 X 1080 resolution Anti-glare, IPS, 16.7 Million colors	
3.	Aspect Ratio	16:9 Aspect Ratio,	
4.	Brightness	250 cd/m ² Brightness,	
5.	Mount	Tilt and Height-adjustable stand, pivot (rotation),	
6.	Ports	1 x DisplayPort, 1 x HDMI, 1 x VGA, 5 x USB, 72% color gamut,	
7.	Certification	TCO Certified	
8.	Prerequisite	Should be of the same make as of the workstation	
9.	Warranty	As mentioned in RFP	



**Workstations with 3 nos. 24" UHD Touch Monitors for C4I application Mike + webcam
+speaker along with operator workstation**

Workstation:			
Sr. No	Parameters	Technical Specifications	Compliance (Yes/No) with comments, if any
1.	Form Factor	Tower	
2.	Processor	Intel Xeon Processor, 8 Cores, 16MB Cache, 3.8Ghz base frequency, 4.75Ghz Turbo frequency or higher processor	
3.	Operating System	Windows 10 Pro, 64bit or latest	
4.	Office	Microsoft office standard edition latest.	
5.	Chipset	Intel Workstation Chipset 400 Series or higher	
6.	Memory	32GB in combination of (4x8GB) DDR4 2666MHz Memory or higher	
7.	Hard Drive	1 TB SATA	
8.	Graphic Card	Nvidia Quadro P2200 GPU or higher	
9.	Keyboard & Mouse	Wired Keyboard & Mouse (Same make as PC)	
10.	Monitor	Should be able to support min 3x 24" Full HD Monitor (min 23.8" diagonal screen size). Monitor should be of same make as of workstation.	
11.	PSU	80PLUS Gold Certified Energy Star Compliant	
12.	Expansion Slots	Minimum "1" PCIe x16 Gen3; "2" PCIe x4/x8 Gen3 and "1" M.2 or more	
13.	Network Card	Dual Intel Ethernet Connection 10/100/1000 or better	
14.	I/O	4 - USB 3.1 1 - USB 3.1 Type C 1 - Audio Jack/ Microphone & Headphone 4 - DisplayPort 2 - RJ45 Network Connector	
15.	Warranty	As mentioned in RFP	
16.	Monitor		
S No.	Parameters	Technical Specifications	
1.	Size	23.8"/ 24" LED Touch Screen Monitor	
2.	Resolution	1920 X 1080 resolution Anti-glare, IPS, 16.7 Million colors	



3.	Aspect Ratio	16:9 Aspect Ratio,	
4.	Brightness	250 cd/m ² Brightness,	
5.	Mount	Tilt and Height-adjustable stand, pivot (rotation),	
6.	Ports	1 x DisplayPort, 1 x HDMI, 1 x VGA, 5 x USB, 72% color gamut,	
7.	Certification	TCO Certified	
8.	Prerequisite	Should be of the same make as of the workstation	
9.	Warranty	As mentioned in RFP	

Workstation for Video wall without Monitor

Workstation:			
Sr. No	Parameters	Technical Specifications	Compliance (Yes/No) with comments, if any
1.	Form Factor	Tower	
2.	Processor	Intel Xeon Processor, 8 Cores, 16MB Cache, 3.8Ghz base frequency, 4.7Ghz Turbo frequency or higher processor	
3.	Operating System	Windows 10 Pro, 64bit or latest	
4.	Office	Microsoft office standard edition latest.	
5.	Chipset	Intel Workstation Chipset 400 Series or higher	
6.	Memory	32GB in combination of (4x8GB) DDR4 2666MHz Memory or higher	
7.	Hard Drive	256GB SSD	
8.	Graphic Card	Nvidia Quadro P2200 GPU or higher	
9.	Keyboard & Mouse	Wired Keyboard & Mouse (Same make as PC)	
10.	Monitor	Should be able to support video-wall	
11.	PSU	80PLUS Gold Certified Energy Star Compliant	
12.	Expansion Slots	Minimum "1" PCIe x16 Gen3; "2" PCIe x4/x8 Gen3 and "1" M.2 or more	
13.	Network Card	Dual Intel Ethernet Connection 10/100/1000 or better	
14.	I/O	4 - USB 3.1 1 - USB 3.1 Type C 1 - Audio Jack/ Microphone & Headphone 4 - DisplayPort 2 - RJ45 Network Connector	
15.	Warranty	As mentioned in RFP	



Network Colour Laser Printer

Sr. No	Item	Specifications	Compliance (Yes/No) with comments, if any
1.	Resolution (black)	Up to 1200 x 1200 dpi or better	
2.	Resolution (color)	Up to 1200 x 1200 dpi or better	
3.	Paper trays, standard	3	
4.	Print technology	Laser	
5.	Display	4-line LCD (color graphics)	
6.	Number of print cartridges	4 (1 each black, cyan, magenta, yellow)	
7.	Connectivity	2 Hi-Speed USB 2.0 Host ports; 1 Hi-Speed USB 2.0 Device port; 1 Gigabit Ethernet 10/100/1000T network port; 1 Hardware Integration Pocket; 2 internal USB Host ports	
8.	Processor speed	Minimum 700 MHz or better	
9.	Paper handling input, standard	100-sheet multipurpose tray, 500-sheet input tray 2, 500-sheet heavy media input tray 3	
10.	Paper handling output, standard	250-sheet output bin	
11.	Duplex printing	Automatic (standard)	
12.	Hard disk	Standard, 250 GB minimum (AES 128 encryption)	
13.	Print speed, black (normal)	Up to 33 ppm	
14.	Memory	Minimum 512 or higher	
15.	Media sizes supported	Tray 1: A4, RA4, A5, B5 (JIS), B6 (JIS), 10 x 15 cm, A6, 16K, envelopes (B5, C5 ISO, C6, DL ISO); custom: 76 x 127 to 216 x 356 mm; Tray 2: A4, A5, B5 (JIS), B6 (JIS), 10 x 15 cm, A6, 16K; custom: 102 x 148.5 to 216 x 297 mm; Tray 3: A4, RA4, A5, B5 (JIS), 16K; custom: 148.5 x 216 to 210 x 356 mm	
16.	Compatible operating systems	Microsoft Windows 7 Professional(64bit), Windows 8 Pro (64 Bit), Windows 8.1, Windows 10, Server 2008 R2, Server 2012 R2, MAC OS 9.0, MAC OS X, Linux	



IP Phones

Sr. No	Parameter	Specification	Compliance (Yes/No) with comments, if any
1.	Protocols/Standards	SIP RFC3261, TCP/IP/UDP, RTP/RTCP, HTTP/HTTPS, ARP, ICMP, DNS (A record, SRV, NAPTR), DHCP, PPPoE, TELNET, TFTP, NTP, STUN, SIMPLE, LLDP, LDAP, TR-069, 802.1x, TLS, IPV6	
2.	Network Interfaces	Dual switched auto-sensing 10/100/1000 Mbps Gigabit Ethernet ports with integrated PoE	
3.	Graphic Display	Min 2.5-inch	
4.	Bluetooth	Yes, integrated	
5.	Feature Keys	8-line keys with up to 4 SIP accounts	
6.	Video Codec	Support for G.729A/B, G.711μ/a-law, G.726, G.722(wide-band), in-band and out-of-band DTMF (in audio, RFC2833, SIP INFO)	
7.	Auxiliary Ports	RJ9 headset jack	
8.	Telephony Features	Hold, transfer, forward, 4-way conference, call park, call pickup, shared-call appearance /bridged-line-appearance, downloadable phonebook, call waiting, call log XML	
9.	HD audio	Yes, HD handset and speakerphone with support for wideband audio	
10.	Language Support	English	
11.	Upgrade/Provisioning	Firmware upgrade via TFTP / HTTP / HTTPS, mass provisioning using TR-069 or AES encrypted XML configuration file	
12.	Power	Input:100-240V; Output: +12V, 0.5A Integrated Power-over-Ethernet (802.3af) Max power consumption: 6.4W (power adapter) or 6.49W (PoE)	
13.	Security	QoS Layer 2 QoS (802.1Q, 802.1P) and Layer 3 (ToS, DiffServ, MPLS) QoS User and administrator level passwords, 256-bit AES encrypted configuration file, SRTP, TLS, 802.1x or better	
14.	Compliance	FCC: Part 15 (CFR 47) Class B CE: EN55022 Class B; EN55024 Class B; EN61000-3-2; EN61000-3-3; EN60950-1 RCM: AS/ACIF S004; AS/NZS CISPR22/24; AS/NZS 60950.1 or Equivalent Indian Standards	



Display port/ HDMI splitter (for C4i & C3i + C2i)

These are tentative HDMI Splitter if required to be provided. Extra Features added to meet the solution requirement

Racks 42U with Smart PDU

Sr No	Specification	Minimum Requirement	Compliance (Yes/No) with comments, if any
1	General	42 U X 600mm X 1200mm (H x W x D) rack should have metal frame supporting more than 1300 Kgs of static load and more than 1000 kg of dynamic load.	
		Single front door and split rear door should have the perforation of more than 75% to provide the maximum airflow eliminating the need of additional FHU in the rack.	
		Doors shall have lift of hinges for tool less field reversibility.	
		Rack should have integrated hole pattern for easy installation of top panel accessories have removable opening for cable entry and shall accommodate 2000 cat 6 cables to suffice the cabling requirements.	
		Rack should have two pair of 19-inch EIA mounting rail with U marking on front and rear of each rail for ease of installation.	
2	Cable Manager	Rack should have dual purpose full height depth adjustable PDU/Cable management brackets and should be mounted in the zero U space.	
		PDU/Cable management brackets shall have button mount keyholes throughout to accommodate the tool less mounting of rack PDU's of various heights and accessories mounting holes for tool less cable mounting accessories.	
3	Panel	Rack should have split side panels with single locking slam latch for quick and easy installation and maintenance, single person removal and installation eliminates the manpower dependencies.	



4	Caster & Levelling	42 U rack frame height that allows access through standard doors on four swivel casters, rack shall have the levelling feet and shall be accessible from the top of the frame for easy adjustment.	
5	Hardware Accessories / Installation ease	Rack shall have the necessary hardware accessories ((50 each M6 cage nuts and screws), Cage nut installation tool, edge protection for top panel cable entry,	
		Rack shall have necessary baying brackets and the bolt down kits	
		Rack frame design should allow 2.5 inch more usable space in the rack for the proper equipment placement and ease of access.	
6	Powder Coating	Rack should have the powder coated black color,	
7	Certification	Rack shall have EIA, UL, RoHS, REACH certified	
8	Power Distribution	Rack shall have two power distribution unit, vertically mounted on the rear of the rack to power on the devices in the rack.	
9	Power Unit Distribution	Monitored, Unit Level, 32Amps, 230V, 1 Phase, 7.3KW, Vertical, 30 IEC C13, 6 IEC C19, Locking Sockets, 3m power Cord with 2P+E (IP44)	
		The PDU shall have locking outlets - cable locking mechanism so that it should not require the locking cable to secure the cables connected to the PDU	
		PDU shall have Input and Breaker level current monitoring. Local high visibility LED display.	
		PDU shall have Phase (A) Monitoring (kWh, W, VA, PF, V, A) Power Measurements Compliant with ANSI C12.1 and IEC 62053-21 at 1% Accuracy Class Requirements and Circuit / Breaker Monitoring (A)	
		Circuit/Breaker Current Measurements Independently Tested and Verified at 2% Accuracy.	
		The PDU shall support the mobile app for the power monitoring and should be easy to be shared in various formats	



		The PDU shall be upgrade ready so that it can be changed to monitored PDU without downtime, by simply changing the Field replaceable IMD unit.	
		PDU shall have button mounting option for easy toolless installation and reinstallation of the PDU's	
		PDU shall have colored outlets to differentiate the outlets based on the breakers.	
		The PDU should be CE certified.	
10	Rack	Both rack and PDU should come with 5 years of default warranty	

Layer 2 Network Switch- 24 Ports

S No..	Technical Specifications of L2 Switch	Compliance (Yes/No) with comments, if any
1.	Should have required accessories for mounting.	
2.	Should have 24 x 10/100/1000 Base-T ports & 2xSFP+ ports. 2x single mode 1GbE transceivers to be provided in switch	
3.	Should have min. 190Watt PoE budget. Stacking cables to be included in each switch.	
4.	Should have non-blocking switch fabric	
5.	Should have minimum 16000 MAC addresses, minimum 500 VLANs.	
6.	Should have 1GB Flash & 1GB CPU memory	
7.	Should support 64 LAG, load balancing, double VLAN tagging.	
8.	Should have dual firmware images on board. USB port for easy config & firmware image upload	
9.	Should support Time Based ACLs, MAC based ACLs from day 1.	
10.	Should have Flow based QoS, DiffServ, port based QoS, WRR, strict queue scheduling	
11.	Should support UDLD, STP, RSTP, MSTP.	
12.	Should support STP, MSTP, minimum 8 hardware queues per port, SP queuing or equivalent, LLDP-MED.	
13.	Should have 802.1x, RADIUS, TACACS+, IGMP v1/v2/v3 snooping	
14.	Should support SFPs for 10km, 80km distance	
15.	Should have Private VLAN & Auto VLAN	
16.	Should Support SNMP, RMON, SSH, telnet, web management, network management software.	
17.	RSPAN, Private VLAN, captive portal	
18.	Power supply/adaptor/cords to be parts of supply	



19.	Switch should have min. 130Watt PoE budget	
20.	RoHS, Energy Efficient Ethernet, REACH compliance. FCC Class A; NRTL UL; FDA 21 CFR, EN 61000-4-5: Surge	
21.	The switch & transceivers should be from the same OEM	
22.	Seamless Integration: For Seamless Integration and Interoperability all the switches and SFP Modules should be fully compatible for smooth functioning of the system	

Joystick for PTZ camera at Workstation

Sr. No	Specification	Description	Compliance (Yes/ No) with comments, if any
1	VMS Compatibility	The Joystick must be compatible with all distributed network video management components.	
2	Technology	Six-degrees-of-freedom (6DoF) sensor - Intuitively and precisely navigate digital models or camera positions in 3D space.	
3	Design	The full-size, soft-coated hand rest positions the hand comfortably, and 15 large, soft-touch, function keys allow quick access to frequently used commands.	
4	Quick View Keys	Fingertip access to 12 views makes it easier to switch cameras	
5	Function Keys	Easy access to 4 application commands for an optimized workflow.	
6	Display	Provides a visual reminder of function key assignments on your computer screen	
7	Modifier	Fingertip access to Ctrl, Shift, Alt and Esc keys saves time by reducing the need to move your hand between mouse and Joystick	
8	Numpad	Allows direct numerical input into your application using your standard mouse rather than the Joystick	
9	System flexibility	The Joystick must be part of an integrated system and shall be configured so any number can be added to the system. When combined with user interfaces (UIs), network storage managers (NSM's), encoders, IP cameras, and video consoles, the Joystick forms an integral part of a	



		complete network-based video control system	
10	Input Connector type (power Supply)	Universal Inter changeable	
11	Joystick Interface	USB 2.0	
12	Cable	USB	
13	Joystick Module	Fully proportional PTZ, variable speed; with zoom, iris and focus controls	
14	Operating temperature	0° to 40°C	

55 Inch LED TV

Sr.No	Standard	HDR (High Dynamic Range)	Compliance (Yes/ No) with comments, if any
1.	Display Type	Ultra HD 4K	
2.	Screen Size (Diagonal)	138.8 cm (55 inch) minimum	
3.	Screen Resolution	Minimum - 3840 x 2160 - Ultra HD	
4.	HDMI & USB Ports	Minimum 2 USB Ports and 3 HDMI Ports	
5.	TV Connectivity	Ethernet, Built-in Chromecast and WiFi	
6.	Speaker Output Power	Minimum 2 X 10 Watts	

Dual TV Stand with Power Distribution

Sr.NO	Product	Features	Compliance (Yes/ No) with comments, if any
1.	Screen size	Fits (2) 30" – 60" Screens	
2.	Material	Steel, Aluminium	
3.	Finish	Powder-Coated, Anodized	
4.	Bracket Type	Tilting, Rotating	
5.	Orientation	Portrait, Landscape	
6.	Placement Style	Floor Standing	
7.	Features	Wheels, Tilting, Adjustable Height	
8.	Weight	30KG minimum load capacity.	
9.	Shelf	Minimum – 2	
10.	Electrical	4 Electrical Outlets with Switch and cable manager	



Civil Works and interiors of C4i

C4i Design and Standards

Sr. No	Specifications	Compliance (Yes/ No), with remarks, if any
1.	This facility being the first of its kind, scale & prestige it is mandatory for the bidder to provide Designer Control Room Solutions without compromising on the safety and functionality of the facility. Materials having the adverse impact on the environment and nature shall be deemed unacceptable. To ensure an integrated solution, to qualify as per the international control room design & safety norms; main bidder shall bring one single professional Control Room Interior Solution Provider on board with an experience of designing, manufacturing and installing at least five control rooms interiors with control desks. Supporting work orders and completion / appreciation certificates to be enclosed along with the bid.	
2.	The scope of the project includes designing; engineering, supply & installation of 24X7 mission critical Control Center Interiors. As this is a project of National repute, this state-of-the art facility & all its components viz Frameless glass partition, modular ceiling, flooring, control desk, modular paneling, ceiling luminaries' and its wiring etc. shall be treated as a part of one single solution. Main bidder to submit MAF (Manufacturer's Authorization Form) from professional Control Room Interior Solution. The professional control room solution provider must have experience of supplying a cumulative value of at-least 1000 square meter of metal wall paneling & 1000 square meter of designer metal false ceiling for control room application in past three financial years, the professional control room agency must have experience of designing, manufacturing and installing at least five police control rooms interior projects with control desks	
3.	The entire design proposal must be modular, Flexible, Dynamic, Scalable, Expandable and re-deployable to accommodate any technological changes / future needs which are not envisaged now. Modularity enables in quick and easy up-gradation. It is mandatory for the main bidder that the control room interior solution provider supplies all elements & executes all the activities like ceiling, flooring, control desks, paneling, partitions & illumination to avoid interface & quality related issues.	
4.	Control room solution provider with an experience of doing at-least Two control room studies will be preferred. Control room solution provider declaration and reference PO copies to be submitted.	
5.	Modular Paneling - Self inter lockable metal panels with front sheet of Preformed Textured galvanized sheet with a coating to avoid rust.	



6.	Control Room Interior shall be Green guard gold Certified (Modular Metal Ceiling, Flooring & Modular Metal wall paneling).	
7.	Integrated Ceiling & Paneling: UL/NABL/Government approved test laboratory certified audited certified design feature of Modular Metal Ceiling & Paneling for integrated look of interior application	
8.	The Modular Metal Paneling, Modular Control Desks and Designer Metal Ceiling shall be RoHS certified to ensure restriction of hazardous substance so that the final product does not contaminate the environment. Valid RoHS Certificate to be submitted along with the technical bid by NABL/Government approved test laboratory.	
9.	Sound transmission class (STC) value should be 35 for Wall Paneling & Partition test report from reputed agency	
10.	Tiles Perforation – UL/NABL/Government approved test laboratory certified audited certified design feature on modular wall paneling tile having clean perforations and providing smooth finish on front fascia of tiles. Valid UL audit certificate to be submitted along with the technical bid.	
11.	UL/NABL/Government approved test laboratory certified audited certified design feature of Load bearing capacity of Paneling - Paneling structure shall have load carrying capacity of 300 Kg to hold any display unit on clamp having minimum length of 750mm. Valid UL audit Certificate / /NABL/Government approved test laboratory certified audited certified to be submitted along with the technical bid.	
12.	UL/NABL/Government approved test laboratory certified audited certified design feature of Modular wall Paneling tile having secure locking arrangement for equidistant mounting.	
13.	The control room solution provider shall propose three colour options in advance during approval stage and shall change the approved colour scheme in future at no cost.	
14.	Paneling/cladding tiles shall be designed to achieve shape and design as per the design consultant with the combination of acrylic panels with lights, designed to enhance visual feel, with provision for easy installation and maintenance.	
15.	Ceiling Material - Factory made acoustic modular metal false ceiling of powder coated panels.	
16.	Factory made acoustic modular metal false ceiling of powder coated panels. Make shall comprising of perforated and non-perforated metal panels made through CNC laser Cutting, bending & punching. Customized 3-D metal ceiling as per the enclosed control room image	
17.	Ceiling in viewing gallery: The baffle ceiling shall be made of GI/MS sheet or extruded Aluminum. The ceiling baffles planks shall have integrated illumination channel which shall be processed on Machine to have dimensions to suit control room illumination requirement.	



18.	Modular perforated metal plank false ceiling should have Noise absorption coefficient (NRC) value 0.60 per IS:8225-1987, test report from reputed agency to be submitted	
19.	The non-uniform gaps (up to 750mm) between the designer metal Ceiling and the adjacent walls / partition shall be covered with calcium silicate ceiling.	
20.	False Flooring: Top surface shall finish with Carpet flooring. top surface should be finished with durable & environment friendly acoustic carpet pasted with special glue.	
21.	Carpet flooring- Minimum 4 mm thick acoustic carpet flooring shall meet the requirement of EN 1307 (shall have Impact sound of minimum $L_w = 19$ dB as per (ISO 717-2)). Flooring shall be decorative type of approved shade, pattern, texture and design and of approved manufacturer with sound absorption of 0.1 as per ISO 354. Dimensions shall be as per the final approved design and site requirement.	
22.	Metal Doors (with OR without Vision Panel): - With door hinges and locking arrangements and both way handle. Prepare with rigid thermo fused film metal panels. Specification: 0.6mm thick Metal panel sheets, cavity filled with honeycomb inside adequate quantity. Material of the partition and that of metal door will remain the same.	
23.	12mm thick frameless tempered clear glass door: - With door spring and locking arrangements and both way handle and patch fittings.	
24.	Illumination: - Control Room illumination shall be designed as per ISO 11064 norms. To ensure an integrated solution, to qualify as per the international control room design & safety norms; main bidder shall bring one single professional Control Room Interior Solution Provider on board with an experience of designing, manufacturing and installing at least twenty control rooms interiors with control desks. These packages should have been executed on or before Bid release date. Supporting work orders and completion / appreciation certificates to be enclosed along with the bid.	
25.	Table-top: - The material of the working surface should be minimum 25 mm thick MDF with High Pressure ANSI/NEMA LD3 certified scratch-resistant Laminate. The EPD (Environmental product declaration) of control desk must be verified in accordance with ISO 14025 for Impacts on Environment by Console. Valid document must be submitted along with the bid. to be audit certified by NABL/Government approved test laboratory.	
26.	Console Structure - To allow future extension and expansion, a weld free system shall be proposed. Interconnecting joints shall not be visible. The structure shall allow easy assembly of Hinged Shutters, Slat wall, Gland Plate, Monitor arms in extremely rigid manner.	
27.	The Console OEM should be an FSC Certified manufacturer from a reputed certifying agency. The professional agency should have valid Trademark registration issued by Government of India for the console	



	offered. Valid Trademark certificate should be attached along with the technical bid.	
28.	The Control Desk cable manager opening, and rear edge of desktop shall be protected from minimum 5mm high no spill edge, it shall come above desktop surface to prevent liquid from spilling inside the CPU/Equipment Cabinet. Material of edge shall be Polyurethane.	
29.	Monitor Arm: - UL/NABL/Government approved test laboratory certified design feature of monitor arm assembly shall have auto lock, push & remove feature for quick release of VESA mounts and modular arm extensions	
30.	Slat Wall: The slat wall shall have provision to install acrylic sheet / glass panel above it. This sheet / panel shall bear laser cut company logo on the upper left corner and shall be programmable to indicate illuminated emergency indication feature.	
31.	Modular metal wall panels (at a height of 1.2 meters from floor) and peripheral metal ceiling tiles shall have integrated illuminated indicators. These indicators can be changed to different colours like blue, green and red during different control room scenarios viz. VIP visits, shift change and emergency respectively.	
32.	Provide live data of Humidity & temperature of the control room.	
33.	Two exhaust fans shall be provided in every cabinet. Both the fans shall automatically start upon crossing the threshold temperature.	
34.	Interactive Desk: One touch table of 55" (diagonal size) shall be provided in viewing gallery for visitor's interface with the control room environment for process understanding of control room. The horizontal touch screen shall become vertical at a touch of a button for multi-purpose use.	
35.	A prototypical design approach must be adopted for design of control centers & consoles so, it must be prepared in strict compliance to ISO 11064 i.e. Ergonomic Design of control centers. Professional control room interior solution provider to submit an ergonomic study report including control room & desk along with the bid. The study must cover, Lux level reports as per industry acceptable illumination levels, spatial arrangement for efficient & safe movement of operators within the control room during normal and emergency situations, Ideal viewing angles (of operators) to ensure little head movement and minimal eye movement. All these considerations must be shown in the drawings during bid submission and the report must be signed by an ergonomist who has an experience of doing at-least Two projects of control room ergonomic study.	
36.	The requirements must be elaborated via a smart virtual-reality module with auto-recommendation during design approval stage before commencement of job.	



37.	To achieve acoustics without deteriorating the aesthetical appeal of the control room it is necessary that the wall paneling tiles have clean micro-perforations all over the surface.	
38.	To ensure operator's well-being it is mandatory that the wall paneling/claddings, modular metal ceilings, false floor finishes & control desk emit low VOCs (within permissible limits) hence, these shall be tested & certified as per standard method for testing and evaluation of volatile organic chemical emissions from indoor sources using environmental chambers. The control room interiors (modular metal ceiling, false flooring, control desk & modular metal wall paneling) must be compliant with the BIFMA X7.1 standard and BIFMA e3 credits or Government approved test laboratory certified audited certified.	
39.	The modular metal paneling, modular control desks and designer metal ceiling must comply to the lead-free directive to ensure restriction of hazardous substances so that the final product does not contaminate the environment. The final product i.e. designer metal ceiling, modular metal paneling, control desk does not contain hazardous substances. Valid document to be submitted along with the bid.	
40.	Console should have certificate of safety for commercial furnishings along with 200 kg of load carrying capacity on the working surface.	
41.	Material like wall paint, gypsum, wood, laminate cladding and fabric should not be used in control room interiors. Conventional office interior shall be deemed unacceptable. From fire safety point of view the metal ceiling tile & metal wall paneling tiles shall be class A fire rated as per the norms of comparative measurements of surface flame spread and smoke density measurements with that of select grade red oak and fiber-cement board surfaces under the specific fire exposure conditions. Valid document to be submitted along with the bid.	
42.	It is mandatory for the main bidder that the control room interior solution provider supplies all elements & executes all the activities like ceiling, flooring, control desks, paneling, partitions & illumination to avoid interface & quality related issues.	

The Other details are enclosed in Chapter-3 of this RFP



4.8.12. Infrastructure at C3i (District Head Quarters)

Workstations with 3 nos. 24" Monitors for C4I application Mike + webcam +speaker along with operator workstation

Sr. No	Parameters	Technical Specifications	Compliance (Yes/No) with comments, if any
1.	Form Factor	Tower	
2.	Processor	Intel Xeon Processor, 8 Cores, 16 MB ,Cache, 3.8 Ghz base frequency,4.7 Ghz Turbo frequency or higher processor	
3.	Operating System	Windows 10 Pro, 64bit or latest	
4.	Office	Microsoft office standard edition latest.	
5.	Chipset	Intel Workstation Chipset 400 Series or higher	
6.	Memory	32GB in combination of (4x8GB) DDR4 2666MHz Memory or higher	
7.	Hard Drive	1 TB SATA	
8.	Graphic Card	Nvidia Quadro P2200 GPU or higher	
9.	Keyboard & Mouse	Wired Keyboard & Mouse (Same make as PC)	
10.	Monitor	Should be able to support min 3x 24" Full HD Monitor (min 23.8" diagonal screen size). Monitor should be of same make as of workstation.	
11.	PSU	80PLUS Gold Certified Energy Star Compliant	
12.	Expansion Slots	Minimum "1" PCIe x16 Gen3; "2" PCIe x4/x8 Gen3 and "1" M.2 or more	
13.	Network Card	Dual Intel Ethernet Connection 10/100/1000 or better	
14.	I/O	4 - USB 3.1 1 - USB 3.1 Type C 1 - Audio Jack/ Microphone & Headphone 4 - DisplayPort 2 - RJ45 Network Connector	
15.	Warranty	As mentioned in RFP	
Monitor			
Sr. No	Parameters	Technical Specifications	Compliance (Yes/No) with comments, if any
1.	Size	23.8"/ 24" LED Monitor	
2.	Resolution	1920 X 1080 resolution Anti-glare, IPS, 16.7 Million colors	
3.	Aspect Ratio	16:9 Aspect Ratio,	



4.	Brightness	250 cd/m ² Brightness,	
5.	Mount	Tilt and Height-adjustable stand, pivot (rotation),	
6.	Ports	1 x DisplayPort, 1 x HDMI, 1 x VGA, 5 x USB, 72% color gamut,	
7.	Certification	TCO Certified	
8.	Prerequisite	Should be of the same make as of the workstation	
9.	Warranty	As mentioned in RFP	

LED Monitor- 55" Display

S. No.	Parameter	Minimum Specification	Compliance (Yes/No) with comments, if any
1.	Technology	LED Based	
2.	Screen Size	55 inches diagonally (± 0.4 inches)	
3.	Resolution	4k (3840 x 2160 at 60 Hz)	
4.	Viewing Angle	178° / 178°	
5.	Brightness	350 cd/m ² (typical)	
6.	Contrast Ratio	4000:1 (typical)	
8.	Aspect Ratio	16:9	
9.	Input	2 x HDMI 2.0 1 x Display Port 1 x VGA 2 x USB Ports	
10.	Remote Management	Asset 1 x RJ45 1 x RS232	
11.	Duty Cycle	12/7	
12.	Certifications	UL/EN/CE/IEC/BIS certification for Safety and CE/FCC Certifications for EMC & Immunity.	
13	Warranty	As mentioned in RFP	

Workstations to Display Wall inputs

Sr. No	Parameters	Technical Specifications	Compliance (Yes/No) with comments, if any
1.	Form Factor	Tower	
2.	Processor	Intel Xeon Processor, 8 Cores, 16 MB Cache, 3.8 Ghz base frequency, 4.7 Ghz Turbo frequency or higher processor	
3.	Operating System	Windows 10 Pro, 64bit or latest	



4.	Office	Microsoft office standard edition latest.	
5.	Chipset	Intel Workstation Chipset 400 Series or higher	
6.	Memory	32GB in combination of (4x8GB) DDR4 2666MHz Memory or higher	
7.	Hard Drive	256GB SSD	
8.	Graphic Card	Nvidia Quadro P2200 GPU or higher	
9.	Keyboard & Mouse	Wired Keyboard & Mouse (Same make as PC)	
10.	Monitor	Should be able to support 55" LED monitors mentioned	
11.	PSU	80PLUS Gold Certified Energy Star Compliant	
12.	Expansion Slots	Minimum "1" PCIe x16 Gen3; "2" PCIe x4/x8 Gen3 and "1" M.2 or more	
13.	Network Card	Dual Intel Ethernet Connection 10/100/1000 or better	
14.	I/O	4 - USB 3.1 1 - USB 3.1 Type C 1 - Audio Jack/ Microphone & Headphone 4 - DisplayPort 2 - RJ45 Network Connector	
15.	Warranty	As mentioned in RFP	

Network colour Laser Printer

Sr. No	Item	Specifications	Compliance (Yes/No) with comments, if any
1.	Resolution (black)	Up to 1200 x 1200 dpi or better	
2.	Resolution (color)	Up to 1200 x 1200 dpi or better	
3.	Paper trays, standard	3	
4.	Print technology	Laser	
5.	Display	4-line LCD (color graphics)	
6.	Number of print cartridges	4 (1 each black, cyan, magenta, yellow)	
7.	Connectivity	2 Hi-Speed USB 2.0 Host ports; 1 Hi-Speed USB 2.0 Device port; 1 Gigabit Ethernet 10/100/1000T network port; 1 Hardware Integration Pocket; 2 internal USB Host ports	
8.	Processor speed	Minimum 700 MHz or better	



9.	Paper handling input, standard	100-sheet multipurpose tray, 500-sheet input tray 2, 500-sheet heavy media input tray 3	
10.	Paper handling output, standard	250-sheet output bin	
11.	Duplex printing	Automatic (standard)	
12.	Hard disk	Standard, 250 GB minimum (AES 128 encryption)	
13.	Print speed, black (normal)	Up to 33 ppm	
14.	Memory	Minimum 512 or higher	
15.	Media sizes supported	Tray 1: A4, RA4, A5, B5 (JIS), B6 (JIS), 10 x 15 cm, A6, 16K, envelopes (B5, C5 ISO, C6, DL ISO); custom: 76 x 127 to 216 x 356 mm; Tray 2: A4, A5, B5 (JIS), B6 (JIS), 10 x 15 cm, A6, 16K; custom: 102 x 148.5 to 216 x 297 mm; Tray 3: A4, RA4, A5, B5 (JIS), 16K; custom: 148.5 x 216 to 210 x 356 mm	
16.	Compatible operating systems	Microsoft Windows 7 Professional(64bit), Windows 8 Pro (64 Bit), Windows 8.1, Windows 10, Server 2008 R2, Server 2012 R2, MAC OS 9.0, MAC OS X, Linux	

IP Phones

Sr. No	Parameter	Specification	Compliance (Yes/No) with comments, if any
1.	Protocols/Standards	SIP RFC3261, TCP/IP/UDP, RTP/RTCP, HTTP/HTTPS, ARP, ICMP, DNS (A record, SRV, NAPTR), DHCP, PPPoE, TELNET, TFTP, NTP, STUN, SIMPLE, LLDP, LDAP, TR-069, 802.1x, TLS, IPV6	
2.	Network Interfaces	Dual switched auto-sensing 10/100/1000 Mbps Gigabit Ethernet ports with integrated PoE	
3.	Graphic Display	Min 2.5-inch	
4.	Bluetooth	Yes, integrated	
5.	Feature Keys	8-line keys with up to 4 SIP accounts	
6.	Video Codec	Support for G.729A/B, G.711μ/a-law, G.726, G.722(wide-band), in-band and out-of-band DTMF (in audio, RFC2833, SIP INFO)	
7.	Auxiliary Ports	RJ9 headset jack	



8.	Telephony Features	Hold, transfer, forward, 4-way conference, call park, call pickup, shared-call appearance /bridged-line-appearance, downloadable phonebook, call waiting, call log XML	
9.	HD audio	Yes, HD handset and speakerphone with support for wideband audio	
10.	Language Support	English	
11.	Upgrade/Provisioning	Firmware upgrade via TFTP / HTTP / HTTPS, mass provisioning using TR-069 or AES encrypted XML configuration file	
12.	Power	Input:100-240V; Output: +12V, 0.5A Integrated Power-over-Ethernet (802.3af) Max power consumption: 6.4W (power adapter) or 6.49W (PoE)	
13.	Security	QoS Layer 2 QoS (802.1Q, 802.1P) and Layer 3 (ToS, DiffServ, MPLS) QoS User and administrator level passwords, 256-bit AES encrypted configuration file, SRTP, TLS, 802.1x or better	
14.	Compliance	FCC: Part 15 (CFR 47) Class B CE: EN55022 Class B; EN55024 Class B; EN61000-3-2; EN61000-3-3; EN60950-1 RCM: AS/ACIF S004; AS/NZS CISPR22/24; AS/NZS 60950.1 or equivalent Indian standard	

Secured Network Devices

- **Solution should support build in NGFW feature (Anti Spyware, IPS, Anti-Virus and application control)** to protect network against threats or external NGFW solution can be quoted separately

Sr. No	Features	Specification	Compliance (Yes/No) with comments, if any
1	General	Proposed vendor must be placed in Leader and Challengers Quadrant in Gartner SD-WAN or leader Gartner quadrant for Enterprise Firewall. NSS recommended vendor shall be preferred.	



		The SDWAN device should be supplied with hot swappable Fan tray and redundant hot swappable Power supplies and shall support IPv6 like application identification, Zone protection, management etc. from Day-1	
1	SDWAN Architecture	Proposed SDWAN solution should have management-based architecture and if management appliances/solution goes offline the SDWAN solution should keep on functioning without any issues. Must support build in GUI as well for any onsite changes if required.	
2		The bidder shall propose at least one management solution as asked above.	
3		Management architecture should have option to be deployed in HA if required in future.	
4		Management architecture should support on premise Model as well as have option of hosting on cloud.	
5		There should not be any impact on SDWAN data forwarding capability in case of complete disconnection of management	
6		Management architecture should support Virtual Firewall/multi-tenancy and the proposed device shall minimally have Common Criteria and Internet Computer Security Association (ICSA) Certification and should not have any wireless code in the offered device or its family in hardware or software. No work around this will be accepted.	
7		Management architecture should support rich policy constructs to manipulate routing information, access control, segmentation, Application control.	
8		Solution should provide transport independence and should allow to use any transport like MPLS, Internet, 3G/4G/broadband, Point to Point link etc.	
9		Licensing of SD-WAN solution must be based on device capacity not on bandwidth capacity / restriction	



10		Architecture must support zero touch deployment, so that minimum effort is required to deploy the solution	
	Operations	It should support multi-cast Network	
		Network would be functional at the time of connectivity failure between controller and branch device.	
		System Should able to support of network elements to deploy any kind of topologies such as any-to-any, Hub-spoke and Partial mesh.	
		System should able to support Multiple WAN Links utilization and detecting blackouts & brownouts by supporting active / active load balancing & Fast session failover	
		System must support Diverse WAN including T1, E1, LTE, PPPoE, DSL, Fibre and Ethernet	
1	Security	Management and SDWAN solution should	
2		communicate over encrypted channel	
3		Solution must support templates to be applied to the groups of police station quickly.	
4		SDWAN Router should support strong encryption like AES 256 or higher	
5		PACKET REDISTRIBUTION must be supported even over IPSec tunnel and it should support sub second path failover and recovery	
6		Proposed solution must support creation of logical separate sub-domain within single physical devices to separate different kind of networks.	
7			
8		SDWAN solution should support integration with cloud based/appliance-based security solutions or should have inbuilt security features like content filtering and antivirus	
9		SDWAN solution should support split tunneling to provide direct internet access from branch	
10		SDWAN solution shall have built in feature to protect CPU under DoS/DDos attacks	



11		SDWAN architecture should support application identification at layer-7 and should able to identify minimum 3000 applications natively or minimum throughput as mentioned above. It should also allow to define custom applications as per requirement	
1	Routing and QoS	SDWAN solution should allow minimum 2 service providers at branch locations and 4 service providers at DC.	
2		SDWAN solution should support BGP and Static routing	
3		SDWAN solution should support performance SLA based on latency, packet loss, jitter or all 3 combined	
4		SDWAN edge devices should support 802.1Q, sub interface, Inter VLAN routing	
5		SDWAN solution should support rule-based routing based on Application, user, user group, source, destination or combination of any of them	
6		SDWAN Solution should support rule creation based on Application or source address or destination address and each rule should have option to use different performance SLA	
7		SDWAN should support QoS based on application	
8		SDWAN device should support FEC (Forward Error correction) and DSCP matching	
9		SDWAN device must support BGP additional path support and route-map	
10		SDWAN device solution must support Auto VPN	
1	Management	Management solution should be appliance/VM which must support around 300 SDWAN devices at Day 1 scalable to 1000. If VM option is quoted than server should be given along with all the necessary licenses	
2		Management solution should have built in GUI which can be accessed by any popular browser and no extra software must be required to open management GUI access	



3		Should have template option to push common policy across all SDWAN solution	
4		Must have dashboard showcasing all the SDWAN solution across the network with their latency and link status	
5		Centralized management should have open APIs to integrate with third party management	
6		Centralized management should support role-based access	
7		Management must support IPSec wizard which can push VPN configuration to various SDWAN devices with the routing information updates.	
1	Logging & Reporting	The Logs and Reporting platform must be a dedicated same OEM appliance and VM/software running on server will not be accepted.	
2		The Logs and Reporting platform support running on-demand and scheduled reports	
3		Should have minimum 10 TB of Hard Drive Capacity in RAID 1, for logging and reporting if provided as separate management as from firewall.	
4		Real-time display of information allows you to follow real-time trends in network usage such as the source IP address and the destination URL for HTTP traffic or IM message traffic.	
5		All log files and messages are searchable and can be filtered to drill down and locate specific information.	
6		The logging Appliance should support multiple types of report format PDF, HTML, CSV and XML.	
1	Licensing	All license for Monitoring, management, VPN and Logging should be quoted. Vendor should quote all the license from day one related to proper SD-WAN deployment and all the feature requested above.	
2		License for any unmentioned feature which require proper deployment and functioning of SD-WAN must be quoted. Vendor shouldn't have any hidden charges	



1	Performance Parameter	The SDWAN device at C3i should have minimum 10x 1GE RJ45 ports and 4x 1G SFP or better and 4X10 SFP+ Optical ports to cater to connectivity from multiple service providers. Additional HA ports, Console and OOB should be provided extra. SFPs Transceivers should be populated as per solution requirement from Day1.	
2		IPSec encryption throughput should be 2 Gbps.	
3		Minimum 50K new session per second, 1 Mn concurrent session, 2000 Site to Site VPN	
4		SDWAN device should support minimum 2 Gbps of Threat Protection Throughput including Firewall, IPS, Application Control and antivirus Protection enabled with mix/application mix production traffic	
5		Minimum 2 Gbps of Application Control Throughput on SDWAN device the device should have Redundant Power Supplies and hot swappable fan tray.	

Layer 2 Network Switches - 24 Ports

S No.	Features	Description of Specs	Compliance (Yes/ No) with comments, if any
1.	Interface requirements	Minimum of 24 ports 10/100/1000 Base-T and 4x 10G SFP+ ports	
2.		1 x Out of Band IP based management Port, 1 Console Port, USB Port / External Flash	
3.		support stacking for upto 8 switches with minimum 40 Gbps stacking.	
4.		Have Redundant Power Supply support and variable speed fan to adjust to varying weather conditions in campus	
1.	Design & Performance	Each switch should have minimum 128 Gbps or more with non-blocking architecture and Forwarding rate of 95 Mpps	
2.		Should be equipped with minimum 1GB RAM and 1GB flash	



3.		Should have LED indicator for per port status, FAN, PSU and Management Status	
4.		0°C to 50°C operating temperature and 10% to 95% relative humidity	
5.		Hardware and software configuration have for Ipv6 from day one	
1.	Switching / Routing	Should have 16 K MAC Address, 4000 active Vlans	
2.		Should support 10 K ARP entries	
3.		802.1D spanning Tree and PVST+, 802.1w, 802.1s, should have BPDU Guard or equivalent feature on edge port to auto disable port for a configurable time period to if an accidental loop occurs in the network	
4.		Audio Video Bridging to enable reliable, real-time audio/video transmission over Ethernet	
5.		Should support aggregating and load balancing of traffic to two or more peer switches within same VLAN	
6.		Should support G.8032 standard based protocol for ring backbone	
7.		Should have Port based VLAN, MAC based VLAN, private vlan and 802.1 AK for dynamic VLAN propagation	
8.		Should have Local, Remote and multisession port mirroring (minimum 4 session)	
9.		Support Standard based protocols for lossless transport of real time data with dynamic QoS reservation.	
10.		Should have 8 Hardware QoS Queues per port	
11.		Should have traffic rate limiting with Configurable bandwidth granularity of 8 KBps	
12.		Should have Link Layer Discovery Protocol (802.1ab) to allow recognition of third-party network devices and LLDP MED for auto configuration	
13.		Should have MAC address tracking and notification for mac address addition, delete or movement in the Network	
14.		Should support policy-based routing and switching	
15.		Should have basic dynamic routing protocols like RIP from day one and be upgradeable to OSPF, PIM, VRRP	



16		Must Support RFC 3619 for sub 50 ms failover and it should seamlessly integrate with Core and Distribution	
17		Should have Configurable multicast session limit per port	
1.	Security	Local authentication database for RADIUS Authentication for 802.1x login	
2.		Should have MAC security – Lockdown & Limit and MAC address tracking with syslog & snmp notification	
3.		Should have SSH-2, SCP, SFTP for secure management	
4.		Should have dynamic arp inspection, DHCP snooping, Private VLAN, SYN attack protection, GARP protection	
5.		Should have ASIC based traffic flow analysis based on Netflow/ sFlow/ Ipfix	
6.		Should have minimum 1 K ACL entry support and Time-Based ACL	
1.	Management	Should have scheduled archiving / uploading of configuration and system log to a central server	
2.		Should support inbuilt DHCP server and Client for quick configuration of endpoints and switch	
3.		Telnet server, ssh server, Ping and traceroute over Ipv6	
4.		Should have L2 Traceroute, L2 Ping and Multicast Traceroute	
5.		Web, Console and CLI management	
6.		Dual firmware and configuration rollback	
7.		Should be SDN capable with Open stack support and OpenFlow API support, should support IEEE P802.1Qaz	
8.		Inbuilt browser-based bandwidth monitoring	
9.		Should support Energy Efficient Ethernet 802.3az	
1.	Certification	Model should have safety and standards certifications as below: IEC & CISPR certificates as below : IEC61000-4-6:2008/EN61000-4-6:2009, IEC61000-4-8:2009/EN61000-4-8:2010 , EN 55022:2010 Class A, CISPR 22:2008 Class A, CISPR24:201 OClassA, Radiated Immunity 10V/criteria, UL60950-1 2ndEd, CE 2.0 Compliant or equivalent Indian standards	
2.		Seamless Integration: For Seamless Integration and Interoperability all the switches and SFP	



		Modules should be fully compatible for smooth functioning of the system	

Network Racks 16U

Sr.	Parameter	Specification	Compliance (Yes/ No) with comments, if any
1	Rack Mount Depth	Standard Depth: 29" (736 mm)	
2		Adjustment Range: 6" to 30" in 1" increments (152 - 762 mm)	
3		Internal Space: 37.25" (946 mm)	
4		Front Space: 1.5" (38 mm) *	
5		Rear Space: 6.75" (171 mm) *	
6	Weight Capacity	1200 lbs. (544 kgs)	
7		Rated capacity on leveling feet (without casters)	
8	Rack Outside Dimensions	40" x 24" x 36.58" (1016 x 607 x 930 mm)	
9		D x W x H	
10	Included Hardware	(2) keys	
11	Hole Type	EIA 3/8" square holes	
12	Rack Post Shape	L Shape	
13	Rack Ventilation	80% perforation on doors.	
14	Rack Doors	Removable, Lockable and Reversible.	
15	Rack Sides	Removable and Lockable	
16	Smart closet feature	Integrated Solution having Cooling, Biometric Secure, Safety & Security and Monitoring at Rack level.	
17	Cooling Options	500W or more	

10KVA UPS with 30 min battery backup at 80% load

Sr. No	Specifications	Requirement	Compliance (Yes/ No) with comments, if any
1.	Capacity	10 KVA / 9 KW	
2.	Technology	IGBT (Rectifier & Inverter both); ECO Mode required Inbuilt Input Isolation Transformer	
3.	Wave form & Freq converter	Pure Sine wave & shall have frequency converter mode	
4.	Display	LCD	



5.	Input power factor correction	0.99 at 100% Linear load	
6.	Input configuration	3Ph, L-N+PE, +/- 10% on full load	
7.		UPS Shall have inbuilt Input Isolation Transformer	
8.	Frequency (Input)	45 to 55 Hz frequency (or 54 to 66 Hz for 60Hz Output)	
9.	Frequency (output)	50Hz or (selectable to 60Hz)	
10.	Output Voltage	220/230/240Vac shall be available with +/-1% regulation	
11.	Output Voltage Distortion	< = 3% max full linear load	
12.	Output Power factor	0.9	
13.	Crest factor	3 or better	
14.	AC-AC Efficiency	Online Mode: Greater than or equal to 88% @ Full Rated Load & Battery Fully charged	
15.	Transfer time Main-Battery	0	
16.	Transfer time Inverter-Bypass	4 msec	
17.	Output Connection	Hardwired Terminal Block required	
18.	Monitoring software for UPS	Shall be provided for monitoring of UPS from remote along with SNMP Card, this project being of high security & safety the SNMP card. shall be in compliance to global cyber security i.e. UL 2900-1 and IEC 62443-4-2 both as mandatory requirement or equivalent Indian standards	
19.	Communication	SNMP	
20.	Port	RS 232	
21.	Battery Type	12V SMF.	
22.	Battery backup	10KVA UPS with 30 min battery backup at 80% load (9984 VAH or more)	
23.	Charger	Shall be minimum 10% of the offered Battery AH	
24.	Battery Flexibility	32 to 40 Battery Flexibility required	
25.	EPO	Shall be available	
Environmental Parameter			



A	Operating temperature range	0-40 deg C	
B	Other	Indication required -> Over Temperature, Load on Battery, Battery low, Mains ON	
C	Humidity	5% to 95% no-condensing	
D	Noise Level	70 dBA max.	
E	Mounting	Tower type only (Rack Mount type not acceptable)	
F	EPO	Shall be available	
26	Protection	IP20	
27	LCD Display		
27.a	Measurements (On LCD)	Input & Output Voltage, Input & Output Frequency, Bypass: Voltage & Frequency, DC Voltage, Remaining time	
28	Manufacturer	Manufacturer -> ISO 9001, ISO 14001, OEM Plant should have water & air pollution control clearance certificate from respective govt. agency. UPS OEM should have registered office in India from last 10 years (certificate of incorporation to be provided)	
29	Product	CE Certified	
30	Management Supports /Software	Windows 7 / 8 or latest, Linux, Unix	

Comfort AC 1.5/2 Ton

- Comfort AC 1.5/2 Ton is mention under Non-IT part of C3i

Edge Gateway for Community Surveillance

Sr. No	Technical Specification	Compliance (Yes/No) with comments, if any
1.	IoT based edge gateway devices will be procured as an integral part of the project solution. It will be used for connecting the feeds of existing cameras reporting to Police Stations/Police District offices or will act as a hub for the SWAT team. The Edge Gateway appliances will be placed in the offices as per need basis.	



	The primary purpose of the gateway is to provide critical situational awareness solution by accessing live video feeds from surveillance system installed in public and private institutions. The gateway with embedded software will have the ability to connect with 3rd Party VMS software/NVR System deployed in the public or private institutions and act as a gateway to get the live cameras feeds into ICCV/ C4I/ VMS application is made available. Live video feed streaming should not have any dependency in any format on the 3rd Party VMS or NVR Systems deployed in the private or public institutions where such gateway would be deployed. The communication between Edge Gateway and VMS/C4I application at command centers or any other location will be secured and encrypted. The Gateway will have the native intelligence to the stream live video with dependency only on the network infrastructure of the 3rd party system and under no circumstances the solution depend/ intervene on 3rd party solution deployed except accessing the live video feeds from the CCTV cameras deployed at sites. The device/ software must be Cyber Security hardened. • Intel SOC based chipset • Min 4 GB or better memory • Min 32 GB SSD or better storage • Min 2*HDMI Ports • Min 2*1 G LAN Ports • Min 2*USB Ports • Min 1*PCI Expansion slot • Operating Temperature 0-50 Degrees • Mounting Options: Wall, VESA or DIN Rail Based • Must be light and easy to carry	



Joystick for PTZ camera at Workstation

Sr. No.	Specification	Description	Compliance (Yes/ No) with comments, if any
1.	VMS Compatibility	The Joystick must be compatible with all distributed network video management components.	
2.	Technology	Six-degrees-of-freedom (6DoF) sensor - Intuitively and precisely navigate digital models or camera positions in 3D space.	
3.	Design	The full-size, soft-coated hand rest positions the hand comfortably, and 15 large, soft-touch, function keys allow quick access to frequently used commands.	
4.	Quick View Keys	Fingertip access to 12 views makes it easier to switch cameras	
5.	Function Keys	Easy access to 4 application commands for an optimized workflow.	
6.	Display	Provides a visual reminder of function key assignments on your computer screen	
7.	Modifier	Fingertip access to Ctrl, Shift, Alt and Esc keys saves time by reducing the need to move your hand between mouse and Joystick	
8.	Numpad	Allows direct numerical input into your application using your standard mouse rather than the Joystick	
9.	System flexibility	The Joystick must be part of an integrated system and shall be configured so any number can be added to the system. When combined with user interfaces (UIs), network storage managers (NSM's), encoders, IP cameras, and video consoles, the Joystick forms an integral part of a complete network-based video control system	
10.	Input Connector type (power Supply)	Universal Inter changeable	
11.	Joystick Interface	USB 2.0	
12.	Cable	USB	
13.	Joystick Module	Fully proportional PTZ, variable speed; with zoom, iris and focus controls	
14.	Operating temperature	0° to 40°C	

Civil Works and interiors of C3i

The details are enclosed in Section 3.1.3 of Chapter-3 of this RFP



4.8.13. Infrastructure at C2i (Police Station)

Workstations with 3 nos. 24" Monitors for C4I application Mike + webcam +speaker along with operator workstation

Workstation:			
Sr. No	Parameters	Technical Specifications	Compliance (Yes/No) with comments, if any
1.	Form Factor	Tower	
2.	Processor	Intel Xeon Processor, 8 Cores, 16 MB Cache, 3.8 Ghz base frequency, 4.7 Ghz Turbo frequency or higher processor	
3.	Operating System	Windows 10 Pro, 64bit or latest	
4.	Office	Microsoft office standard edition latest.	
5.	Chipset	Intel Workstation Chipset 400 Series or higher	
6.	Memory	32GB in combination of (4x8GB) DDR4 2666MHz Memory or higher	
7.	Hard Drive	1 TB SATA HDD	
8.	Graphic Card	Nvidia Quadro P2200 GPU or higher	
9.	Keyboard & Mouse	Wired Keyboard & Mouse (Same make as PC)	
10.	Monitor	Should be able to support min 3x 24" Full HD Monitor (min 23.8" diagonal screen size). Monitor should be of same make as of workstation.	
11.	PSU	80PLUS Gold Certified Energy Star Compliant	
12.	Expansion Slots	Minimum "1" PCIe x16 Gen3; "2" PCIe x4/x8 Gen3 and "1" M.2 or more	
13.	Network Card	Dual Intel Ethernet Connection 10/100/1000 or better	
14.	I/O	4 - USB 3.1 1 - USB 3.1 Type C 1 - Audio Jack/ Microphone & Headphone 4 - DisplayPort 2 - RJ45 Network Connector	
15.	Warranty	As mentioned in RFP	
Monitor			
Sr. No	Parameters	Technical Specifications	Compliance (Yes/No) with comments, if any
1.	Size	23.8" / 24" LED Monitor	
2.	Resolution	1920 X 1080 resolution Anti-glare, IPS, 16.7 Million colors	



3.	Aspect Ratio	16:9 Aspect Ratio,	
4.	Brightness	250 cd/m ² Brightness,	
5.	Mount	Tilt and Height-adjustable stand, pivot (rotation),	
6.	Ports	1 x DisplayPort, 1 x HDMI, 1 x VGA, 5 x USB, 72% color gamut,	
7.	Certification	TCO Certified	
8.	Prerequisite	Should be of the same make as of the workstation	
9.	Warranty	As mentioned in RFP	

LED Monitor- 55" Display

S No.	Parameter	Minimum Specification	Compliance (Yes/No) with comments, if any
1.	Technology	LED Based	
2.	Screen Size	55 inches diagonally (± 0.4 inches)	
3.	Resolution	4k (3840 x 2160 at 60 Hz)	
4.	Viewing Angle	178° / 178°	
5.	Brightness	350 cd/m ² (typical)	
6.	Contrast Ratio	4000:1 (typical)	
7.	Aspect Ratio	16:9	
8.	Input	2 x HDMI 2.0 1 x Display Port 1 x VGA 2 x USB Ports	
9.	Remote Management	Asset 1 x RJ45 1 x RS232	
10.	Duty Cycle	12/7	
11.	Certifications	UL/EN/CE/IEC/BIS certification for Safety and CE/FCC Certifications for EMC & Immunity.	
12.	Warranty	As mentioned in RFP	



Workstations for Display LED without Monitor

Workstation:		
Parameters	Technical Specifications	Compliance (Yes/No) with comments, if any
Form Factor	Tower	
Processor	Intel Xeon Processor, 8 Cores, 16MB Cache, 3.8Ghz base frequency, 4.7Ghz Turbo frequency or higher processor	
Operating System	Windows 10 Pro, 64bit or latest	
Office	Microsoft office standard edition latest.	
Chipset	Intel Workstation Chipset 400 Series or higher	
Memory	32GB in combination of (4x8GB) DDR4 2666MHz Memory or higher	
Hard Drive	256GB SSD	
Graphic Card	Nvidia Quadro P2200 GPU or higher	
Keyboard & Mouse	Wired Keyboard & Mouse (Same make as PC)	
Monitor	Should be able to support 55" LED monitors mentioned	
Expansion Slots	Minimum "1" PCIe x16 Gen3; "2" PCIe x4/x8 Gen3 and "1" M.2 or more	
Network Card	Dual Intel Ethernet Connection 10/100/1000 or better	
I/O	4 - USB 3.1 1 - USB 3.1 Type C 1 - Audio Jack/ Microphone & Headphone 4 - DisplayPort 2 - RJ45 Network Connector	
PSU	80PLUS Gold Certified Energy Star Compliant	
Warranty	As mentioned in RFP	



IP Phones

Sr. No	Parameter	Specification	Compliance (Yes/No) with comments, if any
1.	Protocols/Standards	SIP RFC3261, TCP/IP/UDP, RTP/RTCP, HTTP/HTTPS, ARP, ICMP, DNS (A record, SRV, NAPTR), DHCP, PPPoE, TELNET, TFTP, NTP, STUN, SIMPLE, LLDP, LDAP, TR-069, 802.1x, TLS, IPV6	
2.	Network Interfaces	Dual switched auto-sensing 10/100/1000 Mbps Gigabit Ethernet ports with integrated PoE	
3.	Graphic Display	Min 2.5-inch	
4.	Bluetooth	Yes, integrated	
5.	Feature Keys	8-line keys with up to 4 SIP accounts	
6.	Video Codec	Support for G.729A/B, G.711μ/a-law, G.726, G.722(wide-band), in-band and out-of-band DTMF (in audio, RFC2833, SIP INFO)	
7.	Auxiliary Ports	RJ9 headset jack	
8.	Telephony Features	Hold, transfer, forward, 4-way conference, call park, call pickup, shared-call appearance /bridged-line-appearance, downloadable phonebook, call waiting, call log XML	
9.	HD audio	Yes, HD handset and speakerphone with support for wideband audio	
10.	Language Support	English	
11.	Upgrade/Provisioning	Firmware upgrade via TFTP / HTTP / HTTPS, mass provisioning using TR-069 or AES encrypted XML configuration file	
12.	Power	Input:100-240V; Output: +12V, 0.5A Integrated Power-over-Ethernet (802.3af) Max power consumption: 6.4W (power adapter) or 6.49W (PoE)	
13.	Security	QoS Layer 2 QoS (802.1Q, 802.1P) and Layer 3 (ToS, DiffServ, MPLS) QoS User and administrator level passwords, 256-bit AES encrypted configuration file, SRTP, TLS, 802.1x or better	
14.	Compliance	FCC: Part 15 (CFR 47) Class B CE: EN55022 Class B; EN55024 Class B; EN61000-3-2; EN61000-3-3; EN60950-1 RCM: AS/ACIF	



		S004; AS/NZS CISPR22/24; AS/NZS 60950.1 or equivalent Indian standard	

Secured Network Devices (SD-WAN Enabled Routers)

Sr. No	Features	Specifications	Compliance (Yes/No) with comments, if any
1.	General	Proposed vendor must be placed in Leader and Challengers Quadrant in Gartner SD-WAN or leader Gartner quadrant for Enterprise Firewall. NSS recommended vendor shall be preferred.	
2.		The SDWAN device should be supplied with Redundant hot swappable Power supply shall support IPv6 like application identification, Zone protection, management etc. from Day-1	
1.	SDWAN Architecture	Proposed SDWAN solution should have management-based architecture and if management appliances/solution goes offline the SDWAN solution should keep on functioning without any issues. Must support build in GUI as well for any onsite changes if required.	
2.		The bidder shall propose at least one management solution as asked above.	
3.		Management architecture should have option to be deployed in HA if required in future.	
4.		Management architecture should support on premise Model as well as have option of hosting on cloud.	
5.		There should not be any impact on SDWAN data forwarding capability in case of complete disconnection of management	
6.		Management architecture should support Virtual Firewall/multi-tenancy and the proposed device shall minimally have Common Criteria and Internet Computer Security Association (ICSA) Certification and should not have any wireless code in the offered device or its family in hardware or software. Any work around this will not be accepted.	



7.		Management architecture should support rich policy constructs to manipulate routing information, access control, segmentation, Application control.	
8.		Solution should provide transport independence and should allow to use any transport like MPLS, Internet, 3G/4G/broadband, Point to Point link	
9.		Licensing of SD-WAN solution must be based on device capacity not on bandwidth capacity / restriction	
10.		Architecture must support zero touch deployment, so that minimum effort is required to deploy the solution	
1.	Operations	It should support multi-cast network	
2.		Network would be functional at the time of connectivity failure between controller and branch device.	
3.		System Should able to support of network elements to deploy any kind of topologies such as any-to-any, Hub-spoke and Partial mesh.	
4.		System should able to support Multiple WAN Links utilization and detecting blackouts & brownouts by supporting active / active load balancing & Fast session failover	
5.		System must support Diverse WAN including T1, E1, LTE, PPPoE, DSL, Fibre and Ethernet	
1.	Security	Solution should support build in NGFW feature (Anti Spyware, IPS, Anti-Virus and application control) to protect network against threats or external NGFW solution can be quoted separately	
2.		Management and SDWAN solution should communicate over encrypted channel	
3.		Solution must support templates to be applied to the groups of police station quickly	
4.		SDWAN Router should support strong encryption like AES 256 or higher	
5.		PACKET REDISTRIBUTION must be supported even over IPSec tunnel and it	



		should support sub second path failover and recovery.	
6.		Proposed solution must support creation of logical separate sub-domain within single physical devices to separate different kind of networks. The proposed device should be having at least 10 physical cores.	
7.		SDWAN solution should support integration with cloud based/appliance-based security solutions or should have inbuilt security features like content filtering and antivirus	
8.		SDWAN solution should support split tunneling to provide direct internet access from branch	
9.		SDWAN solution shall have built in feature to protect CPU under DoS/DDos attacks	
10.		SDWAN architecture should support application identification at layer-7 and should able to identify minimum 3000 applications natively or minimum throughput as mentioned above. It should also allow to define custom applications as per requirement	
1.	Routing and QoS	SDWAN solution should allow minimum 2 service providers at branch locations and 4 service providers at DC.	
2.		SDWAN solution should support BGP and Static routing	
3.		SDWAN solution should support performance SLA based on latency, packet loss, jitter or all 3 combined	
4.		SDWAN edge devices should support 802.1Q, sub interface, Inter VLAN routing	
5.		SDWAN solution should support rule-based routing based on Application, user, user group, source, destination or combination of any of them	
6.		SDWAN Solution should support rule creation based on Application or source address or destination address and each rule should have option to use different performance SLA	



7.		SDWAN should support QoS based on application	
8.		SDWAN device should support FEC (Forward Error correction) and DSCP matching	
9.		SDWAN device must support BGP additional path support and route-map	
10.		SDWAN device solution must support Auto VPN	
1.	Management	Management solution should be appliance/VM which must support around 300 SDWAN devices at Day 1 scalable to 1000. If VM option is quoted than server should be given along with all the necessary licenses	
2.		Management solution should have built in GUI which can be accessed by any popular browser and no extra software must be required to open management GUI access	
3.		Should have template option to push common policy across all SDWAN solution	
4.		Must have dashboard showcasing all the SDWAN solution across the network with their latency and link status	
5.		Centralized management should have open APIs to integrate with third party management	
6.		Centralized management should support role-based access	
7.		Management must support IPsec wizard which can push vpn configuration to various SDWAN devices with the routing information updates.	
1.	Logging & Reporting	The Logs and Reporting platform must be a dedicated same OEM appliance and VM/software running on server will not be accepted.	
2.		The Logs and Reporting platform support running on-demand and scheduled reports	
3.		Should have minimum 10 TB of Hard Drive Capacity, in RAID 1 for logging and reporting if provided as separate management as from firewall.	
4.		Real-time display of information allows you to follow real-time trends in network	



		usage such as the source IP address and the destination URL for HTTP traffic or IM message traffic.	
5.		All log files and messages are searchable and can be filtered to drill down and locate specific information.	
6.		The logging Appliance should support multiple types of report format PDF, HTML, CSV and XML.	
1.	Licensing	All license for Monitoring, management, VPN and Logging should be quoted. Vendor should quote all the license from day one related to proper SD-WAN deployment and all the feature requested above.	
2.		License for any unmentioned feature which requires proper deployment and functioning of SD-WAN must be quoted. Vendor shouldn't have any hidden charges	
1.	Performance Parameter	The SDWAN device at DC should have minimum 8x 1GE RJ45 ports Optical ports to cater to connectivity from multiple service providers. Console and OOB should be populated as per solution requirement from Day1.	
2.		IPSec encryption throughput should be 500 Mbps.	
3.		Minimum 4K new session per second, 50,000 concurrent session, 500 Site to Site VPN	
4.		SDWAN device should support minimum 200 Mbps of Threat Protection Throughput including Firewall, IPS, Application Control and antivirus Protection enabled with Enterprise mix/Application Mix production traffic	
		Minimum 500 Mbps of Application Control Throughput on SDWAN device. The device should have Redundant Power Supplies.	



Layer 2 Network Switches - 24 Ports

S No.	Features	Description of Specs	Compliance (Yes/ No) with comments, if any
1.	Interface requirements	Minimum of 24 ports 10/100/1000 Base-T and 4x 10G SFP+ ports	
2.		1 x Out of Band IP based management Port, 1 Console Port, USB Port / External Flash	
3.		support stacking for upto 8 switches with minimum 40 Gbps stacking.	
4.		Have Redundant Power Supply support and variable speed fan to adjust to varying weather conditions in campus	
1.	Design & Performance	Each switch should have minimum 128 Gbps or more with non-blocking architecture and Forwarding rate of 95 Mpps	
2.		Should be equipped with minimum 1GB RAM and 1GB flash	
3.		Should have LED indicator for per port status, FAN, PSU and Management Status	
4.		0°C to 50°C operating temperature and 10% to 95% relative humidity	
5.		Hardware and software configuration have for Ipv6 from day one	
1.	Switching / Routing	Should have 16 K MAC Address, minimum 500 active Vlans minimum	
2.		Should support 10 K ARP entries	
3.		802.1D spanning Tree and PVST+, 802.1w, 802.1s, should have BPDU Guard or equivalent feature on edge port to auto disable port for a configurable time period to if an accidental loop occurs in the network	
4.		Audio Video Bridging to enable reliable, real-time audio/video transmission over Ethernet	
5.		Should support aggregating and load balancing of traffic to two or more peer switches within same VLAN	
6.		Should support G.8032 standard based protocol for ring backbone	
7.		Should have Port based VLAN, MAC based VLAN, private vlan and 802.1 AK for dynamic VLAN propagation	
8.		Should have Local, Remote and multisession port mirroring (minimum 4 session)	



9.		Support Standard based protocols for lossless transport of real time data with dynamic QoS reservation.	
10.		Should have 8 Hardware QoS Queues per port	
11.		Should have traffic rate limiting with Configurable bandwidth granularity of 8 KBps	
12.		Should have Link Layer Discovery Protocol (802.1ab) to allow recognition of third-party network devices and LLDP MED for auto configuration	
13.		Should have MAC address tracking and notification for mac address addition, delete or movement in the Network	
14.		Should support policy-based routing and switching	
15.		Should have basic dynamic routing protocols like RIP on day one and be upgradeable to OSPF, PIM, VRRP	
16.		Must Support RFC 3619 for sub 50 ms failover and it should seamlessly integrate with Core and Distribution	
17.		Should have Configurable multicast session limit per port	
1.	Security	Local authentication database for RADIUS Authentication for 802.1x login	
2.		Should have MAC security – Lockdown & Limit and MAC address tracking with syslog & snmp notification	
3.		Should have SSH-2, SCP, SFTP for secure management	
4.		Should have dynamic arp inspection, DHCP snooping, Private VLAN, SYN attack protection, GARP protection	
5.		Should have ASIC based traffic flow analysis based on Netflow/ sFlow/ Ipfix	
6.		Should have minimum 1 K ACL entry support and Time-Based ACL	
1.	Management	Should have scheduled archiving / uploading of configuration and system log to a central server	
2.		Should support inbuilt DHCP server and Client for quick configuration of endpoints and switch	
3.		Telnet server, ssh server, Ping and traceroute over Ipv6	
4.		Should have L2 Traceroute, L2 Ping and Multicast Traceroute	
5.		Web, Console and CLI management	
6.		Dual firmware and configuration rollback	



7.		Should be SDN capable with Open stack support and OpenFlow API support, should support IEEE P802.1Qaz	
8.		Should support Energy Efficient Ethernet 802.3az	
9		Inbuilt browser-based bandwidth monitoring	
1.	Certification	Model should have safety and standards certifications like IEC & CISPR as below : IEC61000-4-6:2008/EN61000-4-6:2009, IEC61000-4-8:2009/EN61000-4-8:2010 , EN 55022:2010 Class A, CISPR 22:2008 Class A, CISPR24:201 OClassA, Radiated Immunity 10V/criteria, UL60950-1 2ndEd, CE 2.0 Compliant or equivalent Indian standards	
2.		Seamless Integration: For Seamless Integration and Interoperability all the switches and SFP Modules should be fully compatible for smooth functioning of the system	

Network Racks 16U

Sr.	Parameter	Specification	Compliance (Yes/No) with comments, if any
1.	Rack Mount Depth	Standard Depth: 29" (736 mm)	
2.		Adjustment Range: 6" to 30" in 1" increments (152 - 762 mm)	
3.		Internal Space: 37.25" (946 mm)	
4.		Front Space: 1.5" (38 mm) *	
5.		Rear Space: 6.75" (171 mm) *	
6.	Weight Capacity	1200 lbs. (544 kgs)	
7.		Rated capacity on leveling feet (without casters)	
8.	Rack Outside Dimensions	40" x 24" x 36.58" (1016 x 607 x 930 mm)	
9.		D x W x H	
10.	Included Hardware	(2) keys	
11.	Hole Type	EIA 3/8" square holes	
12.	Rack Post Shape	L Shape	
13.	Rack Ventilation	80% perforation on doors.	
14.	Rack Doors	Removable, Lockable and Reversible.	
15.	Rack Sides	Removable and Lockable	
16.	Smart closet feature	Integrated Solution having Cooling, Biometric Secure, Safety & Security and Monitoring at Rack level.	
17.	Cooling Options	500W or more	



3KVA UPS with 30 min battery backup at 80% load

Sr. No	Specifications	Requirement	Compliance (Yes/No) with comments, if any
1.	Capacity	3KVA	
2.	Technology	IGBT (Rectifier & Inverter both); ECO Mode required	
3.	Form Factor	Rack or Tower Type	
4.	Wave form	Pure Sine wave	
5.	Display	LCD	
6.	Input power factor correction	0.99 at 100% Linear load	
7.	Input configuration	Single Phase with ground (Input Voltage range 160VAC~275VAC)	
8.	Frequency (Input)	45-55Hz / 54-66Hz (extendable to 40~70HZ when load < 60%)	
9.	Frequency (output)	45-55Hz / 54-66Hz (extendable to 40~70HZ when load < 60%)	
10.	Output Voltage	Single phase with ground.	
11.	Output Voltage Distortion	< 1% THD@ linear load <5% @non-linear load	
12.	Output Power factor	Unity	
13.	Crest factor	3:1 or better	
14.	AC-AC Efficiency	95% @ 230V output with typical load	
15.	Transfer time Main-Battery	0 ms	
16.	Transfer time Inverter-Bypass	0 ms	
17.	Output Connection	Hardwired Terminal Block required	
18.	Monitoring software for UPS	Shall be provided for monitoring of UPS from remote along with SNMP Card.	
19.	Communication	SNMP	
20.	Port	RS 232	
21.	Battery Type	12V SMF as per 3KVA	
22.	Battery backup	6KVA UPS with 30 min battery backup at 80% load (4950 VAH or more)	
23.	Charger	Shall be minimum 10% of the offered Battery AH	
23.1	Battery Flexibility	16 to 20 Battery Flexibility required	
24	Environmental Parameter		
A	Operating temperature range	0-40 deg C	



B	Other	Indication required -> Over Temperature, Load on Battery, Battery low, Mains ON	
C	Humidity	0% to 95% no-condensing	
D	Noise Level	70 dBA max.	
E	Mounting	Rack or Tower type	
F	EPO	Shall be available	
25	Protection	IP20	
26	LCD Display		
26.1	Measurements (On LCD)	Input & Output Voltage, Input & Output Frequency, Bypass: Voltage & Frequency, DC Voltage, Remaining time	
27	Manufacturer	Manufacturer -> ISO 9001, ISO 14001, OEM Plant should have water & air pollution control clearance certificate from respective govt. agency.	
		UPS OEM should have registered office in India from last 10 years (certificate of incorporation to be provided)	
28.A	Product	CE Certified	
29	Management Supports /Software	Windows® 2000/ 2003 /XP/Vista/ 2008, Windows® 7 / 8, Linux, Unix	

10KVA UPS with 30 min battery backup at 80% load

Sr. No	Specifications	Requirement	Compliance (Yes/ No) with comments, if any
1.	Capacity	10 KVA / 9 KW	
2.	Technology	IGBT (Rectifier & Inverter both); ECO Mode required Inbuilt Input Isolation Transformer	
3.	Wave form & Freq converter	Pure Sine wave & shall have frequency converter mode	
4.	Display	LCD	
5.	Input power factor correction	0.99 at 100% Linear load	
6.	Input configuration	3Ph, L-N+PE, +/- 10% on full load	
7.		UPS Shall have inbuilt Input Isolation Transformer	
8.	Frequency (Input)	45 to 55 Hz frequency (or 54 to 66 Hz for 60Hz Output)	
9.	Frequency (output)	50Hz or (selectable to 60Hz)	
10.	Output Voltage	220/230/240Vac shall be available with +/-1% regulation	



11.	Output Voltage Distortion	< = 3% max full linear load	
12.	Output Power factor	0.9	
13.	Crest factor	3 or better	
14.	AC-AC Efficiency	Online Mode: Greater than or equal to 88% @ Full Rated Load & Battery Fully charged	
15.	Transfer time Main-Battery	0	
16.	Transfer time Inverter-Bypass	4 msec	
17.	Output Connection	Hardwired Terminal Block required	
18.	Monitoring software for UPS	Shall be provided for monitoring of UPS from remote along with SNMP Card, this project being of high security & safety the SNMP card.	
19.	Communication	SNMP	
20.	Port	RS 232	
21.	Battery Type	12V SMF.	
22.	Battery backup	10KVA UPS with 30 min battery backup at 80% load (9984 VAH or more)	
23.	Charger	Shall be minimum 10% of the offered Battery AH	
24.	Battery Flexibility	32 to 40 Battery Flexibility required	
25.	Environmental Parameter		
A	Operating temperature range	0-40 deg C	
B	Other	Indication required -> Over Temperature, Load on Battery, Battery low, Mains ON	
C	Humidity	5% to 95% no-condensing	
D	Noise Level	70 dBA max.	
E	Mounting	Tower type only (Rack Mount type not acceptable)	
F	EPO	Shall be available	
	Protection	IP20	
26.	LCD Display		



a.	Measurements (On LCD)	Input & Output Voltage, Input & Output Frequency, Bypass: Voltage & Frequency, DC Voltage, Remaining time	
b.	Manufacturer	Manufacturer -> ISO 9001, ISO 14001, OEM Plant should have water & air pollution control clearance certificate from respective govt. agency. UPS OEM should have registered office in India from last 10 years (certificate of incorporation to be provided)	
c.	Product	CE Certified	
d.	Management Supports /Software	Windows 7 / 8 or latest, Linux, Unix	

Network laser printer

Sr. No	Item	Specifications	Compliance (Yes/No) with comments, if any
1.	Print speed black (normal, A4)	Up to 25 ppm	
2.	Print quality black (best)	Up to 1200 x 1200 dpi	
3.	Print technology	Monochrome Laser	
4.	Duty cycle (monthly, A4)	Up to 15,000 pages	
5.	Recommended monthly page	volume 250 to 2000	
6.	Standard memory	Minimum 128 MB	
7.	Processor speed	Minimum 700 MHz	
8.	Paper handling standard/input	Up to 250-sheet input tray	
9.	Paper handling standard/output	Up to 150-sheet output bin	
10.	Media sizes supported	A4, A5, A6, B5, postcard	
11.	Media types supported	Paper, transparencies, postcards, envelopes, labels	
12.	Standard connectivity	Hi-Speed USB 2.0 port with USB data cable, Ethernet with RJ45 connectivity	
13.	Duplex printing	Automatic (standard)	



14.	Compatible operating systems	Microsoft Windows 7 Professional(64bit), Windows 8 Pro (64 bit), Windows 8.1, Windows 10, Server 2008 R2, Server 2012 R2, MAC OS 9.0, MAC OS X, Linux	
15.	Power requirements:	Input voltage 220 to 240 VAC (+/- 10%), 50 Hz (+/- 2 Hz);	
16.	Power consumption during printing	Less than 500W	
17.	Energy Efficiency	BEE or Energy Star certified	
18.	Front operating Panel	Graphical LCD display	

Civil Works and interiors of C2i

The details are enclosed in Section 3.1.4 of Chapter-3 of this RFP

Comfort AC 1.5 Ton

- Comfort AC 1.5 Ton is mention under Non-IT part of C2i

Joystick for PTZ camera at Workstation

Sr. No	Specification	Description	Compliance (Yes/ No) with comments, if any
1.	VMS Compatibility	The Joystick must be compatible with all distributed network video management components.	
2.	Technology	Six-degrees-of-freedom (6DoF) sensor - Intuitively and precisely navigate digital models or camera positions in 3D space.	
3.	Design	The full-size, soft-coated hand rest positions the hand comfortably, and 15 large, soft-touch, function keys allow quick access to frequently used commands.	
4.	Quick View Keys	Fingertip access to 12 views makes it easier to switch cameras	
5.	Function Keys	Easy access to 4 application commands for an optimized workflow.	
6.	Display	Provides a visual reminder of function key assignments on your computer screen	
7.	Modifier	Fingertip access to Ctrl, Shift, Alt and Esc keys saves time by	



		reducing the need to move your hand between mouse and Joystick	
8.	Numpad	Allows direct numerical input into your application using your standard mouse rather than the Joystick	
9.	System flexibility	The Joystick must be part of an integrated system and shall be configured so any number can be added to the system. When combined with user interfaces (UIs), network storage managers (NSM's), encoders, IP cameras, and video consoles, the Joystick forms an integral part of a complete network-based video control system	
10.	Input Connector type (power Supply)	Universal Inter changeable	
11.	Joystick Interface	USB 2.0	
12.	Cable	USB	
13.	Joystick Module	Fully proportional PTZ, variable speed; with zoom, iris and focus controls	
14.	Operating temperature	0° to 40°C	



4.8.14. Data Center and near Data Recovery Site Requirements

DC- Functional requirements & KPIs

Data Center will be the data bank and data engine with tier III architecture which stores the entire lot of live streaming feeds and the triggered transactional data at one place. All the field data from the field level devices will flow through robust Network and will be collected in the data bank for definite time period.

This Data Center will facilitate Police Officials to access the Data against Women and Child crime cases, suspicious acts, investigations, etc. to reach to a logical and evidence-based conclusions and reporting.

- a.** Data Center being created at PHQ should be of type Tier III.
- b.** The DC will be provided with an input of adequate bandwidth (46.75 gig approximately) that will be terminated to a MUX with multiple channels through a MPLS cloud.
- c.** Considering the integration of camera under the existing scheme, an additional 4 Gbps bandwidth has been provisioned for 1000 camera.
- d.** The MUX will provide an input to the L2 switches of 100GB throughput with consolidated (Multiple ISP connections) to single termination required for seamless and stable inputs from cameras. The MUX will provide an input to the L2 switches of 100GB throughput with consolidated ISP Multiple connections to single termination.
- e.** L2 48 port Switches are ToR switch and will be able for interconnection of multiple servers.
- f.** L2 48 Port switches will be used for NAS Storage and Server Connectivity with considering the distributed clustered Architecture Scale-Out Storage. 48 ports provide approx. 50 VMs a non-blocking path (in HA) to communicate with the storage.
- g.** SD-WAN will be the first security check for all data packets through every channel entering into Data Center.
- h.** SD-WAN gateway and controller provisioning at Data Center. It will be captive arrangement under the custody of Delhi Police. The SD WAN gateway router will function in HUB & Spoke model with its branch SD-WAN routers located at police Station and DHQs. The SD-WAN gateway will ensure the following:
 - i.** First level check on the packet flow at DC and branch offices, the branch offices will need not to be equipped with firewalls.
 - ii.** The SD-WAN will provide security from the internet-based threats to the DC through exposure from mobile applications.
 - iii.** It will complement the load balancing actions of a dedicated Network Load Balancer in case of multiple ISP on a multicast network. Also, it will ensure aggregation and redundancy with NLB and core switch.
- i.** The SD-WAN router will segregate the bandwidth into 1 gig of private internet and 69.574 Gig of intranet facility. However, 1 gig of dedicated bandwidth on internet through VPN sub-netting will be provisioned for interfacing the system with other applications like



- ITMS, CCTNS, etc. Also, the visuals of the VMS will be provisioned for Police Officials on the Mobile gadgets with device MAC binding and login credentials through a VPN tunnel.
- j.** The firewall/ UTM/ IPS will be provisioned considering 1000 VPN connections. This Firewall will ensure external and internal security concerns.
 - k.** The L3 switches of 48 port each will be provisioned for conducting distribution of multiple VLANs.
 - l.** A unified storage will be provisioned at the Data Center, which will cater to the raw inputs from field cameras and sensors for a periodicity of 30 days scale-out storage with min 12 to 24 controller architecture multiple controllers chosen to as to have a maximum of 2:1 ratio between VMS servers (VM's/physical) and controller This ensures that if a controller fails, and the VMS servers it was servicing move to another controller, the controller does not get chocked. The linear scalability of performance and capacity of every drive bay added, performance will increase by the same amount till the maximum capacity of the storage required. This Storage will be complimented with additional storage of 2 PiB to store the tagged and identified data from Video Analytics (VA) and VMS management tools for a period of 180 days.
 - m.** The Computing will be conducted in Racks equipped with precision cooling and power load factors as required.
 - n.** Bidder has to provide all the required network active and passive components. Network cables, Patch cords (with different colors for 1G, 10G and as per network topology), and patch panels (active). Bidders has to follow standard structured cabling mechanism. Bidder has to consider power cables as per quoted iPDU's.
 - o.** The necessary servers / applications for DC (C4i) will undergo / would be compliant to virtualization layers.
 - p.** The servers will be classified for CPU and GPU logical methodologies as per the requirement of operations. The direct streamlined logical Video Management calculations will be done through machine learning approach with CPU logics which will conduct physical to virtual scenario in 1:1 ratio. With respect to deep learning calculations for Visual Analytics and Artificial intelligence at ICCV platform, a combination of CPU and GPU logics will be required. Henceforth, the system will require a combination of Central Processing and Graphical Processing based servers.
 - q.** The required solution for Safe City needs to Media recording servers for distributed load factors at Data Center along with the Management Servers. Video Analytics Servers with 3x GPU in each server for 2500 cameras each will be required to handle all deep learning structured load with capability of managing minimum 2 use-cases per camera. Each GPU on the machine is capable to handle 40 use-cases on the camera' metadata. Therefore, one server is capable to handle 120 use-cases. Total no. of prime 5000 use-cases require $(5000/120) = 42$ servers
 - r.** The Face Recognition server must be capable to manage minimum 15 / 20 channels (cameras) simultaneously. Total envisaged cameras for FRS will be 370 no. Each FRS server is capable to execute operations on 20 channels/ cameras. Henceforth, total no. of FRS servers to handle 370 cameras need $(374/20) = 19$ servers, also, keeping 1 server for failover redundancy provision results to total no. of 20 servers to be provisioned.



- s.** The ANPR- Vehicle Surveillance server must be capable to manage minimum 30/40 channels (cameras) simultaneously. Each ANPR server will have 40 cores. Each core will cater to 1 ANPR channel/ camera. Henceforth, total 41 servers required, keeping failover redundancy in operation, 44 No. of ANPR analytical servers are provisioned with Open source platform.
- t.** There will be requirement of Lightweight Directory Access Protocol (LDAP) / Active Directory for enterprise wide user management, domain with anti-virus servers and viewing center servers.
- u.** There should be dedicated/shared rack space available in the Data Center for the City Surveillance Infrastructure. As of now provision of 30 racks will be made. However, the scalable arrangement for 36 racks will done.
- v.** It should have access control system implemented for secured access.
- w.** In case the Data Center services are to go down due to any unforeseen circumstance, the Command Center should have access to the critical / flagged data stored in near DR for the last 90/180 days or up to a storage capacity of 2PiB.
- x.** Receiving Power: Commercial power substation next to DC; UPS: UPS system with N+N redundancy (dual supply to rack floor for all IT equipment).
- y.** Monolithic UPS arrangement for dual supplies to IT load has been provisioned. 2 UPS of 400 KVA have been considered for the requirement of 350 KVA at DC for IT load. There will be adequate redundant arrangement for power solutions as follows:
 - Ensure redundancy with pool of 800 KVA capacity;
 - Dual sources being terminated at the rack floor for all IT equipment to ensure power backup of 15+15 (30) min collectively from both UPS. Power Provision: Dual power feed, PDU sources to each rack, Power supply to a rack as per requirement;
 - The above-mentioned arrangement will also ensure fall back arrangement for additional 150 KVA/200 KW requirements of C4i and PAC respectively.
 - The stack of SMF batteries along with the UPS arrangement will be made in the building' basement under AHU provisions.
- z.** Generator: Gen-set with N+N/1 redundancy for ensuring power generation backup arrangement parallel to streaming raw input requirement of 750 KVA that includes 350 KVA for IT load, 150 KVA for C4i and 200 KVA for PAC. Provision of 1000 KVA power generation will made on High Availability Mode.
- aa.** Cooling Features: The system will provision for raised floor AC equipment
- bb.** Extension of Server Infrastructure Zone: This zone has host servers, server racks, storage racks and networking components like routers, switches to passive components. All the infrastructure shall be extended as per requirement.
- cc.** Extension of UPS and Electrical Zone: Zone will have all the Un-Interrupted Power Supply units, Power Distribution Units (PDUs) to feed the UPS. It will be extended with Power Backup requirement and place UPS and Electrical Load extension. This shall also house all the batteries accompanying the UPS components.

- dd.** The near Data Recovery site will be capturing the storage of application and structured data (tagged) only as a backup facility for Data Center. The management server for C4i could be considered for hosting in near DR facility for high reliability and failover.
- ee.** The Electrical SLD and panelling drawing will be shared post the signing of the Non-Disclosure agreement with MSI.
- ff.** Internal Security audit - Half yearly for Network & Applications and operations
- gg.** External Security audit - Yearly for Network and Applications and operations
- hh.** Storage at Data Center:

The Storage at Data Center from all the Field Level Devices will be classified in three sections, as follows:

- i. Open consolidated- Public data;
- ii. Incident based data;
- iii. Core- critical data

Schematic for scale out Storage cluster Network (Open consolidated- Public data):

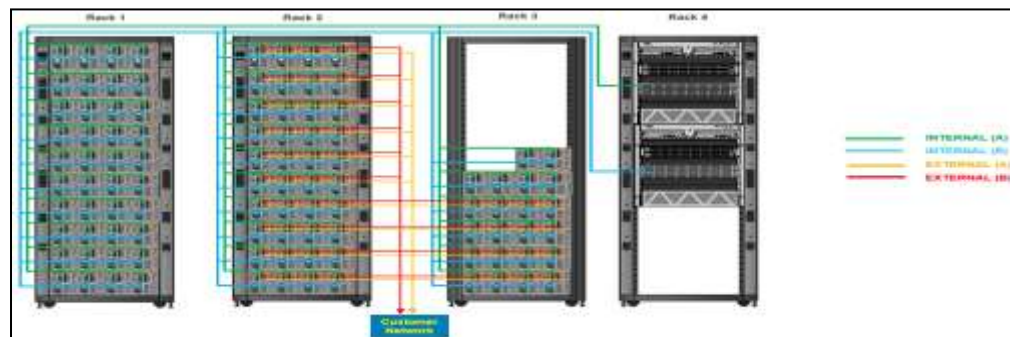


Figure: Scale-out Storage Cluster

It is being assumed that the structural data and battery room and the space allocated for outdoor units for cooling system along with vibration and noise level is being indicated to Delhi police and is currently under evaluation.

Approximately 20 PiB (Depending on the solution proposed) Scale out storage is needed to cater to continuous streams of HD videos from cameras. This will facilitate riddance from allocation of File System to a camera and handling the complexity of shifting the allocation as saturation occurs. The scale out concept will reduce the wastage of the file system remaining unused for the pre-defined time limits for recording data before weeding out. All the unstructured and the structured, cropped videos, snapshots, other bookmarked files by users will reside in other scale-out storage which can be defined for longer retention policy.

Storage will be capable of more than 25 GBPS throughput- at 100 % write on SMB2 and higher version for handling the camera feed and other work load. It will be configured with 20PiB usable capacity in single file system, using equal to or less than 12 TB or more (NL-SAS/ SATA/SSD HDD).

ii. Controllers and Architecture:

Storage will be distributed clustered Architecture written for Scale-Out Storage operations, scale out storage will be configured with minimum 12 controllers of the same type. Over all storage cluster will be upgradable to min 2 x numbers of Storage controllers/Storage nodes, without any disruptions/downtime to production workflow for performance, capacity enhancement, software/firmware upgrades. All storage nodes/controllers will be active for all Storage shares, contributing in performance and capacity of the system. The scale out storage will be configured with minimum 1.5 TB (total) federated/globally coherent or better, DRAM based cache/memory.

jj. DC Architecture

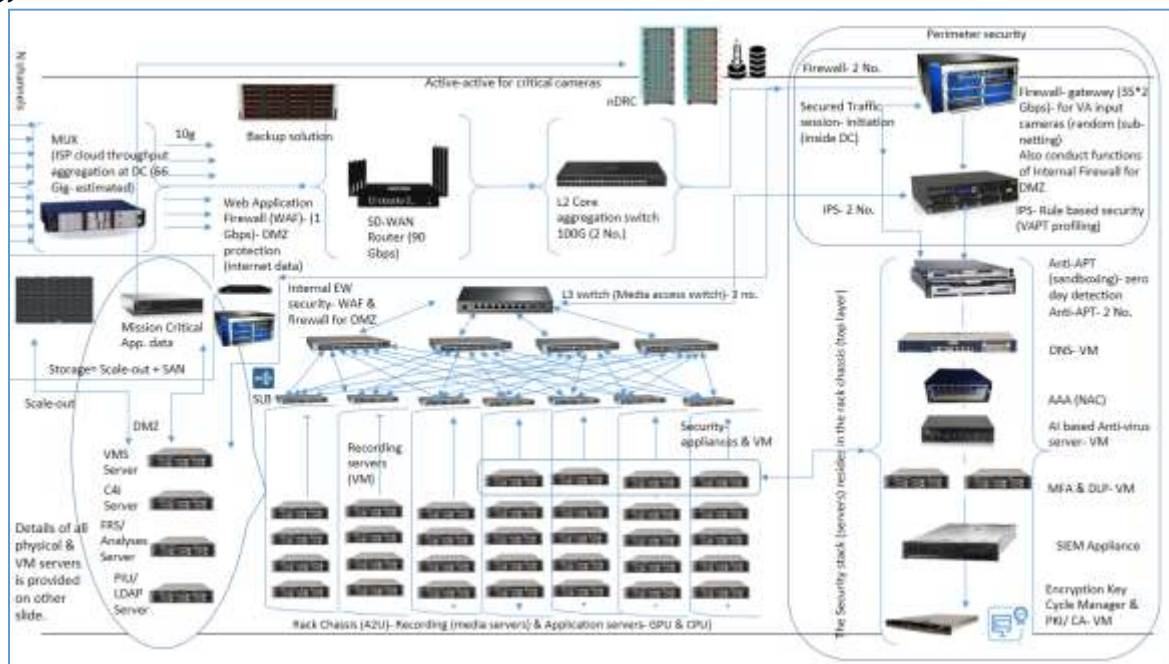


Figure: DC Architecture

kk. Rack Floor- servers, storage & security Appliances inside racks

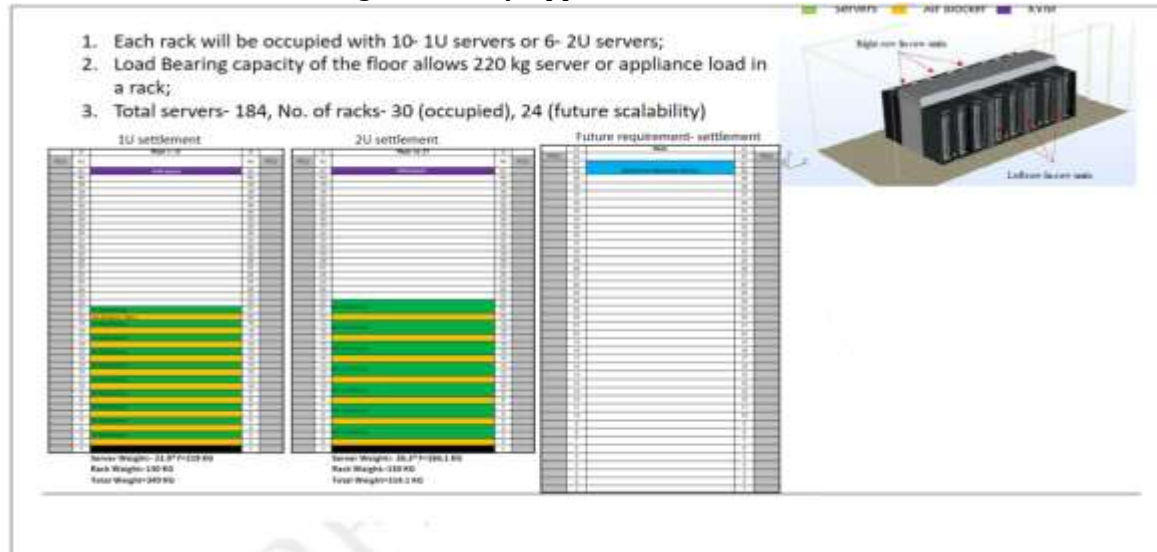


Figure: Rack Floor Architecture- IT Load Distribution

II. SAN Storage Cluster Network (for Incident based and core data):

Host Connectivity of storage:

SAN Storage will be used to store Management VM's, Data Backup of tag data, configured VM's image Backup data, OS ISO Data, infrastructure configuration backup, Surveillance application backups etc. The solution shall be configured efficiently for quick restoration of required data. The activities shall include but is not limited to

- Backup of operating system, database and application
- Monitoring and enhancement of the performance of scheduled backups, schedule regular testing of backups and ensure adherence to related retention policies
- Real-time monitoring, log maintenance and reporting of backup status on a regular basis

It will be a SAN/unified storage using FC connectivity with Storage Operating System optimized for end to end to handle different types of drives like SSD, SAS/NL-SAS technology with built in QoS (Quality of Services) for optimal utilization of resources across the array. The storage will be of capacity 2000TB (2 PiB) Usable Capacity, out of which 400TB Usable Capacity using SSD Drives on RAID6/RAID 5

Concept design & layouts

Data Center (DC) at PHQ 7th floor:

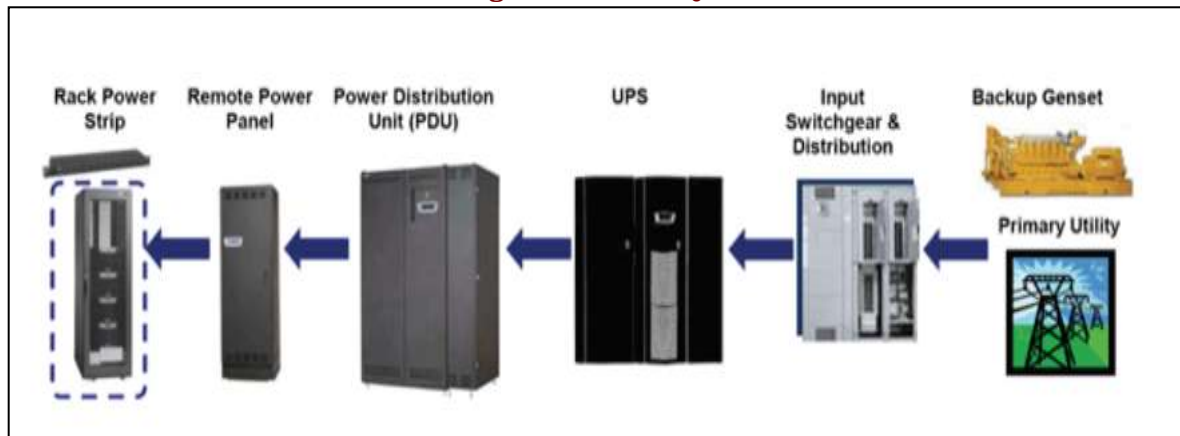
DC will occupy around racks of capacity as per given space, as safe city requirements are concern 33 racks of space including all servers, storage and Network components in centralized architecture framework will be required.

DC will occupy BMC room along with common NOC and SOC room for maintenance of Data Center IT Equipment's. Total 20TR PAC x 7 quantity equals to 140TR PAC will be used for

cooling, whereas 400 KVA UPS for Power to IT load with HA will be used. Power requirement for given infrastructure is around 260 KVA.

Racks and Power are extended looking towards future expansion in Data Center at single point of time.

Figure: DC at PHQ



Data Center will be equipped with Access Control- Biometric Entry/ Exit protocols for ensuring authorized access.



Figure: DC Access (biometric)- (Indicative diagram)

Date Center will be provisioned with leading NOVEC Fire Protection System.

NOVEC 1230 fluid is a sustainable fire extinguishing clean agent that helps protect continuity of operations and high value assets. It will be non-conductive and will leave no residue, putting out fires while preserving both assets and operations. NOVEC Gas Fire Suppression system for the UPS room will be provisioned separately.

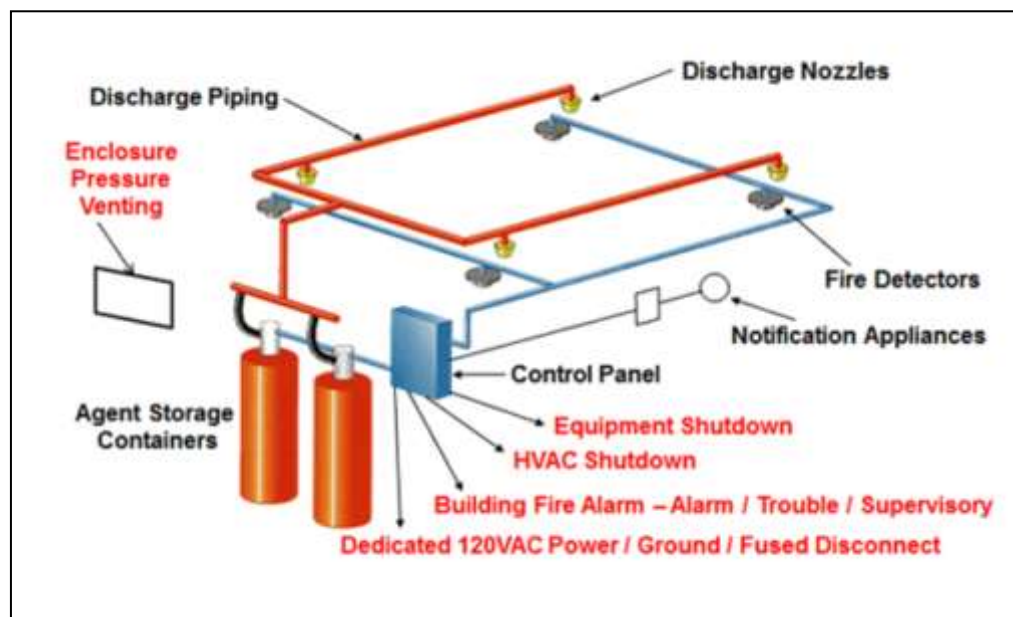


Figure: Fire Protection Layout

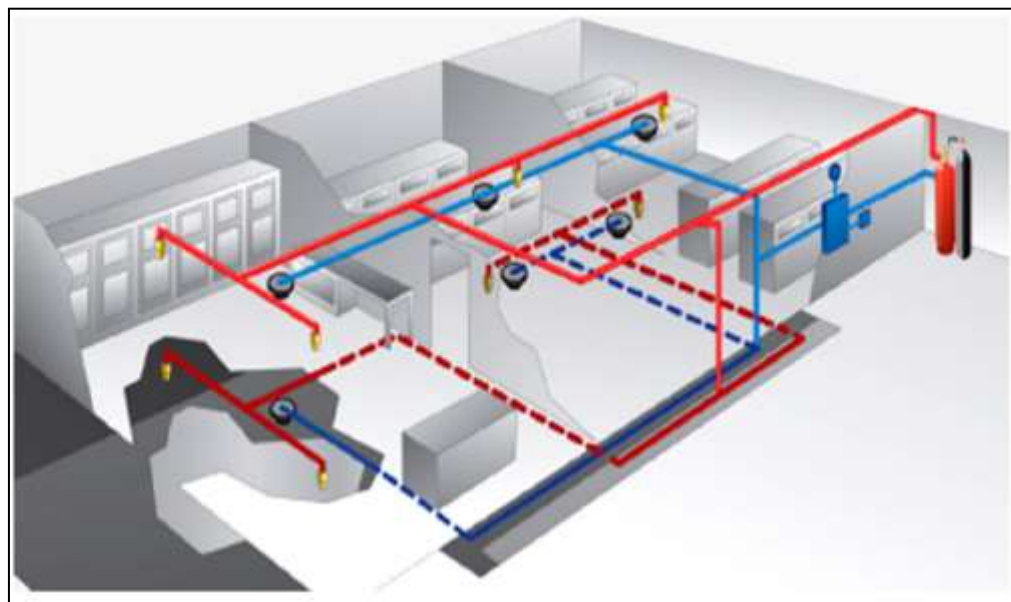


Figure: Fire Protection Layout

Raised Flooring and other essential components of DC

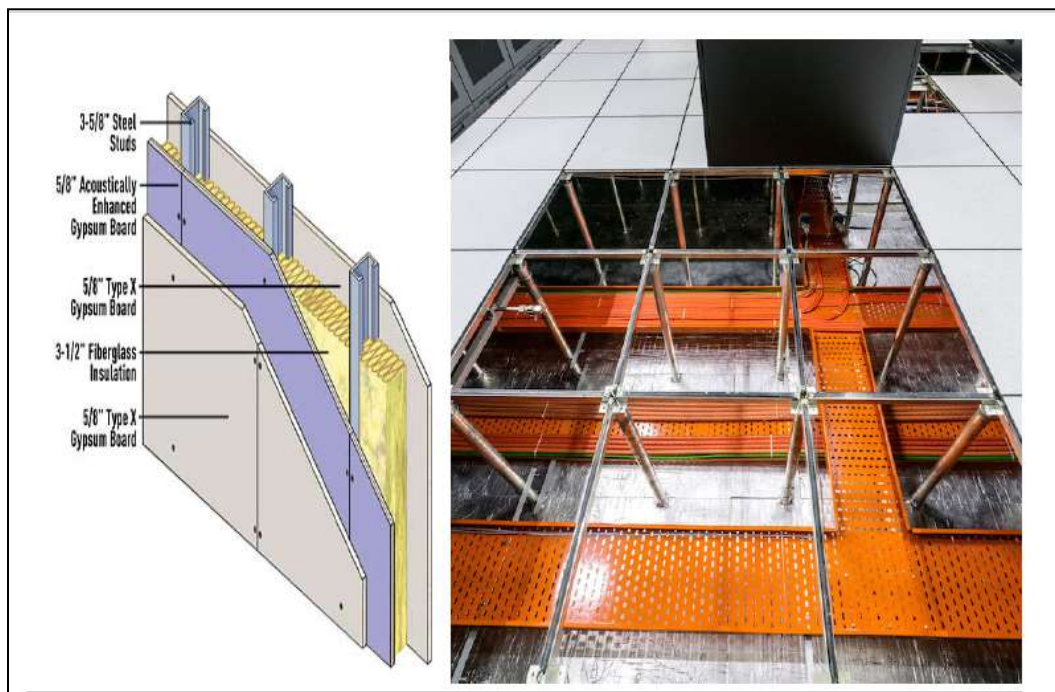


Figure: DC raised flooring

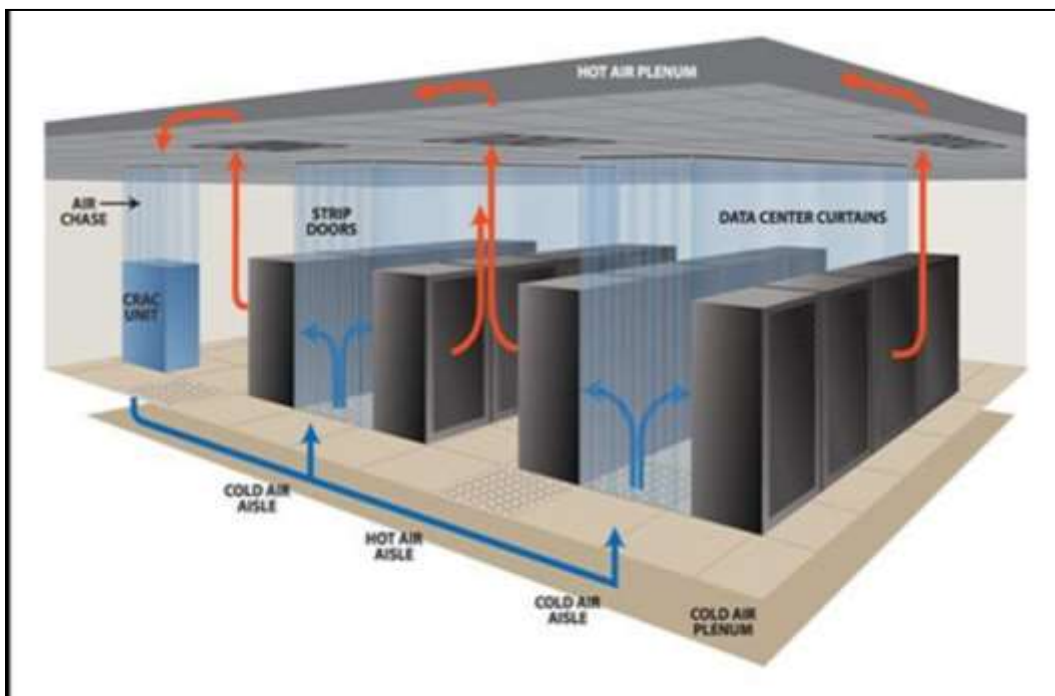


Figure: Hot & Cold Aisle Mechanism- flooring & ceiling



4.8.15. DC- Technical Requirements and Compliance Sheet for MSI Server

a. C4I Server

S No.	Parameter	Specifications	Compliance (Yes/ No) with comments, if any
	Make & Model		
1.	Form Factor	1U rack mounted with sliding rails	
2.	Processor	Up to two Intel® Xeon® Scalable 2nd Gen processors, up to 20 cores/processor @ 2.5 Ghz base freq. or equivalent or better.	
3.	Memory slots	16 DDR4 DIMM slots, speed up to 2666MT/s or better	
4.	Memory configured	Minimum 256 GB, scalable to 512GB	
5.	Disks supported	Front drive bays: Up to 10 x 2.5" SAS/SATA (HDD/SSD) with up to 2 NVMe SSD or higher.	
6.	RAID Controller	12Gbps PCIe 3.0 with RAID 1, 5, 10, 50 with 8GB Cache Memory on single / Multiple controllers.	
7.	Disks configured	3x 600GB 15K RPM SAS drives or higher.	
8.	1G Networking features	2 x 1 Gbps Copper Ethernet with Additional Dedicated Mgmt. Ethernet interface port with 3 mts. Length factory crimped copper Ethernet patch cords for each port including 1 mgmt. port	
9.	10G Networking features	4 x 10G Copper Ethernet ports with 3 mts. Length 10G factory crimped copper Ethernet patch cords for each port	
10.	FC HBA	Dual port 16 Gbps FC HBA with two no. of each 3 mts. Or 5 mts FC patch cables, Quoted HBA should support quoted SAN Switch and Storage	
11.	Certified for OS	Windows Server 2016 or higher, VMWare vSphere, vCenter, Red Hat Enterprise Linux, SUSE Linux Enterprise Server	
12.	Power Supply	Platinum rated redundant Power Supply	



13.	Management integration	Support for integration with Microsoft System Center, VMware vCenter, BMC Software	
14.	Power & temperature	Real-time power meter, thresholds, alerts & capping with historical power counters. Temperature monitoring	
15.	Pre-failure alert	Should provide predictive failure monitoring & proactive alerts of actual or impending component failure for fan, power supply, memory, CPU, RAID, NIC, HDD	
16.	Configuration & Management	• Real-time out-of-band hardware performance monitoring & alerting • Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management, monitoring of FC, HBA & system health if added will be advantage. • Out-of-band hardware & firmware inventory • Zero-touch auto configuration to auto deploy a baseline server configuration profile	
17.	LCD/LED panel	Should display system ID, status information and system error code followed by descriptive text on LED Indicator / LCD Panel.	
18.	HTML5 support	HTML5 support for virtual console & virtual media without using Java or ActiveX plugins	
19.	Server security	Should have a cyber resilient architecture for a hardened server design for protection, detection & recovery from cyber attacks	
		Should protect against firmware which executes before the OS boots	



		Should provide effective protection, reliable detection & rapid recovery using: - Signed firmware updates - Support for Hardware root of trust / Silicon based hardware root of trust - Secure default passwords - Configuration and firmware drift detection - Secure alerting - Rapid OS recovery	
		Configuration upgrades should be only with cryptographically signed firmware and software	
		Should provide system lockdown feature to prevent change (or “drift”) in system firmware image(s) & prevent malicious modification of server firmware	
20.	Warranty	As mentioned in RFP..	

b. Integration Servers

S No.	Parameter	Specifications	Compliance (Yes/ No) with comments, if any
	Make & Model	----	
1.	Form Factor	1U rack mounted with sliding rails	
2.	Processor	Up to two Intel® Xeon® Scalable 2nd Gen processors, up to 20 cores/processor @ 2.5 Ghz base freq. or equivalent or better.	
3.	Memory slots	16 DDR4 DIMM slots, speed up to 2666MT/s or better	
4.	Memory configured	Minimum 256 GB, scalable to 512GB	
5.	Disks supported	Front drive bays: Up to 10 x 2.5” SAS/SATA (HDD/SSD) with up to 2 NVMe SSD or higher.	
6.	RAID Controller	12Gbps PCIe 3.0 with RAID 1, 5, 10, 50 with 8GB Cache Memory on single / Multiple controllers.	
7.	Disks configured	3x 600GB 15K RPM SAS drives or higher.	



8.	1G Networking features	2 x 1 Gbps Copper Ethernet with Additional Dedicated Mgmt. Ethernet interface port with 3 mts. Length factory crimped copper Ethernet patch cords for each port including 1 mgmt. port	
9.	10G Networking features	4 x 10G Copper Ethernet ports with 3 mts. Length 10G factory crimped copper Ethernet patch cords for each port	
10.	FC HBA	Dual port 16 Gbps FC HBA with two no. of each 3 mts. Or 5 mts FC patch cables, Quoted HBA should support quoted SAN Switch and Storage	
11.	Certified for OS	Windows Server 2016 or higher, VMWare vSphere, vCenter, Red Hat Enterprise Linux, SUSE Linux Enterprise Server	
12.	Power Supply	Platinum rated redundant Power Supply	
13.	Management integration	Support for integration with Microsoft System Center, Vmware vCenter, BMC Software	
14.	Power & temperature	Real-time power meter, thresholds, alerts & capping with historical power counters. Temperature monitoring	
15.	Pre-failure alert	Should provide predictive failure monitoring & proactive alerts of actual or impending component failure for fan, power supply, memory, CPU, RAID, NIC, HDD	
16.	Configuration Management &	• Real-time out-of-band hardware performance monitoring & alerting • Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management, external storage management, monitoring of FC, HBA & system health if added will be advantage. • Out-of-band hardware & firmware inventory • Zero-touch auto configuration to	



		auto deploy a baseline server configuration profile	
17.	LCD/LED panel	Should display system ID, status information and system error code followed by descriptive text on LED Indicator / LCD Panel.	
18.	HTML5 support	HTML5 support for virtual console & virtual media without using Java or ActiveX plugins	
19.	Server security	Should have a cyber resilient architecture for a hardened server design for protection, detection & recovery from cyber attacks	
		Should protect against firmware which executes before the OS boots	
		Should provide effective protection, reliable detection & rapid recovery using: - Signed firmware updates - Support for Hardware root of trust / Silicon based hardware root of trust - Secure default passwords - Configuration and firmware drift detection - Secure alerting - Rapid OS recovery	
		Configuration upgrades should be only with cryptographically signed firmware and software	
		Should provide system lockdown feature to prevent change (or “drift”) in system firmware image(s) & prevent malicious modification of server firmware	
	Warranty	As mentioned in RFP.	



c. Video Management Servers

S No.	Parameter	Specifications	Compliance (Yes/No) with comments, if any
	Make & Model		
1.	Form Factor	1U rack mounted with sliding rails	
2.	Processor	Up to two Intel® Xeon® Scalable 2nd Gen processors, up to 20 cores/processor @ 2.5 Ghz base freq. or equivalent or better	
3.	Memory slots	16 DDR4 DIMM slots, speed up to 2666MT/s or better	
4.	Memory configured	Minimum 256 GB, scalable to 512GB	
5.	Disks supported	Front drive bays: Up to 10 x 2.5" SAS/SATA (HDD/SSD) with up to 2 NVMe SSD or higher.	
6.	RAID Controller	12Gbps PCIe 3.0 with RAID 1, 5, 10, 50 with 8 GB Cache Memory on single / Multiple controllers.	
7.	Disks configured	3x 600GB 15K RPM SAS drives or higher.	
8.	1G Networking features	2 x 1 Gbps Copper Ethernet with Additional Dedicated Mgmt. Ethernet interface port with 3 mts. Length factory crimped copper Ethernet patch cords for each port including 1 mgmt. port	
9.	10G Networking features	4 x 10G Copper Ethernet ports with 3 mts. Length 10G factory crimped copper Ethernet patch cords for each port	
10.	FC HBA	Dual port 16 Gbps FC HBA with two no. of each 3 mts. Or 5 mts FC patch cables, Quoted HBA should support quoted SAN Switch and Storage	
11.	Certified for OS	Windows Server 2016 or higher, VMWare vSphere, vCenter, Red Hat Enterprise Linux, SUSE Linux Enterprise Server	
12.	Power Supply	Platinum rated redundant Power Supply	
13.	Management integration	Support for integration with Microsoft System Center, VMware vCenter, BMC Software etc.	



14.	Power & temperature	Real-time power meter, thresholds, alerts & capping with historical power counters. Temperature monitoring	
15.	Pre-failure alert	Should provide predictive failure monitoring & proactive alerts of actual or impending component failure for fan, power supply, memory, CPU, RAID, NIC, HDD	
16.	Configuration & Management	• Real-time out-of-band hardware performance monitoring & alerting • Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management, external storage management, monitoring of FC, HBA & system health if added will be advantage. • Out-of-band hardware & firmware inventory • Zero-touch auto configuration to auto deploy a baseline server configuration profile	
17.	LCD /LED panel	Should display system ID, status information and system error code followed by descriptive text on LED Indicator / LCD Panel.	
18.	HTML5 support	HTML5 support for virtual console & virtual media without using Java or ActiveX plugins	
19.	Server security	Should have a cyber resilient architecture for a hardened server design for protection, detection & recovery from cyber attacks	
		Should protect against firmware which executes before the OS boots	
		Should provide effective protection, reliable detection & rapid recovery using: - Signed firmware updates - Support for Hardware root of trust / Silicon based hardware root of trust - Secure default passwords - Configuration and firmware drift detection - Secure alerting - Rapid OS recovery	



		Configuration upgrades should be only with cryptographically signed firmware and software	
		Should provide system lockdown feature to prevent change (or “drift”) in system firmware image(s) & prevent malicious modification of server firmware	
20.	Warranty	As mentioned in RFP.	

d. Video Recording Servers

S No.	Parameter	Specifications	Compliance (Yes/No) with comments, if any
1.	Make & Model	-----	
2.	Form Factor	1U rack mounted with sliding rails	
3.	Processor	Up to two Intel® Xeon® Scalable 2nd Gen processors, up to 20 cores/processor @ 2.5 Ghz base freq. or equivalent or better	
4.	Memory slots	16 DDR4 DIMM slots, speed up to 2666MT/s or better	
5.	Memory configured	Minimum 128 GB, scalable to 512GB	
6.	Disks supported	Front drive bays: Up to 10 x 2.5” SAS/SATA (HDD/SSD) with up to 2 NVMe SSD or higher.	
7.	RAID Controller	12Gbps PCIe 3.0 with RAID 1, 5, 10, 50 with 8 GB Cache Memory on single / Multiple controllers.	
8.	Disks configured	3x 600GB 15K RPM SAS drives or higher.	
9.	1G Networking features	2 x 1 Gbps Copper Ethernet with Additional Dedicated Mgmt. Ethernet interface port with 3 mts. Length factory crimped copper Ethernet patch cords for each port including 1 mgmt. port	
10.	10G Networking features	4 x 10G Copper Ethernet ports with 3 mts. Length 10G factory crimped copper Ethernet patch cords for each port	
11.	FC HBA	Dual port 16 Gbps FC HBA with two no. of each 3 mts. Or 5 mts FC patch cables, Quoted HBA should support quoted SAN Switch and Storage	



12.	Certified for OS	Windows Server 2016 or higher, VMWare vSphere, vCenter, Red Hat Enterprise Linux, SUSE Linux Enterprise Server	
13.	Power Supply	Platinum rated redundant Power Supply	
14.	Management integration	Support for integration with Microsoft System Center, VMware vCenter, BMC Software	
15.	Power & temperature	Real-time power meter, thresholds, alerts & capping with historical power counters. Temperature monitoring	
16.	Pre-failure alert	Should provide predictive failure monitoring & proactive alerts of actual or impending component failure for fan, power supply, memory, CPU, RAID, NIC, HDD	
17.	Configuration Management &	• Real-time out-of-band hardware performance monitoring & alerting • Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management, external storage management, monitoring of FC, HBA & system health if added will be advantage. • Out-of-band hardware & firmware inventory • Zero-touch auto configuration to auto deploy a baseline server configuration profile	
18.	LED/LCD panel	Should display system ID, status information and system error code followed by descriptive text on LED Indicator / LCD Panel.	
19.	HTML5 support	HTML5 support for virtual console & virtual media without using Java or ActiveX plugins	
20.	Server security	Should have a cyber resilient architecture for a hardened server design for protection, detection & recovery from cyber attacks	
		Should protect against firmware which executes before the OS boots	



		Should provide effective protection, reliable detection & rapid recovery using: - Signed firmware updates - Support for Hardware root of trust / Silicon based hardware root of trust - Secure default passwords - Configuration and firmware drift detection - Secure alerting - Rapid OS recovery	
		Configuration upgrades should be only with cryptographically signed firmware and software	
		Should provide system lockdown feature to prevent change (or “drift”) in system firmware image(s) & prevent malicious modification of server firmware	
21.	Warranty	As mentioned in RFP.	

e. Video Analytics Servers

Video Analytics Servers with 3x GPU in each server for 2500 cameras each having 2 use cases on an average.

S No.	Parameter	Specifications	Compliance (Yes/No) with comments, if any
	Make & Model		
1.	Rack Height	2U rack mounted with sliding rails	
2.	Processors	Up to two Intel® Xeon® Scalable 2nd Gen processors, configured with 20 cores/processor @ 2.5 Ghz base freq. or equivalent or better	
3.	Memory	128 GB RAM 2666 MT/s support up to 512GB RAM, should have min. 24 DIMM slots	
4.	Hard Drives	5x 600GB 15K RPM SAS drives should be configured. Should support up to eight hard disk drives (SAS, SATA, SSD)	
5.	GPU Configured	Should be configured with 3 nos. of Nvidia Tesla T4 GPU. or equivalent or better	
6.	GPU Support	Should support upto 6 single wide GPU's	



7.	RAID Controller	12Gbps PCIe 3.0 with RAID 1, 5, 10, 50 with 8 GB Cache Memory on single / Multiple controllers or higher will be added advantage.	
8.	1G Networking features	2 x 1 Gbps Copper Ethernet with Additional Dedicated Mgmt. Ethernet interface port with 3 mts. Length factory crimped copper Ethernet patch cords for each port including 1 mgmt. port	
9.	10G Networking features	4 x 10G Copper Ethernet ports with 3 mts. Length 10G factory crimped copper Ethernet patch cords for each port	
10.	Redundant Power Supply	Dual, Hot-plug, Redundant Power Supply	
11.	Management integration	Support for integration with Microsoft System Center, VMware vCenter, BMC Software	
12.	Power & temperature	Real-time power meter, thresholds, alerts & capping with historical power counters. Temperature monitoring.	
13.	Pre-failure alert	Should provide predictive failure monitoring & proactive alerts of actual or impending component failure for fan, power supply, memory, CPU, RAID, NIC, HDD	
14.	Configuration Management &	- Real-time out-of-band hardware performance monitoring & alerting - Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management, external storage management, monitoring of FC, HBA & system health if added will be advantage. - Out-of-band hardware & firmware inventory - Zero-touch auto configuration to auto deploy a baseline server configuration profile	
15.	LED/LCD panel	Should display system ID, status information and system error code followed by descriptive text on LED Indicator / LCD Panel.	
16.	HTML5 support	HTML5 support for virtual console & virtual media without using Java or ActiveX plugins	



17.	Server security	Should have a cyber resilient architecture for a hardened server design for protection, detection & recovery from cyber attacks	
		Should protect against firmware which executes before the OS boots	
		Should provide effective protection, reliable detection & rapid recovery using: - Signed firmware updates - Support for Hardware root of trust / Silicon based hardware root of trust - Secure default passwords - Configuration and firmware drift detection - Secure alerting - Rapid OS recovery	
		Configuration upgrades should be only with cryptographically signed firmware and software	
		Should provide system lockdown feature to prevent change (or “drift”) in system firmware image(s) & prevent malicious modification of server firmware.	
		Should maintain repository for firmware and should be able to rollback, if required.	
18.	Certified for OS	Windows Server 2016 or latest, VMWare vSphere & vCenter, Red Hat Enterprise Linux, SUSE Linux Enterprise Server	
19.	Warranty	As mentioned in RFP.	

f. Face Recognition Servers with 3x GPU in each server for 370 FRS Channels

S No.	Parameter	Specifications	Compliance (Yes/No) with comments, if any
	Make & Model		
1.	Rack Height	2U rack mounted with sliding rails	
2.	Processors	Up to two Intel® Xeon® Scalable 2nd Gen processors, configured with 20 cores/processor @ 2.5 Ghz base freq. or equivalent or better	



3.	Memory	128 GB RAM 2666 MT/s support up to 512GB RAM, should have min. 24 DIMM slots	
4.	Hard Drives	5x 600GB 15K RPM SAS drives should be configured. Should support up to eight hard disk drives (SAS, SATA, SSD)	
5.	GPU Configured	Should be configured with 3 nos. of Nvidia Tesla T4 GPU or equivalent or better	
6.	GPU Support	Should support up to 6 single wide GPU's	
7.	RAID Controller	12Gbps PCIe 3.0 with RAID 1, 5, 10, 50 with 8 GB Cache Memory on single / Multiple controllers or higher will be added advantage.	
8.	1G Networking features	2 x 1 Gbps Copper Ethernet with Additional Dedicated Mgmt. Ethernet interface port with 3 mts. Length factory crimped copper Ethernet patch cords for each port including 1mgmt. port	
9.	10G Networking features	4 x 10G Copper Ethernet ports with 3 mts. Length 10G factory crimped copper Ethernet patch cords for each port	
10.	Redundant Power Supply	Dual, Hot-plug, Redundant Power Supply	
11.	Management integration	Support for integration with Microsoft System Center, VMware vCenter, BMC Software	
12.	Power & temperature	Real-time power meter, thresholds, alerts & capping with historical power counters. Temperature monitoring.	
13.	Pre-failure alert	Should provide predictive failure monitoring & proactive alerts of actual or impending component failure for fan, power supply, memory, CPU, RAID, NIC, HDD	
14.	Configuration Management &	- Real-time out-of-band hardware performance monitoring & alerting - Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management, external storage management, monitoring of FC, HBA & system health if added will be advantage. - Out-of-band hardware & firmware	



		inventory • Zero-touch auto configuration to auto deploy a baseline server configuration profile	
15.	LED/LCD panel	Should display system ID, status information and system error code followed by descriptive text on LED Indicator / LCD Panel.	
16.	HTML5 support	HTML5 support for virtual console & virtual media without using Java or ActiveX plugins	
17.	Server security	Should have a cyber resilient architecture for a hardened server design for protection, detection & recovery from cyber attacks	
		Should protect against firmware which executes before the OS boots	
		Should provide effective protection, reliable detection & rapid recovery using: - Signed firmware updates - Support for Hardware root of trust / Silicon based hardware root of trust - Secure default passwords - Configuration and firmware drift detection - Secure alerting - Rapid OS recovery	
		Configuration upgrades should be only with cryptographically signed firmware and software	
		Should provide system lockdown feature to prevent change (or “drift”) in system firmware image(s) & prevent malicious modification of server firmware.	
		Should maintain repository for firmware and should be able to rollback, if required.	
18.	Certified for OS	Windows Server 2016 or latest, VMWare vSphere & vCenter, Red Hat Enterprise Linux, SUSE Linux Enterprise Server	
19.	Warranty	As mentioned in RFP.	



g. AI Training and Continuous Learning Server

S No.	Parameter	Specifications	Compliance (Yes/No) with comments, if any
1.	Make & Model	(Specify)	
2.	Form Factor	3U/ 4U rack mounted with sliding rails	
3.	Processor	Support up to Four Intel® Xeon® Scalable 2nd Gen processors, configured with 20 cores/processor @ 2.5 Ghz base freq. or equivalent or better.	
4.	Memory slots	48x DDR4 slots - RDIMM, LRDIMM, NVDIMM (only on baseboard up to 12 PRTS)	
5.	Memory configured	512 GB scalable to 2TB	
6.	Disks supported	Upto 24 2.5" Drives and upto 12 NVMe SSD capable universal slots	
7.	RAID Controller	12Gbps PCIe 3.0 with RAID 1, 5, 6,10, 50 with 8 GB Cache Memory on single / Multiple controllers.	
8.	Disks configured	6x 600GB 15K RPM SAS drives should be configured. Or higher	
9.	Flexible Onboard NDC	1G/10G/25G	
10.	1G Networking features	2 x 1 Gbps Copper Ethernet with Additional Dedicated Mgmt. Ethernet interface port with 3 mts. Length factory crimped copper Ethernet patch cords for each port including 1 mgmt. port	
11.	10G Networking features	4 x 10G Copper Ethernet ports with 3 mts. Length 10G factory crimped copper Ethernet patch cords for each port	
12.	Certification and compliances	Microsoft Windows Server, Hyper-V, VMWare, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES)	
13.	Power Supply	Platinum rated redundant Power Supply or better	
14.	Management integration	Support for integration with Microsoft System Center, VMware vCenter, BMC Software	
15.	GPU Config	Should come pre-configured with 4X NVIDIA V100 or A100 (better	



		performance card can be provided by supplier)	
16.	Power & temperature	Real-time power meter, graphing, thresholds, alerts & capping with historical power counters. Temperature monitoring & graphing	
17.	Pre-failure alert	Should provide predictive failure monitoring & proactive alerts of actual or impending component failure for fan, power supply, memory, CPU, RAID, NIC, HDD.	
18.	Configuration Management &	Real-time out-of-band hardware performance monitoring & alerting Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management, external storage management, monitoring of FC, HBA & system health if added will be advantage. Out-of-band hardware & firmware inventory Zero-touch auto configuration to auto deploy a baseline server configuration profile	
19.	LED/LCD panel	Should display system ID, status information and system error code followed by descriptive text on LED Indicator / LCD Panel.	
20.	HTML5 support	HTML5 support for virtual console & virtual media without using Java or ActiveX plugins	
21.	Server security	Should have a cyber resilient architecture for a hardened server design for protection, detection & recovery from cyber attacks	
		Should protect against firmware which executes before the OS boots	
		Should provide effective protection, reliable detection & rapid recovery using: - Signed firmware updates - Support for Hardware root of trust / Silicon based hardware root of trust - Secure default passwords - Configuration and firmware drift	



		detection - Persistent event logging including user activity - Secure alerting - Rapid OS recovery	
		Configuration upgrades should be only with cryptographically signed firmware and software	
		Should provide system lockdown feature to prevent change (or “drift”) in system firmware image(s) & prevent malicious modification of server firmware	
22.	Intrusion alert	Intrusion alert in case chassis cover being opened	
23.	Certified for OS	Windows Server 2016, VMWare, Red Hat Enterprise Linux, SUSE Linux Enterprise Server	
24.	Warranty	As mentioned in RFP.	

h. ANPR Servers for 1622 Channels

S No.	Parameter	Specifications	Compliance (Yes/No) with comments, if any
1.	Make & Model		
2.	Form Factor	1U rack mounted with sliding rails	
3.	Processor	Up to two Intel® Xeon® Scalable 2nd Gen processors, up to 20 cores/processor @ 2.5 Ghz base freq. or equivalent or better	
4.	Memory slots	16 DDR4 DIMM slots, speed up to 2666MT/s or better	
5.	Memory configured	Minimum 128 GB, scalable to 512GB	
6.	Disks supported	Front drive bays: Up to 10 x 2.5” SAS/SATA (HDD/SSD) with up to 2 NVMe SSD or higher.	
7.	RAID Controller	12Gbps PCIe 3.0 with RAID 1, 5, 10, 50 with 8 GB Cache Memory on single / Multiple controllers.	
8.	Disks configured	3x 600GB 15K RPM SAS drives or higher.	
9.	1G Networking features	2 x 1 Gbps Copper Ethernet with Additional Dedicated Mgmt. Ethernet	



		interface port with 3 mts. Length factory crimped copper Ethernet patch cords for each port including 1 mgmt. port	
10.	10G Networking features	4 x 10G Copper Ethernet ports with 3 mts. Length 10G factory crimped copper Ethernet patch cords for each port	
11.	Certified for OS	Windows Server 2016 or higher, VMWare vSphere, vCenter, Red Hat Enterprise Linux, SUSE Linux Enterprise Server	
12.	Power Supply	Platinum rated redundant Power Supply	
13.	Management integration	Support for integration with Microsoft System Center, VMware vCenter, BMC Software	
14.	Power & temperature	Real-time power meter, thresholds, alerts & capping with historical power counters. Temperature monitoring	
15.	Pre-failure alert	Should provide predictive failure monitoring & proactive alerts of actual or impending component failure for fan, power supply, memory, CPU, RAID, NIC, HDD	
16.	Configuration & Management	• Real-time out-of-band hardware performance monitoring & alerting • Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management, external storage management, monitoring of FC, HBA & system health if added will be advantage. • Out-of-band hardware & firmware inventory • Zero-touch auto configuration to auto deploy a baseline server configuration profile	
17.	LED / LCD panel	Should display system ID, status information and system error code followed by descriptive text on LED Indicator / LCD Panel.	
18.	HTML5 support	HTML5 support for virtual console & virtual media without using Java or ActiveX plugins	
19.	Server security	Should have a cyber resilient architecture for a hardened server design for	



		protection, detection & recovery from cyber attacks	
		Should protect against firmware which executes before the OS boots	
		Should provide effective protection, reliable detection & rapid recovery using: - Support for Hardware root of trust / Silicon based hardware root of trust - Signed firmware updates - Secure default passwords - Configuration and firmware drift detection - Persistent event logging including user activity - Secure alerting - Rapid OS recovery	
		Configuration upgrades should be only with cryptographically signed firmware and software	
		Should provide system lockdown feature to prevent change (or “drift”) in system firmware image(s) & prevent malicious modification of server firmware	
20.	Warranty	As mentioned in RFP.	

i. Video Summarization and Forensics Server

S No.	Parameter	Specifications	Compliance (Yes/No) with comments, if any
1.	Make & Model		
2.	Rack Height	2U rack mounted with sliding rails	
3.	Processors	Up to two Intel® Xeon® Scalable 2nd Gen processors, configured with 20 cores/processor @ 2.5 Ghz base freq. or equivalent or better.	
4.	Memory	128 GB RAM 2666 MT/s support up to 512GB RAM, should have min. 24 DIMM slots	
5.	Hard Drives	5x 600GB 15K RPM SAS drives should be configured. Should support up to eight hard disk drives (SAS, SATA, SSD)	



6.	GPU Configured	Should be configured with 3 nos. of Nvidia Tesla T4 GPU (better performance card can be provided by supplier)	
7.	GPU Support	Should support upto 6 single wide GPU's	
8.	RAID Controller	12Gbps PCIe 3.0 with RAID 1, 5, 10, 50 with 8GB Cache Memory on single / Multiple controllers.	
9.	1G Networking features	2 x 1 Gbps Copper Ethernet with Additional Dedicated Mgmt. Ethernet interface port with 3 mts. Length factory crimped copper Ethernet patch cords for each port including 1 mgmt. port	
10.	10G Networking features	4 x 10G Copper Ethernet ports with 3 mts. Length 10G factory crimped copper Ethernet patch cords for each port	
11.	Redundant Power Supply	Dual, Hot-plug, Redundant Power Supply	
12.	Management integration	Support for integration with Microsoft System Center, VMware vCenter, BMC Software	
13.	Power & temperature	Real-time power meter, thresholds, alerts & capping with historical power counters. Temperature monitoring.	
14.	Pre-failure alert	Should provide predictive failure monitoring & proactive alerts of actual or impending component failure for fan, power supply, memory, CPU, RAID, NIC, HDD	
15.	Configuration Management &	- Real-time out-of-band hardware performance monitoring & alerting - Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management, external storage management, monitoring of FC, HBA & system health if added will be advantage. - Out-of-band hardware & firmware inventory - Zero-touch auto configuration to auto deploy a baseline server configuration profile	
16.	LED/LCD panel	Should display system ID, status information and system error code	



		followed by descriptive text on LED Indicator / LCD Panel.	
17.	HTML5 support	HTML5 support for virtual console & virtual media without using Java or ActiveX plugins	
18.	Server security	Should have a cyber resilient architecture for a hardened server design for protection, detection & recovery from cyber attacks	
		Should protect against firmware which executes before the OS boots	
		Should provide effective protection, reliable detection & rapid recovery using: - Support for Hardware root of trust / Silicon based hardware root of trust - Signed firmware updates - Secure default passwords - Configuration and firmware drift detection - Persistent event logging including user activity - Secure alerting - Rapid OS recovery	
		Configuration upgrades should be only with cryptographically signed firmware and software	
		Should provide system lockdown feature to prevent change (or “drift”) in system firmware image(s) & prevent malicious modification of server firmware.	
		Should maintain repository for firmware and should be able to rollback, if required.	
19.	Certified for OS	Windows Server 2016 or latest, VMWare vSphere & vCenter, Red Hat Enterprise Linux, SUSE Linux Enterprise Server	
20.	Warranty	As mentioned in RFP. .	



j. PIU (Picture Intelligence Unit) Server

S No.	Parameter	Specifications	Compliance (Yes/No) with comments, if any
1.	Make & Model	-----	
2.	Rack Height	2U rack mounted with sliding rails	
3.	Processors	Up to two Intel® Xeon® Scalable 2nd Gen processors, configured with 20 cores/processor @ 2.5 Ghz base freq. or equivalent or better.	
4.	Memory	128 GB RAM 2666 MT/s support up to 512GB RAM, should have min. 24 DIMM slots	
5.	Hard Drives	5x 600GB 15K RPM SAS drives should be configured. Should support up to eight hard disk drives (SAS, SATA, SSD)	
6.	GPU Configured	Should be configured with 3 nos. of Nvidia Tesla T4 GPU (better performance card can be provided by supplier)	
7.	GPU Support	Should support upto 6 single wide GPU's	
8.	RAID Controller	12Gbps PCIe 3.0 with RAID 1, 5, 10, 50 with 8GB Cache Memory on single / Multiple controllers.	
9.	1G Networking features	2 x 1 Gbps Copper Ethernet with Additional Dedicated Mgmt. Ethernet interface port with 3 mts. Length factory crimped copper Ethernet patch cords for each port including 1 mgmt. port	
10.	10G Networking features	4 x 10G Copper Ethernet ports with 3 mts. Length 10G factory crimped copper Ethernet patch cords for each port	
11.	Redundant Power Supply	Dual, Hot-plug, Redundant Power Supply	
12.	Management integration	Support for integration with Microsoft System Center, VMware vCenter, BMC Software	
13.	Power & temperature	Real-time power meter, thresholds, alerts & capping with historical power counters. Temperature monitoring.	
14.	Pre-failure alert	Should provide predictive failure monitoring & proactive alerts of actual or	



		impending component failure for fan, power supply, memory, CPU, RAID, NIC, HDD	
15.	Configuration & Management	• Real-time out-of-band hardware performance monitoring & alerting • Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management, external storage management, monitoring of FC, HBA & system health if added will be advantage. • Out-of-band hardware & firmware inventory • Zero-touch auto configuration to auto deploy a baseline server configuration profile	
16.	LED/LCD panel	Should display system ID, status information and system error code followed by descriptive text on LED Indicator / LCD Panel.	
17.	HTML5 support	HTML5 support for virtual console & virtual media without using Java or ActiveX plugins	
18.	Server security	Should have a cyber resilient architecture for a hardened server design for protection, detection & recovery from cyber attacks	
		Should protect against firmware which executes before the OS boots	
		Should provide effective protection, reliable detection & rapid recovery using: - Support for Hardware root of trust / Silicon based hardware root of trust - Signed firmware updates - Secure default passwords - Configuration and firmware drift detection - Persistent event logging including user activity - Secure alerting - Rapid OS recovery	
		Configuration upgrades should be only with cryptographically signed firmware and software	



		Should provide system lockdown feature to prevent change (or “drift”) in system firmware image(s) & prevent malicious modification of server firmware.	
		Should maintain repository for firmware and should be able to rollback, if required.	
19.	Certified for OS	Windows Server 2016 or latest, VMWare vSphere & vCenter, Red Hat Enterprise Linux, SUSE Linux Enterprise Server	
20.	Warranty	As mentioned in RFP.	

k. Domain Controller, EMS Server

S No.	Parameter	Specifications	Compliance (Yes/No) with comments, if any
	Make & Model	-----	
	Form Factor	1U rack mounted with sliding rails	
	Processor	Up to two Intel® Xeon® Scalable 2nd Gen processors, up to 20 cores/processor @ 2.5 Ghz base freq. or equivalent or better	
	Memory slots	16 DDR4 DIMM slots, speed up to 2666MT/s or better	
	Memory configured	Minimum 256 GB, scalable to 512GB	
	Disks supported	Front drive bays: Up to 10 x 2.5” SAS/SATA (HDD/SSD) with up to 2 NVMe SSD or higher.	
	RAID Controller	12Gbps PCIe 3.0 with RAID 1, 5, 10, 50 with 8 GB Cache Memory on single / Multiple controllers.	
	Disks configured	3x 600GB 15K RPM SAS drives or higher.	
	1G Networking features	2 x 1 Gbps Copper Ethernet with Additional Dedicated Mgmt. Ethernet interface port with 3 mts. Length factory crimped copper Ethernet patch cords for each port including 1 mgmt. port	
	10G Networking features	4 x 10G Copper Ethernet ports with 3 mts. Length 10G factory crimped copper Ethernet patch cords for each port	
	FC HBA	Dual port 16 Gbps FC HBA with two no. of each 3 mts. Or 5 mts FC patch cables, Quoted HBA should support quoted SAN Switch and Storage	



	Certified for OS	Windows Server 2016 or higher, VMWare vSphere, vCenter, Red Hat Enterprise Linux, SUSE Linux Enterprise Server	
	Power Supply	Platinum rated redundant Power Supply	
	Management integration	Support for integration with Microsoft System Center, VMware vCenter, BMC Software	
	Power & temperature	Real-time power meter, thresholds, alerts & capping with historical power counters. Temperature monitoring	
	Pre-failure alert	Should provide predictive failure monitoring & proactive alerts of actual or impending component failure for fan, power supply, memory, CPU, RAID, NIC, HDD	
	Configuration Management &	- Real-time out-of-band hardware performance monitoring & alerting - Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management, external storage management, monitoring of FC, HBA & system health if added will be advantage. - Out-of-band hardware & firmware inventory - Zero-touch auto configuration to auto deploy a baseline server configuration profile	
	LED / LCD panel	Should display system ID, status information and system error code followed by descriptive text on LED Indicator / LCD Panel.	
	HTML5 support	HTML5 support for virtual console & virtual media without using Java or ActiveX plugins	
1.	Server security	Should have a cyber resilient architecture for a hardened server design for protection, detection & recovery from cyber attacks	
		Should protect against firmware which executes before the OS boots	



		Should provide effective protection, reliable detection & rapid recovery using: - Signed firmware updates - Support for Hardware root of trust / Silicon based hardware root of trust - Secure default passwords - Configuration and firmware drift detection - Secure alerting - Rapid OS recovery	
		Configuration upgrades should be only with cryptographically signed firmware and software	
		Should provide system lockdown feature to prevent change (or “drift”) in system firmware image(s) & prevent malicious modification of server firmware	
	Warranty	As mentioned in RFP.	

I. Antivirus Server and LDAP server

S No.	Parameter	Specifications	Compliance (Yes/No) with comments, if any
	Make & Model	-----	
	Form Factor	1U rack mounted with sliding rails	
	Processor	Up to two Intel® Xeon® Scalable 2nd Gen processors, up to 20 cores/processor @ 2.5 Ghz base freq. or equivalent or better	
	Memory slots	16 DDR4 DIMM slots, speed up to 2666MT/s or better	
	Memory configured	Minimum 256 GB, scalable to 512GB	
	Disks supported	Front drive bays: Up to 10 x 2.5” SAS/SATA (HDD/SSD) with up to 2 NVMe SSD or higher.	
	RAID Controller	12Gbps PCIe 3.0 with RAID 1, 5, 10, 50 with 8 GB Cache Memory on single / Multiple controllers.	
	Disks configured	3x 600GB 15K RPM SAS drives or higher.	
	1G Networking features	2 x 1 Gbps Copper Ethernet with Additional Dedicated Mgmt. Ethernet interface port with 3 mts. Length factory crimped copper Ethernet patch cords for each port including 1 mgmt. port	



	10G Networking features	4 x 10G Copper Ethernet ports with 3 mts. Length 10G factory crimped copper Ethernet patch cords for each port	
	FC HBA	Dual port 16 Gbps FC HBA with two no. of each 3 mts. Or 5 mts FC patch cables, Quoted HBA should support quoted SAN Switch and Storage	
	Certified for OS	Windows Server 2016 or higher, VMWare vSphere, vCenter, Red Hat Enterprise Linux, SUSE Linux Enterprise Server	
	Power Supply	Platinum rated redundant Power Supply	
	Management integration	Support for integration with Microsoft System Center, VMware vCenter, BMC Software	
	Power & temperature	Real-time power meter, thresholds, alerts & capping with historical power counters. Temperature monitoring	
	Pre-failure alert	Should provide predictive failure monitoring & proactive alerts of actual or impending component failure for fan, power supply, memory, CPU, RAID, NIC, HDD	
	Configuration Management &	• Real-time out-of-band hardware performance monitoring & alerting • Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management, external storage management, monitoring of FC, HBA & system health if added will be advantage. • Out-of-band hardware & firmware inventory • Zero-touch auto configuration to auto deploy a baseline server configuration profile	
	LED / LCD panel	Should display system ID, status information and system error code followed by descriptive text on LED Indicator / LCD Panel.	
	HTML5 support	HTML5 support for virtual console & virtual media without using Java or ActiveX plugins	



	Server security	Should provide effective protection, reliable detection & rapid recovery using: - Signed firmware updates - Support for Hardware root of trust / Silicon based hardware root of trust - Secure default passwords - Configuration and firmware drift detection - Secure alerting - Rapid OS recovery	
		Configuration upgrades should be only with cryptographically signed firmware and software	
		Should provide system lockdown feature to prevent change (or “drift”) in system firmware image(s) & prevent malicious modification of server firmware	
	Warranty	As mentioned in RFP.	

m. Viewing Management Server

S No.	Parameter	Specifications	Compliance (Yes/No) with comments, if any
	Make & Model		
	Form Factor	1U rack mounted with sliding rails	
	Processor	Up to two Intel® Xeon® Scalable 2nd Gen processors, up to 20 cores/processor @ 2.5 Ghz base freq. or equivalent or better	
1.	Memory slots	16 DDR4 DIMM slots, speed up to 2666MT/s or better	
	Memory configured	Minimum 128 GB, scalable to 512GB	
	Disks supported	Front drive bays: Up to 10 x 2.5” SAS/SATA (HDD/SSD) with up to 2 NVMe SSD or higher.	
	RAID Controller	12Gbps PCIe 3.0 with RAID 1, 5, 10, 50 with 8 GB Cache Memory on single / Multiple controllers.	
	Disks configured	3x 600GB 15K RPM SAS drives or higher.	
	1G Networking features	2 x 1 Gbps Copper Ethernet with Additional Dedicated Mgmt. Ethernet interface port with 3 mts. Length factory crimped copper Ethernet patch cords for each port including 1 mgmt. port	



	10G Networking features	4 x 10G Copper Ethernet ports with 3 mts. Length 10G factory crimped copper Ethernet patch cords for each port	
	FC HBA	Dual port 16 Gbps FC HBA with two no. of each 3 mts. Or 5 mts FC patch cables, Quoted HBA should support quoted SAN Switch and Storage	
	Certified for OS	Windows Server 2016 or higher, VMWare vSphere, vCenter, Red Hat Enterprise Linux, SUSE Linux Enterprise Server	
	Power Supply	Platinum rated redundant Power Supply	
	Management integration	Support for integration with Microsoft System Center, VMware vCenter, BMC Software	
	Power & temperature	Real-time power meter, thresholds, alerts & capping with historical power counters. Temperature monitoring	
	Pre-failure alert	Should provide predictive failure monitoring & proactive alerts of actual or impending component failure for fan, power supply, memory, CPU, RAID, NIC, HDD	
	Configuration & Management	• Real-time out-of-band hardware performance monitoring & alerting • Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management, external storage management, monitoring of FC, HBA & system health if added will be advantage. • Out-of-band hardware & firmware inventory • Zero-touch auto configuration to auto deploy a baseline server configuration profile	
	LED/LCD panel	Should display system ID, status information and system error code followed by descriptive text on LED Indicator / LCD Panel.	
	HTML5 support	HTML5 support for virtual console & virtual media without using Java or ActiveX plugins	



	Server security	Should have a cyber resilient architecture for a hardened server design for protection, detection & recovery from cyber attacks	
		Should protect against firmware which executes before the OS boots	
		Should provide effective protection, reliable detection & rapid recovery using: - Support for Hardware root of trust / Silicon based hardware root of trust - Signed firmware updates - Secure default passwords - Configuration and firmware drift detection - Persistent event logging including user activity - Secure alerting - Rapid OS recovery	
		Configuration upgrades should be only with cryptographically signed firmware and software	
		Should provide system lockdown feature to prevent change (or “drift”) in system firmware image(s) & prevent malicious modification of server firmware	
	Warranty	As mentioned in RFP.	

n. DLP (Data Leak Protection), PKI + MFA (Multi Factor Authentication) server

S No.	Parameter	Specifications	Compliance (Yes/No) with comments, if any
	Make & Model		
	Form Factor	1U rack mounted with sliding rails	
	Processor	Up to two Intel® Xeon® Scalable 2nd Gen processors, up to 20 cores/processor @ 2.5 Ghz base freq. or equivalent or better	
	Memory slots	16 DDR4 DIMM slots, speed up to 2666MT/s or better	
	Memory configured	Minimum 256 GB, scalable to 512GB	
	Disks supported	Front drive bays: Up to 10 x 2.5” SAS/SATA (HDD/SSD) with up to 2 NVMe SSD or higher.	



	RAID Controller	12Gbps PCIe 3.0 with RAID 1, 5, 10, 50 with 8 GB Cache Memory on single / Multiple controllers.	
	Disks configured	3x 600GB 15K RPM SAS drives or higher.	
	1G Networking features	2 x 1 Gbps Copper Ethernet with Additional Dedicated Mgmt. Ethernet interface port with 3 mts. Length factory crimped copper Ethernet patch cords for each port including 1 mgmt. port	
	10G Networking features	4 x 10G Copper Ethernet ports with 3 mts. Length 10G factory crimped copper Ethernet patch cords for each port	
	FC HBA	Dual port 16 Gbps FC HBA with two no. of each 3 mts. Or 5 mts FC patch cables, Quoted HBA should support quoted SAN Switch and Storage	
	Certified for OS	Windows Server 2016 or higher, VMWare vSphere, vCenter, Red Hat Enterprise Linux, SUSE Linux Enterprise Server	
	Power Supply	Platinum rated redundant Power Supply	
	Management integration	Support for integration with Microsoft System Center, VMware vCenter, BMC Software	
	Power & temperature	Real-time power meter, thresholds, alerts & capping with historical power counters. Temperature monitoring	
	Pre-failure alert	Should provide predictive failure monitoring & proactive alerts of actual or impending component failure for fan, power supply, memory, CPU, RAID, NIC, HDD	
	Configuration & Management	• Real-time out-of-band hardware performance monitoring & alerting • Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management, external storage management, monitoring of FC, HBA & system health if added will be advantage. • Out-of-band hardware & firmware inventory • Zero-touch auto configuration to auto deploy a baseline server configuration profile	



	LED / LCD panel	Should display system ID, status information and system error code followed by descriptive text on LED Indicator / LCD Panel.	
	HTML5 support	HTML5 support for virtual console & virtual media without using Java or ActiveX plugins	
	Server security	Should provide effective protection, reliable detection & rapid recovery using: - Signed firmware updates - Support for Hardware root of trust / Silicon based hardware root of trust. - Secure default passwords - Configuration and firmware drift detection - Secure alerting - Rapid OS recovery	
		Configuration upgrades should be only with cryptographically signed firmware and software	
		Should provide system lockdown feature to prevent change (or “drift”) in system firmware image(s) & prevent malicious modification of server firmware	
	Warranty	As mentioned in RFP.	

4.8.16. Storage and backup solution

a. Scale out NAS Storage with rack for surveillance video data for 30 days – 20 PB

S No.	Feature	Specification	Compliance (Yes/ No) with comments, if any
1	Controllers and Architecture	Storage Should be distributed clustered Architecture clustered Architecture written for Scale-Out NAS Storage operations. Proposed Storage solution should be based on Appliance and not general-purpose servers or software-define storage.	
		Scale out storage should be configured with minimum 12 controllers of the same type	
		Offered storage must be certified/referenced with at least 3 VMS vendors including the offered VMS in this project, public documentation related best practices of offered storage with these 3 VMS vendors to be submitted.	



		The storage cluster should support linear scalability of performance and capacity i.e. for every drive bay added, performance should increase by the same amount till 2x capacity of the quoted storage	
		All storage nodes/controllers must be active for all Storage shares, contributing in performance and capacity of the system	
		Storage Controllers should have processors as per OEM design and application benchmarking.	
2	Onboard Memory	The scale out storage must be configured with minimum 1.5 TB (total) federated/globally coherent or better, DRAM based cache/memory example. Distributed and write should be protected with BB (Beaver Builder) Cache/ D-staging to a flash drive	
3	Operating System	Scale-Out Storage operating system should have distributed specialized Operating System by OEM(s), dedicated for serving data efficiently and customized for True Scale-Out Storage. Entire data should automatically balance across proposed controllers/nodes within each tier without any administrative intervention, or requirement of third-party software	
4	Network Ports	The scale out storage cluster should be offered with minimum 10/25 Gbps, 40G/100G SFP+ ports (Total aggregate front end throughput of 960 Gbps or better), and cluster should be scalable to 4x the number of offered ports. Interconnect switches for internode communication should be proposed in redundancy.	
5	Disk support	Storage cluster should have capability to support different kinds of disks tiers likes SSD, SAS, SATA/NL-SAS drives within single filesystem.	
6	Redundancy with No Single Point of Failure (SPOF)	- The Scale-Out Storage should have self-optimizing architecture so the system does not require manual defragmentation or consistency check like 'fsck' in the event of an ungraceful shutdown of the cluster to ensure higher uptime. - All video data should be striped across all storage controllers in the proposed storage system, so that performance of all controllers can be utilized for all read and write operations. - Redundant and Hot replaceable modules:	



		Controllers, Hard Disk Drive and power supplies (230V AC, 50 Hz.) - The Complete multi-controller Storage System Solution should be fully redundant, configured in High Availability mode and should NOT have any Single Point of Failure (SPOF).	
7	Total Storage Capacity	- Scale out storage should be configured with 20 PiB usable capacity in a single filesystem, using equal to or less than 12TB or more NL-SAS/SATA/SSD HDD. Additional 10% usable space should be reserved, or equivalent number of disks should be provided, as hot spares. - Offered scale out storage should be capable of providing a throughput of greater than 25GBps at 100% write on SMB2 and higher versions, for handling the camera feed and other workloads. OEM Sizer tool output needs to be provided on OEM letterhead for the same showing capacity and performance. - The storage should be scalable upto 2x the capacity, and performance, with same drive size, in a single filesystem/name space.	
8	Capacity/performance Expansion	- There should not be any downtime or migration activity required in the event it is needed to add additional capacity or additional performance to the storage system. - In the event of addition of storage controller/storage node to storage solution, existing data should be rebalanced across all nodes of storage controllers/storage nodes automatically. This should be done with low priority avoiding any impact to client performance. - Addition of storage controller/ storage nodes should not require any complicated configuration of new controller/node. It should be done easily, seamlessly and without having any impact to user access. - The storage file system shall not require metadata performance tuning. - The system must be able to support policy-based tiering to different storage tiers within Storage sub-system.	



9	Protection Levels	- 20PiB usable capacity should be configured with protection level which can protect data against simultaneous 3 disks failures, without data unavailability and data loss - Should have capability to change the protection level on-the-fly without impacting the workflow of VMS - Should be able to assign protection level on cluster, directory or file level.	
10	Protocol Support	- Network protocol Support: • Must provide access for a variety of operating systems (UNIX, Linux, Windows) using native OS protocols. All protocols required for solution, must be included without additional licenses and hardware. - Should support user security mechanisms like AD, LDAP and NIS.	
11	File Locking & Filtering	File Locking for Data protection from corruption while sharing files between UNIX and Windows users. (Should support simultaneous multiple client's access to the storage without any data corruption)	
12	Client Load Balancing	Storage System should have capability to load balance client connectivity across these multiple controllers so that all clients get distributed across all existing controllers/nodes to avoid any performance hotspot.	
13	Heterogenous support for end user systems	Operating system support RedHat Linux/Suse Linux/ Windows Servers 2003/2008 or later, Windows 7 or later. Unix Based operating systems like SUN Solaris/ HP Unix/ IBM AIX	
14	Management Interface software	Support the management, administration and configuration of the whole storage platform through a single management interface along with CLI	
15	Security	- The system must support encrypting data at rest. - The system must be able to support WORM functionality. -Should be able to assign protection level on cluster, directory or file level - The system must support multiple multitenant access zones for different Active Directories and	



		LDAP. Each Access zone must simultaneously support local, Active Directory and LDAP users. - The system must support Role Base Access Control with Integration with Active Directory and LDAP - The system must be able to support System Auditing for system as well as supported protocols. - The system must support multiple DNS. - The system should have file system integrity and data integrity checks built in to prevent data loss due to bit rate and other soft errors	
16	Warranty	As mentioned in RFP, Detailed BoQ with part codes for hardware and OEM support services should be submitted along with bid. Appliance software/Hardware L1 to L3 support from same OEM. Resolution time: NBD for continuation of the I/O to and fro from the storage and all storage related issues.	
17	Investment Protection	Storage System quoted by the OEM to be in the Leaders Quadrant in the latest Gartner Magic Quadrant for Distributed File and Object Storage Arrays Report and Storage System OEM should be in the Top5 Global latest revenue report from IDC	

b. SAN / Unified Enterprise storage for 180 days – 2 PB (Storage for DB, boot, Flagged Data & Backup for 180 days)

Functional Requirement:

This Storage will be used for storing DMZ virtual machines and VMS VM's which will be running on virtual environment. The NVMe or SCM technology must be supported for future and mentioned in the web-site for any of the product descriptions of OEM.

S No.	Item	Description of Requirement	Compliance (Yes/ No) with comments, if any
1.	Market Recognition / Credibility	Storage quoted by the OEM to be in leaders or challengers' quadrant in the latest Gartner report of general-purpose storage system	



2.	SAN Storage Architecture	Hybrid storage system with Storage Operating System optimized for end to end to handle different types of drives like SSD, SAS / NL-SAS technology with built in QoS (Quality of Services) for optimal utilization of resources across the array. The storage should also support automated data tiering between these 3 quoted types of drives.	
3.		Dual active-active controllers each populated with dual socket of intel Xeon Processor	
4.	Scalability	Offered storage should support scale up for future capacity and performance enhancements	
5.	Data Efficiency Features	Deduplication and Compression functionalities should be supplied and supported on SSD capacity with all required licenses. Admin should be able to enable/disable reduction for individual volumes/application	
6.	Controller Scalability	Support for scalability to additional controller pairs (up to 6 pairs or better) to enhance capacity and performance when needed.	
7.	Encryption	Option should be available to support FIPS 140-2 certified self-encrypting drives (SEDs). Or encryption at controller level with license will be fine	
8.	Drive Scalability	Minimum 500 disk drives should be supported within the proposed Controller Pair and Offered storage shall be scalable to 1000 Drives within the same storage	
9.		The system should allow dynamic expansion of volumes / pools without any application downtime.	
10.		The system should be powerful enough to support capacity scalability up to 4PB RAW capacity by adding disks without degrading the performance	
11.	Cache	Minimum protected 256GB DRAM cache across dual controller, Scalable to 2TB or more either by adding memory into existing controllers or by Adding controllers in cluster/federation of arrays.	



12.	Ports	Minimum 16 x 32 Gbps/ 32 x16 Gbps Frontend FC Ports across the proposed controllers and should be scalable up to 24 Nos of FC Ports or higher. Should also be configured with 8 x 10Gbps SFP+ iSCSI Ports. The back-end of the array must be 8 x 12/4 x 25 Gbps or higher SAS ports per array. It should also support configuring native 10Gbps ports for storage-based replication.	
13.	Capacity	The storage must be supplied with 2000TB Usable Capacity in below configuration:	
14.		400TB Usable Capacity using SSD Drives on RAID5 / RAID6	
15.		1600TB Usable Capacity using minimum 7.2k rpm NL-SAS Drives on RAID6	
16.		1 Hot spare for every 30 Drives should be configured.	
17.	Performance	The array should be configured to deliver minimum of 100,000 IOPS with 32 KB block size & 50:50 read: write ratio. The storage system should be scalable to more than 1,00,000 IOPS by adding more controllers.	
18.	Data Protection Features	The array should natively be thin provisioned with built-in space efficient snapshots, clones for optimal utilization and performance of the array	
19.	RAID Support	The storage should support industry standard RAID levels like RAID 0, 1, 5, 6, RAID 10 or better; The storage should support combination of multiple RAID Levels in a single array.	
20.	Remote Replication Features	The System must be supported and supplied with Replication license for synchronous and Asynchronous replication using FC or iSCSI/IP. The Solution must offer storage-based replication for 1:1, 1: many and many:1 from day 1. The storage should additionally support feature of creating active-active storage environment across 2 physically separate sites/datacenters.	
21.	Data Security	The LUN security & masking software to be provided and configured to protect LUNs configured to heterogeneous hosts running different OS	



22.	Management	The Array must be supplied with comprehensive GUI based Management software which is HTML5 based along with storage analytics utilities for current and historic data analysis. The Management software should work with Multiple arrays, Multiple sites.	
23.		The storage should have features like remote diagnostics and performance monitoring, automated alerts, reports and notifications.	
24.		The Management software should be with single console-based performance management software to manage & monitor replication, live & historical usage of the array including FE ports, BE ports, controller, disk drives etc.	
25.	OS & other Software Support	The Storage Management Software shall be certified to work with VMware vSphere Metro Storage Cluster, VMware SRM	
26.		The must be certified to support current versions of OS like Microsoft Windows Server, Red Hat Linux, VMware, Native files, Block Protocols, etc.	
27.	Purpose and compatibility	This dedicated storage section will serve the purpose of DMZ which will ensure better back plane throughput and compatibility of controllers and storage (20 PB) mentioned in the specifications.	
28.	Warranty	As mentioned in RFP.	

c. SAN Switches

S No.	Feature	Technical Specifications	Compliance (Yes/ No) with comments, if any
1.	Switch Architecture	The proposed SAN Switches should have 2U form factor with minimum 48 Nos. of 32Gbps Ports or higher. Should have redundant power supplies and fans.	
2.	Fiber Channel Ports	Should be configured with 48 x 32Gbps FC Ports or higher on day one	
3.	Autosensing capabilities	The proposed ports should have autosensing capabilities to 32/16/8 Gbps FC connectivity	



4.	Trucking capabilities	The switch should support trucking with up to eight 32 Gbps ports per ISL trunk	
5.	Performance	Should support aggregate bandwidth of 4Tbps or higher	
6.	Port Types supported	Should support D_PORT (Clear Link Diagnostic Port), E_PORT, EX_PORT, F_PORT, AE_PORT	
7.	Media/Transceiver Types	Should support hot-pluggable Fibre Channel SFP+ at 32 Gbps SWL/LWL and SFP+ at 16 Gbps SWL/LWL/ELWL	
8.	USB Port	Should have at least One USB port per control processor for firmware download, support save, and configuration upload or download	
9.	Management	Should have switch management feature with support for e HTTP, SNMP v1/v3 (FE MIB, FC Management MIB), SSH; Auditing, Syslog; Command Line Interface (CLI); SMI-S compliant	
10.	Security	Should support DH-CHAP (between switches and end devices), FCAP switch authentication; HTTPS, IPsec, IP filtering, LDAP with Ipv6, OpenLDAP, Port Binding, RADIUS, TACACS+, user-defined Role-Based Access Control (RBAC), Secure Copy (SCP), Secure RPC, Secure Syslog, SFTP, SSH v2, SSL, Switch Binding, Trusted Switch. Should also support up to 12 in-flight encryption and compression ports.	
11.	Cables	Fc cables can be provided along with SAN switches with different lengths to cater server connectivity. Or if provided along with the server	
12.	Warranty	As mentioned in RFP.	

d. Backup Appliance and Backup software solutions

S No.	Description	Compliance (Yes/ No) with comments, if any
1.	Proposed disk-based backup appliance should be able to interface with various industry leading server platforms, operating systems	



	and Must support LAN/SAN based D2D backup and VTL backup simultaneously via NFS v3, CIFS, FC, OST and NDMP protocols.	
2.	Proposed appliance should support global and inline data duplication using automated variable block length deduplication technology.	
3.	Proposed appliance should be offered with protocols like VTL, OST, CIFS and NFS. All of the protocols should be available to use concurrently with global deduplication for data ingested across all of them.	
4.	Proposed appliance should support industry leading backup software like EMC Networker, Symantec NetBackup, Commvault and HP Data Protector etc. and should Support deduplication at backup server/ host / application level so that only changed blocks travel through network to backup device.	
5.	Proposed appliance should be sized appropriately for backup of front end data 150 TB (50% DB and 50% File System) data as per below backup policies: • Daily Incremental Backup – retained for 4 weeks in disk based backup appliance. • Weekly Full Backup for all data types – retained for 3 months in disk based backup appliance. • Monthly Full Backups – Retained for 12 Months in the same disk-based backup appliance. • Yearly Full Backups – Retained for 7 years in the same disk-based backup appliance. The Purpose-built backup appliance should be quoted with adequate capacity with 15% YoY data growth and 3% daily change rate for entire duration of 5 years warranty. • Any additional software or backup storage capacity (in addition to minimum 150 TB usable capacity) or any other component required as per sizing needs to be provided by the OEM & bidder during the entire warranty period of 5 years.	
6.	Proposed Appliance should have the capability to tier backup data in deduplicated format to an external cloud storage (on premise / public cloud).	
7.	Proposed appliance should have the ability to perform different backup, restore, replication jobs simultaneously and Must supports communications and data transfers through 8GB SAN, 10 Gb & 1 Gb ethernet LAN over copper and SFP+. The proposed backup appliance should be offered with min. 2 x 1Gbps NIC, 4 x 10Gbps NIC and 4 x 16Gbps FC ports and should support redundant controller for high availability of appliance in future.	



8.	Proposed appliance should support minimum backup throughput of 30 TB/hr while maintaining a single deduplication pool with RAID 6 and min. one hot spare disk as well.	
9.	Proposed appliance should support different retentions for primary and DR backup storage and should support instant copy creation on remote site for better DR readiness with support for transmitting only deduplicated unique data in encrypted format to remote sites.	
10.	Proposed appliance should support retention lock (WORM) feature which ensures that no data is deleted accidentally and support for point-in-time copies of a LUN or volumes with minimal performance impact.	
11.	Proposed disk appliance should be offered with battery backed up RAM / NVRAM for protection against data loss in power failure scenario and continuous automated file system check to ensure data integrity.	
12.	Proposed appliance should Support Enterprise Applications and Database Backups without integration with Backup Software, for better visibility of Backups to Application and database Owners, thus ensuring faster and direct recovery on application/database level. This integration should be available for Oracle, SAP, SAP HANA, DB2, MS SQL, Hadoop, MongoDB, Cassandra etc.	
13.	Proposed appliance should support bi-directional, many-to-one, one-to-many, and one-to-one replication.	
14.	Proposed appliance should support 256-bit AES encryption for data at rest and data-in-flight during replication. It should offer internal and external key management for encryption.	
15.	Proposed appliance should be offered RAID-6 with SAS/SATA/NL-SAS disk drives along with hot-spare disks in the ratio of 15:1 or better.	
16.	Proposed appliance should be offered with Multi-Tenancy features which provides a separate logical space for each tenant user while maintaining a global deduplication across data from all tenant users.	
17.	Warranty: As mentioned in RFP.	
18.	Proposed backup software should be available on various OS platforms like Windows, Linux, HP-UX, IBM AIX, Solaris etc. The backup server should be compatible to run on both Windows and Linux OS platforms	
19.	The backup software should be able to encrypt the backed-up data using 256-bit AES encryption on the backup client and should not demand for additional license, any such license if needed should be quoted for the total number of backup clients asked for.	

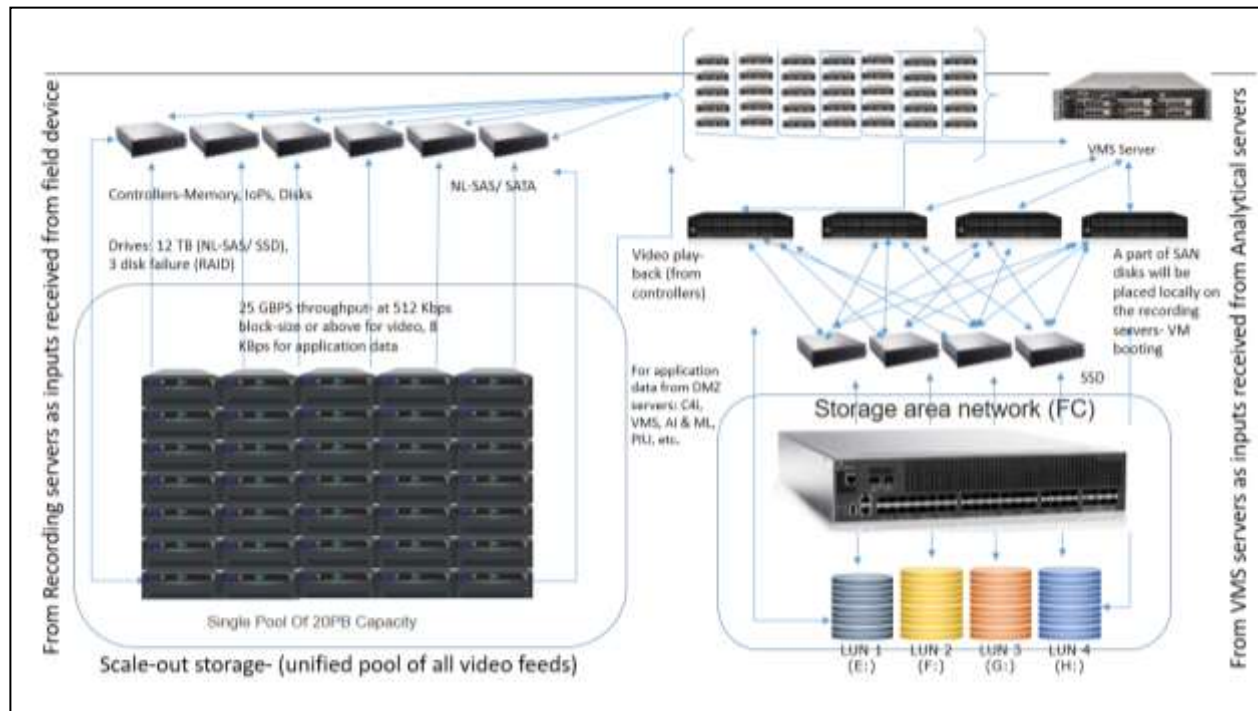


20.	The backup solution should also support online LAN Free SAN based backups of databases through appropriate agents; Important Applications being Oracle, Microsoft SQL Server, Exchange, SharePoint, IBM DB2 UDB, Informix, Lotus Notes/Domino, MySQL, SAP, SAP HANA & Sybase etc.	
21.	Should able to dynamically break up large save sets into smaller save sets to be backed up in parallel to allow backups to complete faster for Windows, Unix and Linux clients.	
22.	Should have in-built calendar-based scheduling system and also support check-point restart able backups for file systems. It should support various level of backups including full, incremental, differential, synthetic and virtual synthetic backups	
23.	The proposed backup software should have the capability to enable WORM on the backup sets from the backup software console on proposed disk backup appliance	
24.	The solution must support client-direct backup feature for file system, applications and databases to reduce extra hop for backup data at backup/media server to cater stringent backup window.	
25.	Bidder should provide 150TB capacity-based licenses. SI need to provide backup solution on the offered IT Infra stack from single OEM for backup software & purpose-built backup appliance.	
26.	Must have Agent/Modules for online backup of applications and databases such as MS SQL, Oracle, Exchange, Lotus, DB2, Informix, Sybase, SharePoint, Meditech and SAP. Must support NAS and storage array-based snapshot backup for off host zero downtime and zero load on the primary backup client with wizard-based configuration.	
27.	Backup Solution must support multi tenancy feature for creation of distinct data zones where the end users have access without being able to view data, backups, recoveries, or modify in other data zones.	
28.	Backup Solution should also have configurable ReST API support for management, administration and reporting on backup infrastructure via custom applications and out of box integration with VMWare vRealize Automation for complete orchestration.	
29.	The proposed backup software should support restore a single VM, single file from a VM, a VMDK restore from the same management console for ease of use.	
30.	Proposed backup software should not need a physical proxy server for VMWare backups and should have a minimum of 16 concurrent sessions capability for the VMWARE VM machines image-based backups with single virtual proxy. It should support instant access of a VM machine.	
31.	The proposed solution should have inbuilt feature for extensive alerting and reporting with pre-configured and customizable	



	formats. The proposed solution must have capability to do trend analysis for capacity planning of backup environment not limiting to Backup Application/Clients, Virtual Environment, Replication etc.	
32.	The proposed backup software should be able to recreate backed up data from existing volumes from metadata backups. The solution should offer recovery of specific volumes for recovery from metadata in case of a disaster recovery.	
33.	The proposed Backup software should have the capability for Block based backups with granular recovery capability for Windows, Linux, Hyper-V, VMWARE and Exchange for faster backups on supported Disk platforms.	
34.	The proposed backup solution should provide search capability from a web portal to allow search for a single file from complete backup store.	
35.	The solution should be capable of integration with active directory infrastructure for ease of user rights management along with role-based access control to regulate the level of management.	
36.	The solution should have the capability to manage and monitor backups at remote locations from a single backup server, where clients can backup data to a local disk backup device without the need of local media server or sending primary backup copy over the WAN.	
37.	The solution should have the capabilities to backup as well as archive data to cloud with cloud service providers like Azure / Amazon etc. In addition to this if data has to be moved from Cloud A to Cloud B the solution should be capable of cloud portability.	
38.	Proposed backup software should be in the leader's quadrant of 2017 Gartner report for Enterprise Backup software and recovery solutions.	
39.	Software updates and patches: For the period of minimum 5 years.	
40.	Use of Source and Target Based De-duplication for Backups. In order to improve the backup performance and reduce the disk footprint for storing backup data, the disk-appliance solution proposed by the Bidder must support inline global de-duplication and must integrate with the backup software to facilitate client direct backups to the backup disk with source based de-duplication to reduce data transfer over IP and FC Networks.	
41.	Replication of the Backup Data. The backup solution at DC shall allow automated scheduled replication to remote site (DR) for facilitating Disaster Recovery copy of backup data at DC.	

Storage- write & read operations



4.8.17. Networking- Data Center

a. L2 Switch (100 Gbps) WAN

Sr.#	Specifications	Compliance (Yes/ No) with comments, if any
A	General Features	
1.	High Density Wire-speed Layer3 Enterprise Class Switch	
2.	19" rack mountable – 1RU	
3.	Should have high-availability feature for active-active & active-passive operation from day-1	
B	Interfaces	
1.	12x40GbE & 12x100GbE & above ports from day-1. Additionally, it should support 2x10GbE SFP+ native ports. All ports should be populated with Multi-mode transceivers.	
2.	As per solution requirement the switch should support 1G, 10G, 25G, 40G & 100G transceivers from day-1. Bidder need to size the quantities of transceivers accordingly to solution	
3.	1 RJ45 console port, 1 RJ45 management port	
4.	USB port for external storage	



5.	HA cables to be included as part of solution	
C	Performance	
1	Minimum Switch Fabric Capacity: 4 Tbps or better	
2	Minimum forwarding rate of 1.4Bpps or better	
D	Architecture	
1	Should have redundant hot-swap power supplies & fans	
2	32MB packet buffer memory	
3	Modular operating system, OpenFlow 1.3 for software defined networking	
4	CLI commit, Uplink Failure Detection, BFD, Zero Touch Provisioning.	
5	Leaf/Spine fabric architecture using BGP EVPN, VXLAN.	
E	High Availability	
1	VRRP, active-active, active-passive operation	
2	Scripting function, control plane services, automation features, DevOps framework	
3	LAG load balancing based on L2, Ipv4 or Ipv6 headers	
F	Layer 2 features	
1	128 LAG groups with 16 ports per LAG	
2	128K ARP table, 160K MAC addresses	
3	Port, subnet based 802.1Q VLANs. The switch should support 4000 VLANs	
4	132K MAC addresses	
5	The switch should support IEEE 802.1w RSTP and IEEE 802.1s MSTP	
G	Routing Protocols	
1	BGPv4, OSPF v1/v2/v3, VXLAN routing from Day 1	
2	Ipv6 routing & VRF-Lite feature from day-1	
H	Security Features	
1	Layer 2-4 Access Control Lists	
2	RADIUS with EAP, 802.1X with RADIUS,	
3	SNMP ACLs, IP ACLs	
4	Streaming Telemetry, Control Plane Services	
5	WRR, deficit round robin, WRED, SP	
6	sFlow, NTP	
I	Traffic Policing	
1	Ingress/Egress shaping and policies	
2	Filter, mark and limit traffic flows	
3	Minimum 8 hardware queues per port	
4	Policy based traffic classification based on MAC Address, Port, DSCP, IP Address, VLAN	
J	Multicast	



1	MLD v1/v2	
2	IGMP v1, v2, v3, IGMP Snooping	
K	Network Management	
1	SNMP, RESTCONF APIs, Zero Touch Deployment (ZTD), Ansible, Puppet, Chef, SaltStack	
2	Ipv6 Management support telnet, FTP, TACACS, RADIUS, SSH, NTP	
L	IEEE Standards	
1	802.3ae, 802.3x, 802.3z, 802.1Qbb, 802.1Qaz	
2	IEEE 802.3ad LACP, 802.3ab LLDP, LAG loadbalancing	
3	IEEE 802.1p CoS Prioritization	
4	NTPv4, DHCPv4 server & relay	
M	Power Rating & Certifications	
1	Should operate on AC power ~50Hz. Power consumption should not be more than 650 Watts under full load.	
2	RoHS, Ipv6 ready for host and router, Fresh Air Compliant	
N	Connectivity required	
1	Required number of switches to be proposed in HA, SFPs from the to be from same OEM	
2	Switch should support direct attach cables, breakout cables of same OEM	
3	Cables – ethernet cables to be provided with switch for each port with throughput define.	
4	Seamless Integration: For Seamless Integration and Interoperability all the switches and SFP Modules should be fully compatible for smooth functioning of the system	
O	Event Management: There has to be a feature of Management Module/ tool to establish link with EMS platform.	

b. Layer 3 Core Switches – 48 ports 100G

S No.	Technical Specifications	Compliance (Yes/ No) with comments, if any
A	General Features	
1	High Density Wire-speed Layer3 Switch	
2	19" rack mountable – 2RU Switch can be chassis or fixed form Factor.	
3	Should have high-availability feature for active-active & active-passive operation from day-1	
B	Interfaces	
1	Wire rate 48x100GbE & above OSFP28 ports, all ports should be populated with Multi-mode transceivers.	
2	As per solution requirement bidder need to type & no. of transceivers accordingly.	



2	1x RJ45/USB console port, 1x ethernet management port	
3	USB port for external storage	
4	HA cables to be included as part of solution	
C	Performance	
1	Minimum Switch Fabric Capacity: 12.8Tbps or better	
2	Latency 300ns	
D	Architecture	
1	Should have redundant hot-swap power supplies & fans	
2	40MB packet buffer memory.	
3	Modular operating system, OpenFlow 1.3	
4	CLI commit, Uplink Failure Detection, BFD, Zero Touch Deployment.	
5	Should support Leaf/Spine fabric architecture using BGP EVPN, VXLAN.	
E	High Availability	
1	VRRP, active-active, active-passive operation	
2	Software upgrades with minimal traffic disruption during the upgrade	
3	LAG load balancing based on L2, Ipv4 or Ipv6 headers	
F	Layer 2 features	
1	128 LAG groups with 16 ports per LAG	
2	128K ARP table, 160K MAC addresses	
3	Port, subnet based 802.1Q VLANs. The switch should support 4000 VLANs	
4	130K or better MAC addresses	
5	The switch should support IEEE 802.1w RSTP and IEEE 802.1s MSTP	
G	Routing Protocols	
1	BGPv4, OSPF v1/v2/v3, VXLAN routing from Day 1	
2	Ipv6 routing & VRF-Lite feature from day-1	
H	Security Features	
1	Layer 2-4 Access Control Lists	
2	ACLs – port based/VLAN based.	
3	Integrated security features like DHCP relay, Control Plane DoS protection	
4	Streaming Telemetry, Control Plane Services	
5	802.1X Network Security and Authentication	
6	RADIUS, TACACS, sFlow, NTP	
I	Traffic Policing	
1	Ingress/Egress shaping and policies	
2	Filter, mark and limit traffic flows	
3	Minimum 8 hardware queues per port	
4	Policy based traffic classification based on MAC Address, Port, DSCP, IP Address, VLAN	
J	Multicast	



1	H/W based Ipv4 or Ipv6 Multicasting (minimum 10000 group supported)	
2	IGMP v1, v2, v3, IGMP Snooping	
3	Protocol Independent Multicast – Sparse Mode and PIM – SSM	
K	Network Management	
1	Ansible, Puppet, Chef, SaltStack, RESTCONF APIs	
2	Ipv6 Management support telnet, FTP, TACACS, RADIUS, SSH, NTP	
L	IEEE Standards	
1	802.3ae, 802.3x, 802.3z	
2	IEEE 802.3ad LACP, 802.3ab LLDP	
3	IEEE 802.1p CoS Prioritization	
4	802.1Qbb, 802.1Qaz	
M	Power Rating & Certifications	
1	Should operate on AC power ~50Hz. Power consumption should not be more than 1200Watts under full load.	
2	RoHS, Ipv6 ready, FCC CFR 47 Part 15, EN 61000-4-5: Surge	
N	Connectivity required	
1	The switch & transceivers should be from the same OEM	
2	Cables - - ethernet cables to be provided with switch for each port with throughput define.	
3	Seamless Integration: For Seamless Integration and Interoperability all the switches and SFP Modules should be fully compatible for smooth functioning of the system	
P	Event Management: There has to be a feature of Management Module/ tool to establish link with EMS platform.	

c. Layer 2 TOR Switches (For NAS storage) – 48 Ports 10G

Sr No.	Technical Specifications of ToR Switch	Compliance (Yes/ No) with comments, if any
A	General Features	
1	High Density Wire-speed Layer3 Switch	
2	19" rack mountable – 1RU	
3	Should have high-availability feature for active-active & active-passive operation from day-1	
B	Interfaces	
1	Wire rate 48x10 GbE SFP28 ports and 6x100GbE QSFP28 ports. All ports should be populated with Multi-mode transceivers.	
2	As per solution requirement the switch should support 1G, 10G, 25G, 40G & 100G transceivers from day-1. Bidder need to size the quantities of transceivers accordingly.	



3	1 RJ45 console port, 1 RJ45 management port	
4	USB port for external storage	
5	HA cables to be included as part of solution	
C	Performance	
1	Minimum Switch Fabric Capacity: 4Tbps or better	
2	Latency 850ns	
D	Architecture	
1	Should have redundant hot-swap power supplies & fans	
2	32MB packet buffer memory.	
3	Modular operating system, OpenFlow 1.3	
4	CLI commit, Uplink Failure Detection, BFD, Zero Touch Deployment.	
5	Should support Leaf/Spine fabric architecture using BGP EVPN, VXLAN.	
E	High Availability	
1	VRRP, active-active, active-passive operation	
2	Software upgrades with minimal traffic disruption during the upgrade	
3	LAG load balancing based on L2, Ipv4 or Ipv6 headers	
F	Layer 2 features	
1	128 LAG groups with 16 ports per LAG	
2	128K ARP table, 160K MAC addresses	
3	Port, subnet based 802.1Q VLANs. The switch should support 4000 VLANs	
4	132K MAC addresses	
5	The switch should support IEEE 802.1w RSTP and IEEE 802.1s MSTP	
G	Routing Protocols	
1	BGPv4, OSPF v1/v2/v3, VXLAN routing from Day 1	
2	Ipv6 routing & VRF-Lite feature from day-1	
H	Security Features	
1	Layer 2-4 Access Control Lists	
2	ACLs – port based/VLAN based.	
3	Integrated security features like DHCP relay, Control Plane DoS protection	
4	Streaming Telemetry, Control Plane Services	
5	802.1X Network Security and Authentication	
6	RADIUS, TACACS, sFlow, NTP	
I	Traffic Policing	
1	Ingress/Egress shaping and policies	
2	Filter, mark and limit traffic flows	
3	Minimum 8 hardware queues per port	
4	Policy based traffic classification based on MAC Address, Port, DSCP, IP Address, VLAN	



J	Multicast	
1	H/W based Ipv4 and Ipv6 Multicasting (minimum 10000 group support)	
2	IGMP v1, v2, v3, IGMP Snooping	
3	Protocol Independent Multicast – Sparse Mode and PIM – SSM	
K	Network Management	
1	Ansible, Puppet, Chef, SaltStack, RESTCONF APIs	
2	Ipv6 Management support telnet, FTP, TACACS, RADIUS, SSH, NTP	
L	IEEE Standards	
1	802.3ae, 802.3x, 802.3z	
2	IEEE 802.3ad LACP, 802.3ab LLDP	
3	IEEE 802.1p CoS Prioritization	
4	802.1Qbb, 802.1Qaz	
M	Power Rating & Certifications	
1	Should operate on AC power ~50Hz. Power consumption should not be more than 650 Watts under full load.	
2	RoHS, Ipv6 ready, FCC CFR 47 Part 15, EN 61000-4-5: Surge	
N	Connectivity required	
1	The switch & transceivers should be from the same OEM	
2	Cables – ethernet cables to be provided with switch for each port with throughput define.	
O	Seamless Integration: For Seamless Integration and Interoperability all the switches and SFP Modules should be fully compatible for smooth functioning of the system	
P	Event Management: There has to be a feature of Management Module/ tool to establish link with EMS platform.	

d. Layer 2 switch – KVM Management switches

S No.	Features	Specification	Compliance (Yes/ No) with comments, if any
1.	Interface requirements	Minimum of 24 ports 10/100/1000 Base-T and 4x 10G SFP+ ports	
2.		1 x Out of Band IP based management Port, 1 Console Port, USB Port / External Flash	
3.		support stacking for upto 8 switches with minimum 40 Gbps stacking.	
4.		Have Redundant Power Supply support and variable speed fan to adjust to varying weather conditions in campus	



1.	Design & Performance	Each switch should have minimum 128 Gbps or more with non-blocking architecture and Forwarding rate of 95 Mpps	
2.		Should be equipped with minimum 1GB RAM and 1GB flash	
3.		Should have LED indicator for per port status, FAN, PSU and Management Status	
4.		0°C to 45°C operating temperature and 10% to 95% relative humidity	
5.		Hardware and software configuration have for Ipv6 from day one	
1.	Switching / Routing	Should have 16 K MAC Address, 500 active Vlans	
2.		802.1D spanning Tree and PVST+, 802.1w, 802.1s, should have BPDU Guard or equivalent feature on edge port to auto disable port for a configurable time period to if an accidental loop occurs in the network	
3.		Audio Video Bridging to enable reliable, real-time audio/video transmission over Ethernet	
4.		Should support aggregating and load balancing of traffic to two or more peer switches within same VLAN	
5.		Should support MSTP protocol	
6.		Should have Port based VLAN, MAC based VLAN, private vlan and support GVRP	
7.		Should have Local, Remote and multisession port mirroring (minimum 4 session)	
8.		Support Standard based protocols for lossless transport of real time data with dynamic QoS reservation.	
9.		Should have 8 Hardware QoS Queues per port	
10.		Should have traffic rate limiting with Configurable bandwidth granularity of 64 KBps	
11.		Should have Link Layer Discovery Protocol (802.1ab) to allow recognition of third-party network devices and LLDP MED for auto configuration	
12.		Should have MAC address tracking and notification for mac address addition, delete or movement in the Network	
13.		Should support policy-based routing and switching	
14.		Should have basic dynamic routing protocols like RIP, OSPF, PIM, VRRP on day one	



15.		Should have Configurable multicast session limit per port	
1.	Security	Local authentication database for RADIUS Authentication for 802.1x login	
2.		Should have MAC security – Lockdown & Limit and MAC address tracking with syslog & snmp notification	
3.		Should have SSH-2, SCP, SFTP for secure management	
4.		Should have dynamic arp inspection, DHCP snooping, Private VLAN, SYN attack protection, GARP protection	
5.		Should have ASIC based traffic flow analysis based on Netflow/ sFlow/ Ipflix	
6.		Should have minimum 1 K ACL entry support and Time-Based ACL or Port-based ACL	
1.	Management	Should have scheduled archiving / uploading of configuration and system log to a central server	
2.		Should support inbuilt DHCP server and Client for quick configuration of endpoints and switch	
3.		Telnet server, ssh server, Ping and traceroute over Ipv6	
4.		Should have L2 Traceroute, L2 Ping and Multicast Traceroute	
5.		Console and CLI management	
6.		Dual firmware and configuration rollback	
7.		Should be SDN capable with Open stack support and OpenFlow API support, should support IEEE P802.1Qaz	
8.		Should support Energy Efficient Ethernet 802.3az	
1.	Certification	Model should have safety and standards certifications as below: IEC61000-4-6:2008/EN61000-4-6:2009, IEC61000-4-8:2009/EN61000-4-8:2010 , EN 55022:2010 Class A, CISPR 22:2008 Class A, CISPR24:2010ClassA, Radiated Immunity 10V/criteria, UL60950-1 2ndEd, CE 2.0 Compliant or equivalent Indian Standards.	
2.		Seamless Integration: For Seamless Integration and Interoperability all the switches and SFP Modules should be fully compatible for smooth functioning of the system	



1	Event Management	There has to be a feature of Management Module/ tool to establish link with EMS platform.	

e. Layer 2 TOR Switches – 48 Ports 10G

S No..	Technical Specifications of ToR Switch	Compliance (Yes/No) with comments, if any
A	General Features	
1	High Density Wire-speed Layer3 Switch	
2	19" rack mountable – 1RU	
3	Should have high-availability feature for active-active & active-passive operation from day-1	
B	Interfaces	
1	Wire rate 48x10 GbE SFP28 ports and 6x100GbE QSFP28 ports. All ports should be populated with Multi-mode transceivers.	
2	As per solution requirement the switch should support 1G, 10G, 25G, 40G & 100G transceivers from day-1. Bidder need to size the quantities of transceivers accordingly.	
3	1 RJ45 console port, 1 RJ45 management port	
4	USB port for external storage	
5	HA cables to be included as part of solution	
C	Performance	
1	Minimum Switch Fabric Capacity: 4Tbps or better	
2	Latency 850ns	
D	Architecture	
1	Should have redundant hot-swap power supplies & fans	
2	32MB packet buffer memory.	
3	Modular operating system, OpenFlow 1.3	
4	CLI commit, Uplink Failure Detection, BFD, Zero Touch Deployment.	
5	Should support Leaf/Spine fabric architecture using BGP EVPN, VXLAN.	
E	High Availability	
1	VRRP, active-active, active-passive operation	
2	Software upgrades with minimal traffic disruption during the upgrade	
3	LAG load balancing based on L2, Ipv4 or Ipv6 headers	
F	Layer 2 features	
1	128 LAG groups with 16 ports per LAG	
2	128K ARP table, 160K MAC addresses	
3	Port, subnet based 802.1Q VLANs. The switch should support 4000 VLANs	
4	132K MAC addresses	



5	The switch should support IEEE 802.1w RSTP and IEEE 802.1s MSTP	
G	Routing Protocols	
1	BGPv4, OSPF v1/v2/v3, VXLAN routing from Day 1	
2	Ipv6 routing & VRF-Lite feature from day-1	
H	Security Features	
1	Layer 2-4 Access Control Lists	
2	ACLs – port based/VLAN based.	
3	Integrated security features like DHCP relay, Control Plane DoS protection	
4	Streaming Telemetry, Control Plane Services	
5	802.1X Network Security and Authentication	
6	RADIUS, TACACS, sFlow, NTP	
I	Traffic Policing	
1	Ingress/Egress shaping and policies	
2	Filter, mark and limit traffic flows	
3	Minimum 8 hardware queues per port	
4	Policy based traffic classification based on MAC Address, Port, DSCP, IP Address, VLAN	
J	Multicast	
1	H/W based Ipv4 and Ipv6 Multicasting (minimum 10000 group support)	
2	IGMP v1, v2, v3, IGMP Snooping	
3	Protocol Independent Multicast – Sparse Mode and PIM – SSM	
K	Network Management	
1	Ansible, Puppet, Chef, Salt Stack, RESTCONF APIs	
2	Ipv6 Management support telnet, FTP, TACACS, RADIUS, SSH, NTP	
L	IEEE Standards	
1	802.3ae, 802.3ba, 802.3bj, 802.3x, 802.3z	
2	IEEE 802.3ad LACP, 802.3ab LLDP	
3	IEEE 802.1p CoS Prioritization	
4	802.1Qbb, 802.1Qaz	
M	Power Rating & Certifications	
1	Should operate on AC power ~50Hz. Power consumption should not be more than 650 Watts under full load.	
2	RoHS, Ipv6 ready, FCC CFR 47 Part 15, EN 61000-4-5: Surge	
N	Connectivity required	
1	The switch & transceivers should be from the same OEM	
2	Cables - - ethernet cables to be provided with switch for each port with throughput define.	
O	Integration	
1	Seamless Integration: For Seamless Integration and Interoperability all the switches and SFP Modules should be fully compatible for smooth functioning of the system	
P	Event Management:	



1	There has to be a feature of Management Module/ tool to establish link with EMS platform.	

f. Secure Network Device (SD-WAN Gateway Router)

Solution should support build in NGFW feature (Anti Spyware, IPS, Anti-Virus and application control) to protect network against threats or external NGFW solution can be quoted separately

S No.	Features	Specification	Compliance (Yes/ No) with comments, if any
1	General	Proposed vendor must be placed in Leader and Challengers Quadrant in Gartner SD-WAN or leader Gartner quadrant for Enterprise Firewall. NSS recommended vendor shall be preferred.	
		The SDWAN device should be supplied with Redundant hot swappable Fan trays/ multiple fan module and Power supply and solution shall support Ipv6 like application identification, Zone protection, management etc. from Day-1	
1	SDWAN Architecture	Proposed SDWAN solution should have management-based architecture and if management appliances/solution goes offline the SDWAN solution should keep on functioning without any issues. Must support build in GUI as well for any onsite changes if required	
2		The bidder shall propose at least one management solution as asked above	
3		Management architecture should have option to be deployed in HA if required in future.	
4		Management architecture should support on premise Model as well as have option of hosting on cloud.	
5		There should not be any impact on SDWAN data forwarding capability in case of complete disconnection of management	
6		Management architecture should support Virtual firewall/ multi-tenancy and the proposed device shall minimally have Common Criteria and Internet Computer Security Association (ICSA) Certification and should not have any enabled wireless code in the offered device or its family in hardware or software.	



7		Management architecture should support rich policy constructs to manipulate routing information, access control, segmentation, Application control.	
8		Solution should provide transport independence and should allow to use any transport like MPLS, Internet, 3G/4G/broadband, Point to Point link	
9		Licensing of SD-WAN solution must be based on device capacity not on bandwidth capacity / restriction	
10		Architecture must support zero touch deployment, so that minimum effort is required to deploy the solution	
Chapter	Operations	It should support multi-cast network	
Chapter		Network would be functional at the time of connectivity failure between controller and branch device.	
Chapter		System Should able to support of network elements to deploy any kind of topologies such as any-to-any, Hub-spoke and Partial mesh.	
Chapter		System should able to support Multiple WAN Links utilization and detecting blackouts & brownouts by supporting active / active load balancing & Fast session failover	
Chapter		System must support Diverse WAN including T1, E1, LTE, PPPoE, DSL, Fibre and Ethernet	
1	Security	Management and SDWAN solution should	
2		communicate over encrypted channel	
3		Solution must support templates to be applied to the groups of police station quickly	
4		SDWAN Router should support strong encryption like AES 256 or higher	
5		PACKET REDISTRIBUTION must be supported even over IPSec tunnel and it should support sub second path failover and recovery	
6		Proposed solution must support creation of logical	
7		separate sub-domain within single physical devices to separate different kind of networks.	
8		SDWAN solution should support integration with cloud based/appliance-based security solutions or should have inbuilt security features like content filtering and antivirus	
9		SDWAN solution should support split tunneling to provide direct internet access from branch	



10		SDWAN solution shall have built in feature to protect CPU under DoS/DDos attacks	
11		SDWAN architecture should support application identification at layer-7 and should able to identify minimum 3000 applications or as per throughput mention above natively. It should also allow to define custom applications as per requirement	
1	Routing and QoS	SDWAN solution should allow minimum 2 service providers at branch locations and 4 service providers at DC.	
2		SDWAN solution should support BGP and Static routing	
3		SDWAN solution should support performance SLA based on latency, packet loss, jitter or all 3 combined	
4		SDWAN edge devices should support 802.1Q, sub interface, Inter VLAN routing	
5		SDWAN solution should support rule-based routing based on Application, user, user group, source, destination or combination of any of them	
6		SDWAN Solution should support rule creation based on Application or source address or destination address and each rule should have option to use different performance SLA	
7		SDWAN should support QoS based on application	
8		SDWAN device should support FEC (Forward Error correction) and DSCP matching	
9		SDWAN device must support BGP additional path support and route-map	
10		SDWAN device solution must support Auto VPN	
1	Management	Management solution should be appliance/VM which must support around 300 SDWAN devices at Day 1 scalable to 1000. If VM option is quoted than server should be given along with all the necessary licenses	
2		Management solution should have built in GUI which can be accessed by any popular browser and no extra software must be required to open management GUI access	
3		Should have template option to push common policy across all SDWAN solution	
4		Must have dashboard showcasing all the SDWAN solution across the network with their latency and link status	



5		Centralized management should have open APIs to integrate with third party management	
6		Centralized management should support role-based access	
7		Management must support IPSec wizard which can push vpn configuration to various SDWAN devices with the routing information updates.	
1	Logging & Reporting	The Logs and Reporting platform must be a dedicated same OEM appliance and VM/software running on server will not be accepted.	
2		The Logs and Reporting platform support running on-demand and scheduled reports	
3		Should have minimum 10 TB or more of Hard Drive Capacity in RAID1, for logging and reporting if provided as separate management as from firewall	
4		Real-time display of information allows you to follow real-time trends in network usage such as the source IP address and the destination URL for HTTP traffic or IM message traffic.	
5		All log files and messages are searchable and can be filtered to drill down and locate specific information.	
6		The logging Appliance should support multiple types of report format PDF, HTML, CSV and XML.	
1	Licensing	All license for Monitoring, management, VPN and Logging should be quoted. Vendor should quote all the license from day one related to proper SD-WAN deployment and all the feature requested above.	
2		License for any unmentioned feature which require proper deployment and functioning of SD-WAN must be quoted. Vendor shouldn't have any hidden charges	
1	Performance Parameter	The SDWAN device at DC should have minimum 4x40 QSFP+/QSF28, 10x 10GE SFP+ slots and 10x GE RJ45 ports to cater to connectivity from multiple service providers. SFPs Transceivers should be populated as per solution requirement from Day1. HA ports, Console and OOB should be taken extra	
2		Threat Prevention Throughput of 30 Gbps on enterprise mix/ Application mix and IPSec encryption throughput should be minimum 25 Gbps.	



3		Minimum 400K new session per second, 30Mn concurrent session, 15K Site to Site VPN Tunnels, 20K Concurrent SSL VPN Users.	
4		The device should have Internal Redundant Power Supplies and redundant hot swappable fan trays	



g. Racks with Smart PDU

Sr No	Specification	Minimum Requirement	Compliance (Yes/No) with comments, if any
1	General	42 U X 600mm X 1200mm (H x W x D) rack should have metal frame supporting more than 1300 kgs of static load and more than 1000 kg of dynamic load.	
2		Single front door and split rear door should have the perforation of more than 75% to provide the maximum airflow eliminating the need of additional FHU in the rack.	
3		Doors shall have lift of hinges for tool less field reversibility.	
4		Rack should have integrated hole pattern for easy installation of top panel accessories have removable opening for cable entry and shall accommodate 2000 cat 6 cables to suffice the cabling requirements.	
5		Rack should have two pair of 19-inch EIA mounting rail with U marking on front and rear of each rail for ease of installation.	
6	Cable Manager	Rack should have dual purpose full height depth adjustable PDU/Cable management brackets and should be mounted in the zero U space.	
7		PDU/Cable management brackets shall have button mount keyholes throughout to accommodate the tool less mounting of rack PDU's of various heights and accessories mounting holes for toolless cable mounting accessories.	
8	Panel	Rack should have split side panels with single locking slam latch for quick and easy installation and maintenance, single person removal and installation eliminates the manpower dependencies.	



9	Caster & Levelling	42 U rack frame height that allows access through standard doors on four swivel casters, rack shall have the levelling feet and shall be accessible from the top of the frame for easy adjustment.	
10	Hardware Accessories / Installation ease	Rack shall have the necessary hardware accessories ((50 each M6 cage nuts and screws), Cage nut installation tool, edge protection for top panel cable entry, T30 / Phillips L key, T30 extension driver.	
11		Rack shall have necessary baying brackets and the bolt down kits	
12		Rack frame design should allow 2.5 inch more usable space in the rack for the proper equipment placement and ease of access.	
13	Powder Coating	Rack should have the powder coated black color, RAL 7021.	
14	Certification	Rack shall have EIA, UL, RoHS, REACH certified	
15	Power Distribution	Rack shall have two power distribution unit, vertically mounted on the rear of the rack to power on the devices in the rack.	
16	Power Distribution Unit	Monitored, Unit Level, 32Amps, 230V, 1 Phase, 7.3KW, Vertical, 30 IEC C13, 6 IEC C19, Locking Sockets, 3m power Cord with 2P+E (IP44)	
17		The PDU shall have locking outlets – cable locking mechanism so that it should not require the locking cable to secure the cables connected to the PDU	
18		PDU shall have Input and Breaker level current monitoring. Local high visibility LED display.	
19		PDU shall have Phase (A) Monitoring (kWh, W, VA, PF, V, A) Power Measurements Compliant with ANSI C12.1 and IEC 62053-21 at 1% Accuracy Class Requirements and Circuit / Breaker Monitoring (A)	



20		Circuit/Breaker Current Measurements Independently Tested and Verified at 2% Accuracy.	
21		The PDU shall support the mobile app for the power monitoring and should be easy to be shared in various formats	
22		The PDU shall be upgrade ready so that it can be changed to monitored PDU without downtime, by simply changing the Field replaceable IMD unit.	
23		PDU shall have button mounting option for easy toolless installation and reinstallation of the PDU's	
24		PDU shall have colored outlets to differentiate the outlets based on the breakers.	
25		The PDU should be CE certified.	
26	Rack	Both rack and PDU should come with 5 years of default warranty	

h. IPPBX

S No.	Description	Compliance (Yes/No) with comments, if any
A.	The system should be based on server-gateway architecture running on Linux OS supporting Analog, Digital, IP, SIP and Wireless Extensions.	
	System shall be non-blocking and open standard (based on H.323 and SIP). The call control system should be fully redundant solution and should provide 1:1 redundancy.	
	The servers should be of industry standard make COTS product. The proposed server configuration should be capable of supporting at least 3000 extensions in future without changing the hardware. The expansion should not require any additional hardware or clustering of multiple PBX.	
	The server should have the following minimum specifications in Virtual or physical environment: 12 cores @ 2.4 GHz base, 32 GB RAM, 3Gbps network connectivity.	
	The system should be capable of deployment on virtualized platforms like VMWare/Hyper-V etc.	
	System should provide call control, mobility, IM and presence, Web-Collaboration, Messaging and centralized licensing.	



	The system should support standards-based multi-site networking, using QSIG, H.323 trunks or advanced networking, to interoperate with other PABX's, allowing feature transparency.	
	Voice CODEC support G.711, G.729, G.729a & G.722 or any less utilization bandwidth across WAN and LAN	
	Video CODEC: H.264 or Equal	
	System should have built-in SIP and H.323 gatekeeper functionality without the need to put any additional hardware	
	System should support SIP trunking to Internet Telephony Service Providers, allowing non-SIP phones to make SIP calls	
	Multiple building is planned in the campus and the same system should support at least 100 remote sites on the same platform through gateways.	
	The system should provide complete inbuilt encryption capabilities or features without any external firewall, with the ability to encrypt all traffic (media and call control signaling) between IP phones, soft phones, call controllers and all other associated endpoints via a strong encryption algorithm like IPSec or SRTP etc.	
	System should be able to provide centralized voicemail with the option of Distributed centralized voicemail in case of connectivity failure.	
	The system should support BRI/ PRI/ T1/ E1/Analog/IP/SIP Trunks.	
	The communication server should offer BHCC (Busy Hour Call Completion) of at least 20000 per server to ensure superior traffic handling capacities.	
	The offered system should be modular in design. The architecture of IP PBX should be capable of seamless migration to its maximum capacity by simply adding licenses/peripheral cards on the set of control server without compromising on any functions/ features of this system or any degradation of service.	
	The system should be able to provide hybrid end points i.e. both IP and TDM. They should also provide support for 100% TDM endpoints.	
	The proposed communication system should have a highly secured, encrypted IP supporting hybrid Trunks e.g. Analog CO, Digital Trunks (BRI and PRI), IP Trunks (H.323/SIP)	
	System should have in built-in DHCP Server, which should be able to give IP Addresses to the endpoints.	
	System should support built-in Remote access server (RAS) functionality.	
	System should support DiffServ for QoS (Quality of service) for the voice packets traveling over data networks	
	System should support standards-based CTI integration with 3rd party applications	
	System should support WebRTC based application for Web Collaboration users for Windows and Mac OS	



	Should support Active Directory integration for directory synchronization and user authentication.	
	The equipment quoted by bidder must be SIP compliant	
	The offered system should have a valid TEC approval. TEC approval certificate copies for ISDN connectivity should be enclosed along with the offer.	
B	DESIRED FEATURES & FACILITIES OF IP PBX:	
	The offered solution should provide the following features as a part of its telephony functions.	
	Call Coverage	
	Call Forwarding	
	Call Hold	
	Call Intrude	
	Call Park	
	DND	
	Ring Back When Free	
	Suspend Call Waiting	
	Distinctive and Personalized Ringing	
	Toggle Calls	
	Account Codes	
	Call Barring	
	Bridged Appearance	
	Group Paging	
	Hot Desking	
	Mobile Twinning	
	Multiple Appearance Directory Number (MADN)	
	Intrusion Warning Tone	
	Alternate Route Selection	
	Flexible numbering Schemes	
	Time of Day and Date Routing of Calls	
	Call Recording	
	PIN Restricted Calling	
	Time Profiles	
	Queue announcements	
	Call Detail Recording	
	SMDR (Station Messaging Detail Record)	
	Fax on demand integration	
	Station Call – User can dial any extension anywhere in central location and other distributed location by dialing simple extension number.	
	Support Tone dialing from an extension.	
	Authorization Codes - 5-7-digit authorization code to make outgoing toll calls for ensuring no misuse of the system.	
	Automatic Call Back – User can register ACB feature to any extension of the offered system.	



	Call pickup within the group as well as outside the group	
	Alternate Routing – Automatically re-route calls which encounter a busy trunk on the initial route. Automatic digital translation is carried out by the system. Provides the possibility of reaching external destinations via different routes.	
	Call Detail Recording – Records detailed call information on all incoming and outgoing calls on specified trunk groups and stations, including those administered for intra-switch recordings, and send this information to any printer of time/duration as and when required. Necessary hardware and software if required to be quoted separately.	
	Class of Service – Defines whether or not voice terminal users may access the following features and functions:	
	Automatic Call-back, Call Forwarding, Call Forward, Busy/Don't Answer, Data Privacy, Extended Forwarding, Extended Call Forward Busy/Don't Answer, Priority Calling, Restrict Call Forwarding Off-Net, Personal Station Access, Trunk -to-Trunk, Transfer Restriction Override, Off-Hook Alert & Console Permission.	
	DID/DOD (Direct Inward/Outward Dialing) – The proposed system must support direct inward dialing for external parties to call in.	
	Direct Inward Station Access – This feature must be optionally available, allowing an outside caller to access switch features by dialing a special telephone number without attendant assistance, it should permit access to the server and long-distance facilities from off-premise stations. For security, there should be the option of turning off this feature.	
	Day/Night Trunk Control – To reduce cost and improve system security it should be possible to restrict the access to certain trunks depending on time of day.	
	Distinctive Ringing – To provide audibly different ringing patterns between internal, external and special feature calls.	
	Flexible numbering plan – Support up-to 2-15 Digit for an extension number and allow phone number assigned to a station to a station to be changed through software.	
	System Abbreviated Dialing - To have the ability to store a list of frequently called numbers that will be available on a systemwide basis to all users.	
	The system should support internal MOH (Music on Hold), which should be uploaded using the .Wav file and should have an audio input port for external MOH connectivity.	
	CLI (Caller Line Identification) facility (CLIP/CLIR) - Calling Numbers (internal & external) should be displayed on all Analog extensions (FSK support phone).	



	Web collaboration for desktop and application collaboration, whiteboarding and document sharing. It should be possible to escalate from an audio call to web collaboration. It should provide a document library possible to upload documents, presentations and pictures to a document library for quickly sharing during a web collaboration session.	
C	Voice Gateway	
	GW should support X.21/V.35 WAN Interface.	
	GW should have relays for door entry systems.	
	GW should be 19" rack mountable.	
	GW should have in-built 2 port auto-sensing LAN Switch (Layer 3)	
	GW should have Integral Static or Dynamic (RIP I/II) routing for both Internet and Branch-to-Branch solutions	
	GW should support Frame Relay WAN protocol	
	GW should support the following protocols: PPP, ML-PPP, CHAP, PAP, ARP, BACP	
	GW should be able to provide redundancy to all users in case of failure of redundant servers	
	GW should support at least 148 DSP channels on each gateway.	
	For a seamless integration GW should be of same make of IPPBX	
D	Terminal Support	
	System should support the following type of terminals	
	Analog Phones	
	Digital Phones	
	IP Handphones	
	IP/SIP Softphones	
	Video Hard/Softphone	
	Wireless IP Phones (802.a/b/g/n)	
	3rd party SIP phones RFC3261 Compliant	
E	Trunk Support	
	System should support following types of trunks:	
	Analog Trunks	
	PRI	
	BRI	
	T1/ E1/ E1R2	
F	Voicemail Features	
	System should have inbuilt voice mail system	
	Voicemail to email option should be available	
	System should support unified messaging with Microsoft Exchange or any IMAP compliant email application.	
	System should support voicemail access through web-browser	
	External Fax server integration should be possible.	
	VM should support text-to-Speech functionality	
	VM should support Dial-by-Name functionality	



	VM should support Auto Attendant	
	IVR functionality should be available	
G	Conferencing Features	
	The campus will have various departments each with a capacity of 50-60 people. Each department can have it conference call. 6-7 such departments can have parallel calls at any given time. So, system should have built-in 64*8 party Ad-Hoc or Meet-Me audio conferencing bank from day 1.	
	Multiple conferences with variable number of users should be possible within each of the conferencing banks.	
	System should be able to generate detailed reports about the conference.	
	System should be able to send emails to all the participants giving them the conferencing details	
	System should support PIN based security for conference calls.	
	System should support scheduling of conference call.	
H	Management Interface	
	System should be able to be configured and administered using a GUI based application	
	System should support SNMP based network management	
	In case SNMP management is not available, system should be capable of sending event notifications to up-to 3 email addresses, each with a different set of alarms	
I	UC Functionalities	
	Same Unified Communications (UC) client that provides users with real time collaboration capabilities	
	Support for Windows and Mac OS	
	Support for Android and iOS devices Smartphones	
	The Softphone should provide full call control from an iPhone or Android powered smartphone.	
	Make and receive phone calls and instant messages, host and attend audio conferences.	
	See employee availability via presence, and use Geo-tracking to determine the location in the field.	
	All of this is done using the corporate directory, so there are no personal cell phone numbers will be involved.	
	The Softphone application should be downloadable from Google Play store or Apple iTunes without any additional cost for any number of devices.	
	Solution should provide a “presence” application for users, so that they can see the availability status of their contacts in their contact list.	
	The common supported status for this application should be available, busy, idle, away etc.	



	The instant messaging application should support manual setting of user status to: Available, Away, Do Not Disturb (DND) etc.	
	Shall provide support for open protocols like XMPP.	
J	IP PHONE TYPE 1	
	2.8" (diagonal) color display—320 x 240 pixels	
	Multiple line phone with four red / green line / feature indicators around display	
	4 Context Sensitive Soft Keys	
	Hard buttons for phone, messages, contacts, history, home, navigation cluster, headset, speaker, volume, mute	
	LEDs for speaker, mute, headset, message, history	
	Wideband audio in handset and wired headset	
	Full duplex speakerphone & Handset	
	Ergonomic hearing aid compatible handset supports TTD acoustic coupler	
	Message waiting indicator	
	Mute key with optional mute alerting	
	IC call alerting with 360—degree visibility	
	Rich, classic, alternate, and downloadable ringtones	
	Dual—position stand, optional wall—mount stand	
	Gigabit Ethernet (10 / 100 / 1000) line interface	
	Second Ethernet interface 10 / 100 / 1000 Mbps	
	PoE Class (IEEE 802.3af) registers as class 1 device and supports 802.3az	
	Optional AC to 5-volt power supply	
	SIP protocol support	
	Standards—based codec support: G.711, G.726, G.729A / B, G.722, Opus	
	Configurable via Web Interface	
	Support for TLS / SRTP for encryption	
	Recent Call Log (100 entries) / Contact List (250 entries)	
	IP Phone should be from the same OEM of PBX	
K	IP Phone Type 2	
	8" Capacitive Touch color display	
	Resolution: 1280 X 800 pixel	
	24 bits color depth	
	An integrated camera (A mechanical camera shutter that covers the camera lens)	
	Standards-based codec support: G.711, G.726, G.729A/B, G.722, H 264, Opus.	
	No mechanical dial-pad	
	Message Waiting Indicator	
	1X RJ9 analog headset port or higher	
	1X 3.5 mm audio jack socket or higher	



	1X USB Type-C port or higher	
	1X Handset cradle connector	
	Power over Ethernet IEEE 802.3af (Class 3) or 802.3at (Class 4)	
	SIP protocol support	
	Downloadable ring tones	
	Downloadable Wallpapers	
	End users can install third party applications on Google Play™ store. The system administrator can restrict installation of certain applications	
	16 GB flash memory	
	Dual Port RJ45 connected Ethernet	
	Wireless access point mode	
	5GHz Wireless 802.11a/b/g/n/ac	
	Hotspot	
L	Analog Phone	
1.	- FSK & DTMF Dual mode – Type 1 - Open listening & hands-free talking - Handset Volume Adjustable - Mute function (With melody) - 50 entries for CLIP - Real time clock - Last 5 number redial. - Adjustable ringer Volume & tone Sequence - 10 Repertory Keys - Call Duration display	
M	Citizen Notification	
	Notification Formats	
	System must Support Voice Call Notification – Office Phone, Cell Phone, Home Phone	
	System must support SMS, Email, Speakers / Paging	
	User Contact Lists	
	System must offer Web based self-service management	
	It should be possible by administrator to define attributes (location, role, etc.) for users	
	It should support CSV File Upload for contacts	
	Message Configurations	
	System should support One-way Notification & ACK	
	System should be able to notify and respond and Notify to Conference to all stake holders	
	System should support auto Escalation or cascading chains of notifications whenever needed	
	Administration Portal (Web Application)	
	User/Group Mgmt.	
	Partition Mgmt for different departments	



	Conferencing Configuration	
	Security Configuration	
	Channel (Device) Configuration & Mgmt.	
	Communications Resource Mgmt.	
	Broadcast Trigger Configuration	
	Inbound Call Trigger Configuration	
	Message Inbox Configuration	
	Operations Portal (Web Application)	
	System Admin must be able to define Notification Scenario for quick management and for the tight integration IPPBX and Notification system must be from same OEM	
	System admin must be able to do Message Mgmt. (Pre-recorded, "record on the fly", Text-To-Speech)	
	User / Group Profile Mgmt.	
	Escalation Configuration	
	Security Configuration	
	Message Broadcast (Priority)	
	Audit logs and Reports (Web and PDF formats), Data and Analytics	
	System must be able to reach 500 people within 10 minutes to play 30 second voice announcements.	
N.	Video End point	
	Video Standards: H.263, H.264, H.265	
	The Video Conferencing unit should support inbuilt 1+8 Full HD Multi Party Conferencing	
	Should support 30 fps & 60fps (frames per second) with 1080p resolution from day one	
	Video Features: Ability to send and receive two live simultaneous video sources in a single call, so that the image from the main camera and PC or document camera can be seen simultaneously	
	Should support H.239 and BFCP protocols with 1080p resolution	
	Video Output: Should have at least 2 HDMI / DVI (High Definition Multimedia Interface) output to connect Full High Definition display devices such as LCD / LED and projectors for both Video and Content. (Dual Monitor Support)	
	It should be possible to display the main video on one HD screen and the presentation / dual video on the other HD screen	
	Video Input: Should have at least one HD video Input to connect HD camera with full functionalities as mentioned in the camera specifications	
	Should have DVI (Digital Video Interface) input to connect PC / Laptop directly to the Video conferencing system and display resolutions WXGA / HD720p along with PC Audio	
	Audio standards: G.711, G.722, G.722.1, 64 kbps MPEG-4 AAC-LD or equivalent standards must be supported.	



	Audio Inputs: Should support minimum 2 Microphone inputs. 1 needs to be supplied from day one.	
	1 LAN / Ethernet – 10/100/1000 Mbps	
	IP – at least 6 Mbps bandwidth support	
	Security: Password protected system menu	
	ITU-T standards-based Encryption of the video call	
	Camera: Minimum of 12X Optical zoom	
	1920 x 1080 pixels progressive @ 30fps	
	Should have at least 70 degrees field of view (horizontal)	
	The Camera and codec should be from the same manufacturer	
	The end point should support local recording from day 1 through DVR, USB, etc.	
O	MCU	
1.	The Bridging should be running on the standard Intel servers on standard Virtualized platforms. The hardware, software and virtualization software should be supplied and supported by a single bidder	
2.	From day one the bridge must provide 10 full HD video ports @1080p 30 fps and 30 audio conference ports	
3.	All necessary hardware to support the above capacity needs to be supplied from day one. Bridge must have a redundant power supply	
4.	All the 10 ports must be able to connect different sites at different bandwidths and protocols. H.264 AVC standard must be supported at the minimum to connect all the 10 sites.	
5.	The bridge should support room-based video end points, users joining from browsers' supporting WebRTC and HTML5 and its own clients. In case additional components are required for this functionality, all additional components required to have this functionality has to be included in the solution	
6.	The bridge should have the capability to host meetings with internal and external participants in a secure way such that it should co-exist with the enterprise security policies	
7.	The bridge should have components such as the Web Server for Web RTC, Scheduler as part of the offering from day one.	
8.	Should support H.263, H.263+, H.263++, H.264, WebRTC video algorithms	
9.	Should support video resolution from SD to Full HD to join into a conference	
10.	Along with the Support for basic algorithms like G.711 and G.722.1 the bridge should also support wideband Audio protocols like MPEG 4 AAC – LC / MPEG 4 AAC – LD	
11.	Must support the ability to allow Video conferencing devices, Clients on Mobile phones, Smart phones and Laptops to join into conference. These clients can be inside the WAN network or even on the Internet without a VPN.	



12.	The bridge should support transcoding of different Audio/video Protocols.	
13.	The bridge should have H.239/BFCP protocol for sending and receiving dual video streams (Presenter + Presentation).	
14.	The bridge must also support advanced continuous presence such that the site that is “on-air” to be seen on a larger window and the other sites are seen in smaller quadrants	
15.	The bridge must be a secure Non-PC Hardware with a strong operating system. The Hardware and software must be from the same OEM	
16.	The bridge should support 128 Bit strong AES encryption for calls and H.235/SHA1 for authentication	
17.	It should be possible for outside agencies (for state government, central government, police department, etc.) to join the bridge for multi-party video conference call securely over internet	
18.	They should be able to join the bridge using standards-based VC endpoints using internet (as long as these endpoints are exposed to internet) securely.	
19.	It should be possible to connect 5 such external endpoints / locations concurrently at any given point of time.	
20.	It should use secure firewall traversal technology.	
21.	It should support any standards-compliant SIP or H.323 video conferencing endpoints	
22.	It should support for H.323 SIP Interworking Encryption and H.323 SIP Interworking Duo Video	
23.	It should use standards-based firewall traversal methods – H.460.18/19	
24.	The MCU should support viewing of minimum 25 parties in continuous presence mode.	
25.	There should be seamless integration between Video IP phone and Video End point for point to point and multipoint conferences. For this both the components should be from the same OEM	
26.	MCU should support 50 software licenses to be deployed on iOS or on android from day 1	
P	Installation, Configuration etc. and overall management of all associated infrastructure under the responsibility of MSI	



Network Operation Center (NoC)

i. Workstation with single Monitor 24" for Management

Workstation:			
Sr. No	Parameter	Specifications	Compliance (Yes/No) with comments, if any
	Form Factor	Tower/ Rack	
1.	Processor	Intel Xeon Processor, 8 Cores, 16 MB Cache, 3.8Ghz base frequency, 4.7 Ghz Turbo frequency or higher processor	
2.	Operating System	Windows 10 Pro, 64bit or latest	
3.	Office	Microsoft office standard edition latest.	
4.	Chipset	Intel Workstation Chipset 400 Series or latest	
5.	Memory	32GB in combination of (4x8GB) DDR4 2666MHz Memory or higher	
6.	Hard Drive	1 TB SATA HDD	
7.	Graphic Card	Nvidia Quadro P2200 GPU or higher	
8.	Keyboard & Mouse	Wired Keyboard & Mouse (Same make as PC)	
9.	Monitor	Should be able to support min 3x 24" Full HD Monitor (min 23.8" diagonal screen size). Monitor should be of same make as of workstation.	
10.	PSU	80PLUS Gold Certified Energy Star Compliant	
11.	Expansion Slots	Minimum "1" PCIe x16 Gen3; "2" PCIe x4/x8 Gen3 and "1" M.2 or more	
12.	Network Card	Dual Intel Ethernet Connection 10/100/1000 or better	
13.	I/O	4 – USB 3.1 1 – USB 3.1 Type C 1 – Audio Jack/ Microphone & Headphone 4 – DisplayPort 2 – RJ45 Network Connector	
14.	Warranty	As mentioned in RFP.	
Monitor			
1.	Size	23.8"/ 24" LED Monitor	



2.	Resolution	1920 X 1080 resolution Anti-glare, IPS, 16.7 Million colors	
3.	Aspect Ratio	16:9 Aspect Ratio,	
4.	Brightness	250 cd/m ² Brightness,	
5.	Mount	Tilt and Height-adjustable stand, pivot (rotation),	
6.	Ports	1 x DisplayPort, 1 x HDMI, 1 x VGA, 5 x USB, 72% color gamut,	
7.	Certification	TCO Certified	
8.	Prerequisite	Should be of the same make as of the workstation	
9.	Warranty	As mentioned in RFP.	

j. Layer 2 Network Switch 24 Ports

S.No.	Specification	Compliance (Yes/ No) with comments, if any
1	Should have required accessories for mounting.	
2	Should have 24 x 10/100/1000 Base-T ports & 2xSFP+ ports. 2x single mode 1GbE transceivers to be provided in switch	
3	Should have min. 190Watt PoE budget. Stacking cables to be included in each switch.	
4	Should have non-blocking switch fabric	
5	Should have minimum 16000 MAC addresses, minimum 500 VLANs.	
6	Should have 1GB Flash & 1GB CPU memory	
7	Should support 64 LAG, load balancing, double VLAN tagging.	
8	Should have dual firmware images on board. USB port for easy config & firmware image upload	
9	Should support Time Based ACLs, MAC based ACLs from day 1.	
10	Should have Flow based QoS, DiffServ, port based QoS, WRR, strict queue scheduling	
11	Should support UDLD, STP, RSTP, MSTP.	
12	Should support STP, MSTP, minimum 8 hardware queues per port, SP queuing or equivalent, LLDP-MED.	
13	Should have 802.1x, RADIUS, TACACS+, IGMP v1/v2/v3 snooping	
14	Should support SFPs for 10km, 80km distance	
15	Should have Private VLAN & Auto VLAN	
16	Should Support SNMP, RMON, SSH, telnet, web management, network management software.	



17	RSPAN, Private VLAN, captive portal	
18	Power supply/adaptor/cords to be parts of supply	
19	Switch should have min. 130Watt PoE budget	
20	RoHS, Energy Efficient Ethernet, REACH compliance. FCC Class A; NRTL UL; FDA 21 CFR, EN 61000-4-5: Surge	
21	The switch & transceivers should be from the same OEM	

k. IP Phone

S. No	Parameter	Specification	Compliance (Yes/No) with comments, if any
1.	Protocols/Standards	SIP RFC3261, TCP/IP/UDP, RTP/RTCP, HTTP/HTTPS, ARP, ICMP, DNS (A record, SRV, NAPTR), DHCP, PPPoE, TELNET, TFTP, NTP, STUN, SIMPLE, LLDP, LDAP, TR-069, 802.1x, TLS, SRTP, IPV6	
2.	Network Interfaces	Dual switched auto-sensing 10/100/1000 Mbps Gigabit Ethernet ports with integrated PoE	
3.	Graphic Display	Min 2.5-inch	
4.	Bluetooth	Yes, integrated	
5.	Feature Keys	8-line keys with up to 4 SIP accounts	
6.	Video Codec	Support for G.729A/B, G.711μ/a-law, G.726, G.722(wide-band), in-band and out-of-band DTMF (in audio, RFC2833, SIP INFO)	
7.	Auxiliary Ports	RJ9 headset jack	
8.	Telephony Features	Hold, transfer, forward, 4-way conference, call park, call pickup, shared-call appearance /bridged-line-appearance, downloadable phonebook, call waiting, call log XML	
9.	HD audio	Yes, HD handset and speakerphone with support for wideband audio	
10.	Language Support	English	
11.	Upgrade/Provisioning	Firmware upgrade via TFTP / HTTP / HTTPS, mass provisioning using TR-069 or AES encrypted XML configuration file	
12.	Power	Input:100-240V; Output: +12V, 0.5A	



		Integrated Power-over-Ethernet (802.3af) Max power consumption: 6.4W (power adapter) or 6.49W (PoE)	
13.	Security	QoS Layer 2 QoS (802.1Q, 802.1P) and Layer 3 (ToS, DiffServ, MPLS) QoS User and administrator level passwords, 256-bit AES encrypted configuration file, SRTP, TLS, 802.1x or better	
14.	Compliance	FCC: Part 15 (CFR 47) Class B CE: EN55022 Class B; EN55024 Class B; EN61000-3-2; EN61000-3-3; EN60950-1 RCM: AS/ACIF S004; AS/NZS CISPR22/24; AS/NZS 60950.1or Equivalent Indian Standards	

I. SMS Gateway

S No.	Parameter	Specifications	Compliance (Yes/No) with comments, if any
1.	Processor type:	ARM A53 1.2GHz (quad-core)	
2.	Network interface:	Ethernet 10/100/1000 TX (1xRJ45)	
3.	Internal storage:	4GB eMMC storage	
4.	Other interfaces:	1x HDMI, 2x USB, 4xDI, 4x DO, 1x 1 Wire	
5.	Power consumption:	max 20W	
6.	Noise level:	Fanless	
7.	Built-in 4G modem:	2x RF Bands:	
8.		LTE FDD: 1-5, 7, 8, 12, 13, 17, 20, 25, 26, 28, 29, 30 (Rx only), 66	
9.		LTE TDD: 38, 40, 41	
10.		3G: 1, 2, 4, 5, 8 or better	
11.	SIM card standard:	mini	
12.	Antenna connector:	SMA-J	
13.	External Antenna:	2x Omnidirectional 2Bi antenna with magnetic foot Cable length 3m	
14.	Temp & Humidity sensor:	Accuracy ± 0.5 °C, ± 2 %RH	
15.	Power supply:	Voltage ranges: 100–240 V AC Frequency: 50–60Hz	
16.	Approvals:	CE, FCC, IC, GCF (for RF-module), PTCRB (for RF-module), RCM (for RF-module)	



17.	LTE standard:	Cat. 11: max 600Mbps download/ 75Mbps upload (disabled/enabled)	
18.	SENDING/RECEIVING THROUGHPUT	- incoming transmission rate: up to 60 SMS/min - outgoing transmission rate: up to 60 SMS/min	
19.	SOFTWARE PLATFORM		
20.	operating System:	Linux/Windows	
21.		built-in Apache2 web server - built-in PostgreSQL database server - built-in Postfix server - built-in SNMP agent - responsive web interface - watchdog mechanism for 4G modem - failover mechanism support (HA cluster)	

m. Laptop

S No.	Item	Laptop	Compliance (Yes/No) with comments, if any
1	Processor	6 th Generation Intel® Core i7 processor 6600U Up to 3.4 GHZ 4 MB Smart Cache with Integrated 2GB Graphics or better	
2	Chipset	Integrated with processor	
3	Memory	8 GB DIMM DDR4 2133MHz; 2 slots supporting up to 16GB	
4	Display	14-inch Non-Touch HD (1366x768) Anti-Glare LCD with Front camera	
5	Optical drive	NO DVD R/W	
6	Hard disk drive	1 TB Serial ATA Hard Drive	
7	Graphics	Integrated 2GB Graphics	
8	Accessory	Power Adaptor, Laptop Bag, Power Cord (India),	
9	Digital media reader	SD, SDHC, SDXC	
10	Battery	Up to 7 Hours backup.	
11	Connectivity	1 x USB 2.0, 2 x USB 3.0, Bluetooth, Microphone, Wi-Fi integrated adapter, Integrated 10/100/1000 LAN, HDMI	



		port & VGA Port, LAN connectivity – External adapter for connectivity.	
12	Security	TCG Certified/FIPS 140-2 TPM 1.2 (Win 7, 8.1, 10. Field upgradable Spring 2016 to TPM 2.0 with Win10) TCG Certified/FIPS 140-2 TPM 2.0 available Spring 2016 (Win 10 only)	
13	Wireless Mouse	Wireless Mouse from Same OEM	
14	OS	Microsoft Windows 10 Professional 64 bit	
15	office	Microsoft office standard edition latest	
16	Weight	up to 2 kg	
17	Warranty	As mentioned in RFP.	
18	Back-Pack	OEM Original Back-Pack	



Non – IT Components
n. UPS (15 minute backup) - 400 KVA

S. No	Feature	Specification	Compliance (Yes/No) with comments, if any
1	Capacity	400 KVA Online Double Conversion (IT Application) with In-Built Isolation Transformer.	
2	Technology	IGBT (Rectifier & Inverter both); ECO Mode required	
		Continuous duty, three phase, solid state UPS. Each 400KVA UPS should be one single standalone UPS. No Parallel arrangement shall be accepted	
3	Wave form & Freq converter	Pure Sine wave & shall have frequency converter mode	
4	Display	LCD	
5	Input power factor correction	0.99 at 100% Linear load	
6	Input configuration	3Phase, L-N+PE, +/- 10% on full load	
7		UPS Shall have inbuilt Input Dust Filters	
8	Frequency (Input)	40 to 72 Hz frequency	
9	Frequency (output)	50Hz +/- 3%	
10	Output Voltage	380/400/415 Vac shall be available with +/-1% regulation	
11	Output Voltage Distortion	< 1.5% max full linear load	
12	Output Power factor	Unity	
13	Crest factor	3:1 or better	
14	AC-AC Efficiency	Online Mode: Greater than or equal to 95% @ Full Rated Load & Battery Fully charged in load range 30% to 100% load.	
15	Transfer time Main-Battery	0	
16	Transfer time Inverter-Bypass	4 msec	
17	Output Connection	Hardwired	
18	Monitoring software for UPS	Shall be provided for monitoring of UPS from remote along with SNMP Card, this project being of high security & safety the SNMP card shall be in compliance to global cyber security standards i.e UL 2900-1 and IEC 62443-4-2 both as mandatory requirement.	



19	Communication	SNMP for monitoring over LAN	
		&	
		Environment Monitoring Probe for monitoring Temp. & Humidity in UPS room through SNMP Software	
		&	
		Backnet Card for monitoring through Building management system	
20	Port	RS 232	
21	Battery Type	SMF VRLA Lead Acid- Battery with Five years on site warranty	
22	Battery backup	Overall solution design is N+N, Each UPS will be loaded 50% of rated load. Battery Back-up shall be minimum 15 Minutes @0.9 PF for each UPS.	
23	Environmental Parameter		
	Operating temperature range for UPS	0-30 degrees C(KVA=KW)	
	Other	Indication required -> Over Temperature, Load on Battery, Battery low, Mains ON	
	Humidity	5% to 95% no-condensing	
	Noise Level	<75 dBA @ 75% loading	
	Mounting	Tower type	
	EPO	Shall be available	
24	Protection	IP20 with Washable dust filters at Air Inlet Point	
25	LCD Display		
26	Measurements (On LCD)	Input & Output Voltage, Input & Output Frequency, Bypass: Voltage & Frequency, DC Voltage, Remaining time	
27	Manufacturer	Manufacturer -> ISO 9001, ISO 14001, OEM Plant should have water & air pollution control clearance certificate from respective govt. agency.	
		UPS OEM should have registered office in India from last 10 years (certificate of incorporation to be provided)	
28	Product	CE Certified and Made in India	
29	Management Supports /Software	Windows® 2000/ 2003 /XP/Vista/ 2008, Windows® 7 / 8, Linux, Unix	



o. DG Set – 1000 KVA

Sr. no	Feature	Specification	Compliance (Yes/No) with comments, if any
1	General Requirement	The diesel generator set should be of 1000 KVA. The service provider shall be responsible for regular operations and maintenance of the DG set. The service provider shall be responsible for but not limited to: • Fuel • Preventive maintenance • Corrective maintenance • AMC, if any • Replacement of any parts etc.	
		Auto Starting DG Set mounted on a common base frame with AVM (Anti- Vibration) pads, residential silencer with exhaust piping, complete conforming to ISO 8528 specifications and CPCB certified for emissions.	
		b) KVA rating as per the requirement to provide the supply for ICCC and Data Center	
2	Engine	Radiator cooled, multi cylinder, 1500 RPM diesel engine, with electronic/manual governor and electrical starting arrangement complete with battery, conforming to BS 5514/ ISO 3046/ IS 10002 High Speed Diesel (HSD)	
3	Fuel	High Speed Diesel (HSD)	
4	Alternator	Self-exciting, self-regulating type alternator rated at 0.8 PF or better, 415 Volts, 3 Phase, 4 wires, 50 cycles/sec, 1500 RPM, conforming to IS 4722/ BS 5000, Windings of 100% Copper, class H insulation, Protection as per IP 23.	



5	AMF (Auto Main Failure) Panel	AMF Panel fitted inside the enclosure, with the following: It should have the following meters/indicators: Time indication for hours/minutes of operation Fuel Level in fuel tank, low fuel indication Emergency Stop button Auto/Manual/Test selector switch Incoming and outgoing voltage Current in all phases Frequency KVA and power factor	
6	Acoustic Enclosure	The DG set shall be provided with acoustic enclosure / canopy to reduce the sound level and to house the entire DG set (Engine & Alternator set) assembly outside (open-air). The enclosure must be weather resistant powder coated, with insulation designed to meet latest MOEF/CPCB norms for DG sets, capable to withstand climate. The enclosure must have ventilation system, doors for easy access for maintenance, secure locking arrangements etc.	
7	Fuel Tank Capacity	It should be sufficient and suitable for containing fuel for minimum 12 hours continuous operation, Complete with level indicator, fuel inlet and outlet, air vent, drain plug, inlet arrangement for direct filling and set of fuel hoses for inlet and return.	



Civil, Interior, Electrical, Networking, Furniture, Security, NOVEC, FAS, PAC, HVAC etc. for basement and 7th floor + floor strengthening

The details are enclosed in Section 1.5 of Chapter-3 of this RFP

Near Data Recovery Center (nDRC)

- Near DR Center- nDRC will act on active backup arrangement for the DC operations related to critically identified minimum 250 cameras by Delhi Police.
- It will be a down-sized replica of DC which will work in Active-active operations for applications
- DC & nDR Block Diagram:

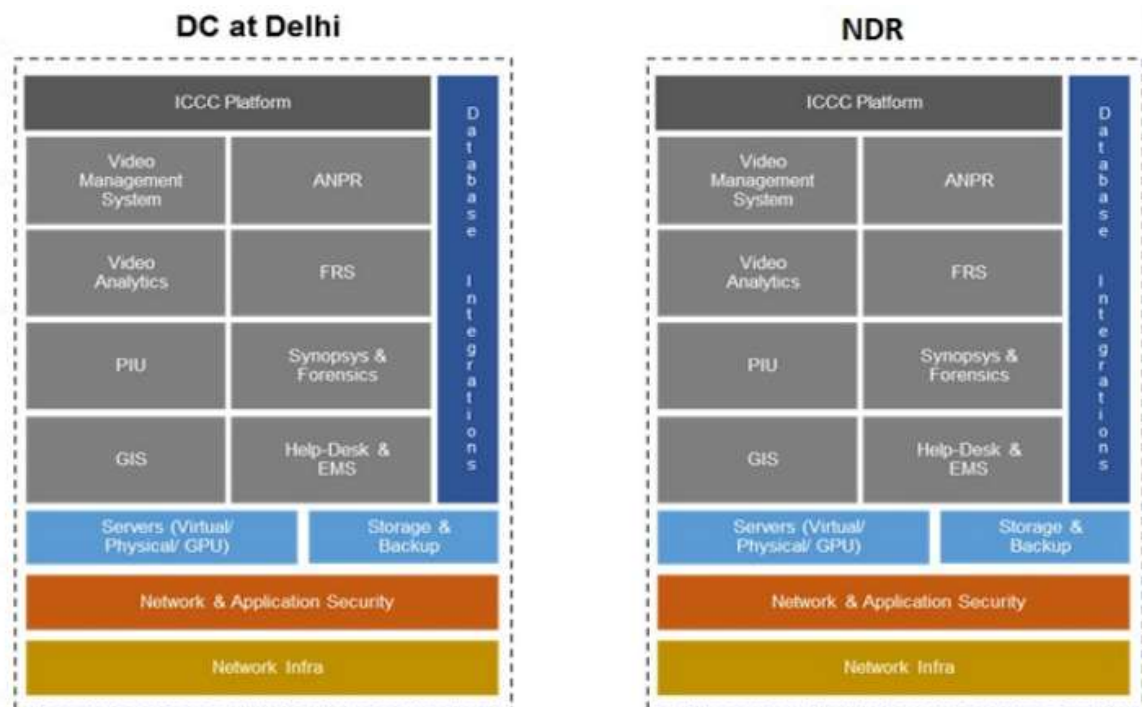
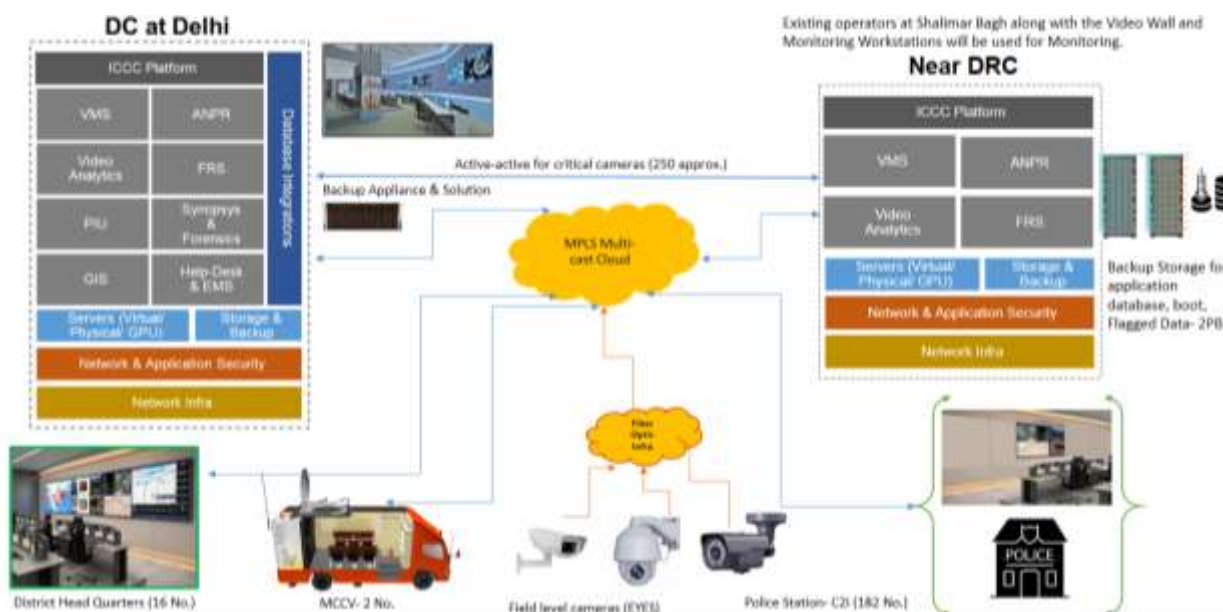


Figure: DC & nDR Block Diagram

d. Near DR Architecture for Delhi Safe City



Near DRC- Technical Requirements and Compliance Sheet for MSI

C4i servers, Video management Servers; Server (Recording); ANPR Servers; Domain Controller; Antivirus Server; LDAP Server

Sr. No	Parameter	Specifications	Compliance (Yes/No) with comments, if any
1.	Make & Model		
2.	Form Factor	1U rack mounted with sliding rails	
3.	Processor	Up to two Intel® Xeon® Scalable 2 nd Gen processors, up to 20 cores/processor @ 2.5 Ghz base freq. or better or equivalent	
4.	Memory slots	16 DDR4 DIMM slots, speed up to 2666MT/s or better	
5.	Memory configured	Minimum 256 GB, scalable to 512GB	
6.	Disks supported	Front drive bays: Up to 10 x 2.5" SAS/SATA (HDD/SSD) with up to 2 NVMe SSD or higher.	
7.	RAID Controller	12Gbps PCIe 3.0 with RAID 1, 5, 10, 50 with 8GB Cache Memory on single / Multiple controllers.	



8.	Disks configured	3x 600GB 15K RPM SAS drives or higher.	
9.	1G Networking features	2 x 1 Gbps Copper Ethernet with Additional Dedicated Mgmt. Ethernet interface port with 3 mts. Length factory crimped copper Ethernet patch cords for each port including 1 mgt. port	
10.	10G Networking features	4 x 10G Copper Ethernet ports with 3 mts. Length 10G factory crimped copper Ethernet patch cords for each port	
11.	FC HBA	Dual port 16 Gbps FC HBA with two no. of each 3 mts. Or 5 mts FC patch cables, Quoted HBA should support quoted SAN Switch and Storage	
12.	Certified for OS	Windows Server 2016 or higher, VMWare vSphere, vCenter, Red Hat Enterprise Linux, SUSE Linux Enterprise Server	
13.	Power Supply	Platinum rated redundant Power Supply	
14.	Management integration	Support for integration with Microsoft System Center, VMware vCenter, BMC Software	
15.	Power & temperature	Real-time power meter, thresholds, alerts & capping with historical power counters. Temperature monitoring	
16.	Pre-failure alert	Should provide predictive failure monitoring & proactive alerts of actual or impending component failure for fan, power supply, memory, CPU, RAID, NIC, HDD	
17.	Configuration Management &	- Real-time out-of-band hardware performance monitoring & alerting - Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management, external storage management, monitoring of FC, HBA & system health if added will be advantage. - Out-of-band hardware & firmware inventory - Zero-touch auto configuration to auto deploy a baseline server configuration profile	
18.	LED/LCD panel	Should display system ID, status information and system error code	



		followed by descriptive text on LED Indicator / LCD Panel.	
19.	HTML5 support	HTML5 support for virtual console & virtual media without using Java or ActiveX plugins	
20.	Server security	Should have a cyber resilient architecture for a hardened server design for protection, detection & recovery from cyber attacks	
		Should protect against firmware which executes before the OS boots	
		Should provide effective protection, reliable detection & rapid recovery using: - Signed firmware updates - Support for Hardware root of trust / Silicon based hardware root of trust - Secure default passwords - Configuration and firmware drift detection - Secure alerting - Rapid OS recovery	
		Configuration upgrades should be only with cryptographically signed firmware and software	
		Should provide system lockdown feature to prevent change (or “drift”) in system firmware image(s) & prevent malicious modification of server firmware	
21.	Warranty	As mentioned in RFP.	



Viewing Centre Management Server

Sr. No	Parameter	Specifications	Compliance (Yes/No) with comments, if any
1.	Make & Model		
2.	Form Factor	1U rack mounted with sliding rails	
3.	Processor	Up to two Intel® Xeon® Scalable 2nd Gen processors, up to 20 cores/processor @ 2.5 Ghz base freq. or better or equivalent	
4.	Memory slots	16 DDR4 DIMM slots, speed up to 2666MT/s or better	
5.	Memory configured	Minimum 128 GB, scalable to 512GB	
6.	Disks supported	Front drive bays: Up to 10 x 2.5" SAS/SATA (HDD/SSD) with up to 2 NVMe SSD or higher.	
7.	RAID Controller	12Gbps PCIe 3.0 with RAID 1, 5, 10, 50 with 8 GB Cache Memory on single / Multiple controllers.	
8.	Disks configured	3x 600GB 15K RPM SAS drives or higher.	
9.	1G Networking features	2 x 1 Gbps Copper Ethernet with Additional Dedicated Mgmt. Ethernet interface port with 3 mts. Length factory crimped copper Ethernet patch cords for each port including 1 mgt. port	
10.	10G Networking features	4 x 10G Copper Ethernet ports with 3 mts. Length 10G factory crimped copper Ethernet patch cords for each port	
11.	FC HBA	Dual port 16 Gbps FC HBA with two no. of each 3 mts. Or 5 mts FC patch cables, Quoted HBA should support quoted SAN Switch and Storage	
12.	Certified for OS	Windows Server 2016 or higher, VMWare vSphere, vCenter, Red Hat Enterprise Linux, SUSE Linux Enterprise Server	
13.	Power Supply	Platinum rated redundant Power Supply	
14.	Management integration	Support for integration with Microsoft System Center, VMware vCenter, BMC Software	
15.	Power & temperature	Real-time power meter, thresholds, alerts & capping with historical power counters. Temperature monitoring	



16.	Pre-failure alert	Should provide predictive failure monitoring & proactive alerts of actual or impending component failure for fan, power supply, memory, CPU, RAID, NIC, HDD	
17.	Configuration Management &	• Real-time out-of-band hardware performance monitoring & alerting • Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management, external storage management, monitoring of FC, HBA & system health if added will be advantage. • Out-of-band hardware & firmware inventory • Zero-touch auto configuration to auto deploy a baseline server configuration profile	
18.	LED/LCD panel	Should display system ID, status information and system error code followed by descriptive text on LED Indicator / LCD Panel.	
19.	HTML5 support	HTML5 support for virtual console & virtual media without using Java or ActiveX plugins	
20.	Server security	Should have a cyber resilient architecture for a hardened server design for protection, detection & recovery from cyber attacks	
		Should protect against firmware which executes before the OS boots	
		Should provide effective protection, reliable detection & rapid recovery using: - Signed firmware updates - Support for Hardware root of trust / Silicon based hardware root of trust - Secure default passwords - Configuration and firmware drift detection - Secure alerting - Rapid OS recovery	
		Configuration upgrades should be only with cryptographically signed firmware and software	



		Should provide system lockdown feature to prevent change (or “drift”) in system firmware image(s) & prevent malicious modification of server firmware	
21.	Warranty	As mentioned in RFP.	

Video Analytics Servers with 3x GPU in each server

Sr. No	Parameter	Specifications	Compliance (Yes/No) with comments, if any
1.	Make & Model	-----	
2.	Rack Height	2U rack mounted with sliding rails	
3.	Processors	Up to two Intel® Xeon® Scalable 2nd Gen processors, configured with 20 cores/processor @ 2.5 Ghz base freq. or better or equivalent	
4.	Memory	128 GB RAM 2666 MT/s support up to 512GB RAM, should have min. 24 DIMM slots	
5.	Hard Drives	5x 600GB 15K RPM SAS drives should be configured. Should support up to eight hard disk drives (SAS, SATA, SSD)	
6.	GPU Configured	Should be configured with 3 nos. of Nvidia Tesla T4 GPU	
7.	GPU Support	Should support upto 6 single wide GPU's	
8.	RAID Controller	12Gbps PCIe 3.0 with RAID 1, 5, 10, 50 with 8 GB Cache Memory on single / Multiple controllers	
9.	1G Networking features	2 x 1 Gbps Copper Ethernet with Additional Dedicated Mgmt. Ethernet interface port with 3 mts. Length factory crimped copper Ethernet patch cords for each port including 1 mgt. port	
10.	10G Networking features	4 x 10G Copper Ethernet ports with 3 mts. Length 10G factory crimped copper Ethernet patch cords for each port	
11.	Redundant Power Supply	Dual, Hot-plug, Redundant Power Supply	
12.	Management integration	Support for integration with Microsoft System Center, VMware vCenter, BMC Software	



13.	Power & temperature	Real-time power meter, thresholds, alerts & capping with historical power counters. Temperature monitoring.	
14.	Pre-failure alert	Should provide predictive failure monitoring & proactive alerts of actual or impending component failure for fan, power supply, memory, CPU, RAID, NIC, HDD	
15.	Configuration Management &	• Real-time out-of-band hardware performance monitoring & alerting • Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management, external storage management, monitoring of FC, HBA & system health if added will be advantage. • Out-of-band hardware & firmware inventory • Zero-touch auto configuration to auto deploy a baseline server configuration profile	
16.	LED/LCD panel	Should display system ID, status information and system error code followed by descriptive text on LED Indicator / LCD Panel.	
17.	HTML5 support	HTML5 support for virtual console & virtual media without using Java or ActiveX plugins	
		Should have a cyber resilient architecture for a hardened server design for protection, detection & recovery from cyber attacks	
		Should protect against firmware which executes before the OS boots	
		Should provide effective protection, reliable detection & rapid recovery using: - Signed firmware updates - Support for Hardware root of trust / Silicon based hardware root of trust - Secure default passwords - Configuration and firmware drift detection - Persistent event logging including user activity	



		- Secure alerting	
		- Rapid OS recovery	
		Configuration upgrades should be only with cryptographically signed firmware and software	
		Should provide system lockdown feature to prevent change (or “drift”) in system firmware image(s) & prevent malicious modification of server firmware.	
		Should maintain repository for firmware and should be able to rollback, if required.	
18.	Certified for OS	Windows Server 2016 or latest, VMWare vSphere & vCenter, Red Hat Enterprise Linux, SUSE Linux Enterprise Server	
19	Warranty	As mentioned in RFP.	



Face Recognition Servers with 3x GPU in each server

Sr. No	Parameter	Specifications	Compliance (Yes/No) with comments, if any
1.	Make & Model		
2.	Rack Height	2U rack mounted with sliding rails	
3.	Processors	Up to two Intel® Xeon® Scalable 2nd Gen processors, configured with 20 cores/processor @ 2.5 Ghz base freq. or better or equivalent	
4.	Memory	128 GB RAM 2666 MT/s support up to 512GB RAM, should have min. 24 DIMM slots	
5.	Hard Drives	5x 600GB 15K RPM SAS drives should be configured. Should support up to eight hard disk drives (SAS, SATA, SSD)	
6.	GPU Configured	Should be configured with 3 nos. of Nvidia Tesla T4 GPU	
7.	GPU Support	Should support upto 6 single wide GPU's	
8.	RAID Controller	12Gbps PCIe 3.0 with RAID 1, 5, 10, 50 with 8 GB Cache Memory on single / Multiple controllers	
9.	1G Networking features	2 x 1 Gbps Copper Ethernet with Additional Dedicated Mgmt. Ethernet interface port with 3 mts. Length factory crimped copper Ethernet patch cords for each port including 1 mgmt. port	
10.	10G Networking features	4 x 10G Copper Ethernet ports with 3 mts. Length 10G factory crimped copper Ethernet patch cords for each port	
11.	Redundant Power Supply	Dual, Hot-plug, Redundant Power Supply	
12.	Management integration	Support for integration with Microsoft System Center, VMware vCenter, BMC Software	
13.	Power & temperature	Real-time power meter, thresholds, alerts & capping with historical power counters. Temperature monitoring.	
14.	Pre-failure alert	Should provide predictive failure monitoring & proactive alerts of actual or impending component failure for fan, power supply, memory, CPU, RAID, NIC, HDD	



15.	Configuration & Management	• Real-time out-of-band hardware performance monitoring & alerting • Agent-free monitoring, driver updates & configuration, power monitoring & capping, RAID management, external storage management, monitoring of FC, HBA & system health if added will be advantage. • Out-of-band hardware & firmware inventory • Zero-touch auto configuration to auto deploy a baseline server configuration profile	
16.	LED/LCD panel	Should display system ID, status information and system error code followed by descriptive text on LED Indicator / LCD Panel.	
17.	HTML5 support	HTML5 support for virtual console & virtual media without using Java or ActiveX plugins	
		Should provide effective protection, reliable detection & rapid recovery using: - Signed firmware updates - Support for Hardware root of trust / Silicon based hardware root of trust - Secure default passwords - Configuration and firmware drift detection - Persistent event logging including user activity - Secure alerting - Rapid OS recovery	
		Configuration upgrades should be only with cryptographically signed firmware and software	
		Should provide system lockdown feature to prevent change (or “drift”) in system firmware image(s) & prevent malicious modification of server firmware.	
		Should maintain repository for firmware and should be able to rollback, if required.	
18.	Certified for OS	Windows Server 2016 or latest, VMWare vSphere & vCenter, Red Hat Enterprise Linux, SUSE Linux Enterprise Server	
19.	Warranty	As mentioned in RFP.	

Storage of application and tagged data (2 PB storage)- SAN/ Unified



Sr. No	Item	Description of Requirement	Compliance (Yes/No) with comments, if any
1.	Market Recognition / Credibility	The OEM Should be present in Gartner Leader Quadrant for General Purpose Disk Array Report Consecutively in last 5 years report will be added advantage.	
2.	Purpose and compatibility	This dedicated storage section will serve the purpose of DMZ which will be from the same OEM of the storage (20PiB) above mention box in order to ensure better back lane throughput and compatibility of controllers.	
3.	SAN / Unified Storage Architecture	Hybrid storage system with Storage Operating System optimized for end to end to handle different types of drives like SSD, SAS & NL-SAS technology with built in QoS (Quality of Services) for optimal utilization of resources across the array. The storage should also support automated data tiering between these 3 types of drives.	
4.		Dual active-active controllers each populated with dual socket of intel® Xeon® Processor.	
5.	Scalability	Offered storage should support scale up for future capacity and performance enhancements	
6.	Data Efficiency Features	Deduplication and Compression functionalities should be supplied and supported on complete capacity with all required licenses. Admin should be able to enable/disable reduction for individual volumes/application	
7.	Controller Scalability	Support for scalability to additional controller pairs (up to 6 pairs or better) to enhance capacity and performance when needed	
8.	Encryption	Option should be available to support FIPS 140-2 certified self-encrypting drives (SEDs).	
9.	Drive Scalability	Minimum 500 disk drives should be supported within the proposed Controller Pair and Offered storage shall be scalable to 1000 Drives or above in cluster/federation of arrays.	



10.		The system should allow dynamic expansion of volumes / pools without any application downtime.	
11.		The system should be powerful enough to support capacity scalability up to 8PB RAW capacity by adding disks in cluster	
12.	Cache	Minimum 256GB DRAM cache across dual controllers, Scalable to 1TB or more either by adding memory into existing controllers or by Adding controllers in cluster/federation of arrays.	
13.	Ports	Minimum 16 x 32 Gbps Frontend FC Ports across the proposed controllers and should be scalable up to 24 Nos of FC Ports or higher. Should also be configured with 8 x 10Gbps SFP+ iSCSI Ports. The back-end of the array must be 8 x 12 Gbps or higher SAS ports per array. It should also support configuring native 10Gbps ports for storage-based replication.	
14.	Capacity	The storage must be supplied with 2000TB Usable Capacity in below configuration:	
15.		400TB Usable Capacity using SSD Drives on RAID5/RAID6	
16.		1600TB Usable Capacity using minimum 7.2K rpm NL-SAS Drives on RAID6	
17.		1 Hot spare for every 30 Drives should be configured.	
18.	Performance	The array should be configured to deliver minimum of 70,000 IOPS with 64KB block size & 50:50 read: write ratio. The storage system should be scalable to more than 1,00,000 IOPS by adding more controllers in cluster/federation mode.	
19.	Data Protection Features	The array should natively be thin provisioned with built-in space efficient snapshots, clones for optimal utilization and performance of the array	
20.	RAID Support	The storage should support industry standard RAID levels like RAID 0, 1, 5, 6, RAID 10 or better; The storage should support combination in a single array.	



21.	Remote Replication Features	The System must be supported and supplied with Replication license for synchronous and Asynchronous replication using FC or iSCSI. The Solution must offer storage-based replication for 1:1, 1: many and many:1 from day 1. The storage should additionally support feature of creating active-active storage environment across 2 physically separate sites/datacenters.	
22.	Data Security	The LUN security & masking software to be provided and configured to protect LUNs configured to heterogeneous hosts running different OS	
23.	Management	The Array must be supplied with comprehensive GUI based Management software which is HTML5 based along with storage analytics utilities for current and historic data analysis. The Management software should work with Multiple arrays, Multiple sites.	
24.		The storage should have features like remote diagnostics and performance monitoring, automated alerts, reports and notifications.	
25.		The Management software should be with single console-based performance management software to manage & monitor replication, live & historical usage of the array including FE ports, BE ports, controller, disk drives etc.	
26.	OS & other Software Support	The Storage Management Software shall be certified to work with VMware vSphere Metro Storage Cluster, VMware SRM and additional support for Native Files, Block Protocols etc.	
27.		The must be certified to support current versions of OS like Microsoft Windows Server, Red Hat Linux, VMware	
28.	Warranty	As mentioned in RFP.	



L3 Switch 24 Port 10/25 GB

Sr.No.	Technical Specifications of ToR Switch	Compliance (Yes/No) with comments, if any
A	General Features	
1	High Density Wire-speed Layer3 Switch	
2	19" rack mountable – 1RU	
3	Should have high-availability feature for active-active & active-passive operation from day-1	
B	Interfaces	
1	Wire rate 24x 10/25 GbE SFP28 ports and 4x100GbE QSFP28 ports. All ports should be populated with Multi-mode transceivers.	
2	As per solution requirement the switch should support 1G, 10G, 25G, 40G & 100G transceivers from day-1. Bidder need to size the quantities of transceivers accordingly.	
3	1 RJ45 console port, 1 RJ45 management port	
4	USB port for external storage	
5	HA cables to be included as part of solution	
C	Performance	
1	Minimum Switch Fabric Capacity: 2Tbps or better	
2	Latency 900ns	
D	Architecture	
1	Should have redundant hot-swap power supplies & fans	
2	32MB packet buffer memory.	
3	Modular operating system, OpenFlow 1.3	
4	CLI commit, Uplink Failure Detection, BFD, Zero Touch Deployment.	
5	Should support Leaf/Spine fabric architecture using BGP EVPN, VXLAN.	
E	High Availability	
1	VRRP, active-active, active-passive operation	
2	Software upgrades with minimal traffic disruption during the upgrade	
3	LAG load balancing based on L2, Ipv4 or Ipv6 headers	
F	Layer 2 features	
1	128 LAG groups with 16 ports per LAG	
2	128K ARP table, 160K MAC addresses	
3	Port, subnet based 802.1Q VLANs. The switch should support 4000 VLANs	
4	132K MAC addresses	
5	The switch should support IEEE 802.1w RSTP and IEEE 802.1s MSTP	
G	Routing Protocols	
1	BGPv4, OSPF v1/v2/v3, VXLAN routing from Day 1	
2	Ipv6 routing & VRF-Lite feature from day-1	



H	Security Features	
1	Layer 2-4 Access Control Lists	
2	ACLs – port based/VLAN based.	
3	Integrated security features like DHCP relay, Control Plane DoS protection	
4	Streaming Telemetry, Control Plane Services	
5	802.1X Network Security and Authentication	
6	RADIUS, TACACS, sFlow, NTP	
I	Traffic Policing	
1	Ingress/Egress shaping and policies	
2	Filter, mark and limit traffic flows	
3	Minimum 8 hardware queues per port	
4	Policy based traffic classification based on MAC Address, Port, DSCP, IP Address, VLAN	
J	Multicast	
1	H/W based Ipv4 and Ipv6 Multicasting	
2	IGMP v1, v2, v3, IGMP Snooping	
3	Protocol Independent Multicast – Sparse Mode and PIM – SSM	
K	Network Management	
1	Ansible, Puppet, Chef, SaltStack, RESTCONF APIs	
2	Ipv6 Management support telnet, FTP, TACACS, RADIUS, SSH, NTP	
L	IEEE Standards	
1	802.3ae, 802.3x, 802.3z	
2	IEEE 802.3ad LACP, 802.3ab LLDP	
3	IEEE 802.1p CoS Prioritization	
4	802.1Qbb, 802.1Qaz	
M	Power Rating & Certifications	
1	Should operate on AC power ~50Hz. Power consumption should not be more than 460 Watts under full load.	
2	RoHS, Ipv6 ready, FCC CFR 47 Part 15, EN 61000-4-5: Surge	
N	Connectivity required	
1	The switch & transceivers should be from the same OEM	
2	Cables - - ethernet cables to be provided with switch for each port with throughput define.	
3	Seamless Integration: For Seamless Integration and Interoperability all the switches and SFP Modules should be fully compatible for smooth functioning of the system	



L2 Switch 24 Port 1GB

S No.	Features	Description of Specs	Compliance (Yes/ No) with comments, if any
1.	Interface requirements	Minimum of 24 ports 10/100/1000 Base-T and 4x 10G SFP+ ports	
2.		1 x Out of Band IP based management Port, 1 Console Port, USB Port / External Flash	
3.		support stacking for upto 8 switches with minimum 40 Gbps stacking.	
4.		Have Redundant Power Supply support and variable speed fan to adjust to varying weather conditions in campus	
1.	Design & Performance	Each switch should have minimum 128 Gbps or more with non-blocking architecture and Forwarding rate of 95 Mpps	
2.		Should be equipped with minimum 1GB RAM and 1GB flash	
3.		Should have LED indicator for per port status, FAN, PSU and Management Status	
4.		0°C to 45°C operating temperature and 10% to 95% relative humidity	
5.		Hardware and software configuration have for Ipv6 from day one	
1.	Switching / Routing	Should have 16 K MAC Address, 500 active Vlans	
2.		802.1D spanning Tree and PVST+, 802.1w, 802.1s, should have BPDU Guard or equivalent feature on edge port to auto disable port for a configurable time period to if an accidental loop occurs in the network	
3.		Audio Video Bridging to enable reliable, real-time audio/video transmission over Ethernet	
4.		Should support aggregating and load balancing of traffic to two or more peer switches within same VLAN	
5.		Should support MSTP protocol	
6.		Should have Port based VLAN, MAC based VLAN, private vlan and support GVRP	
7.		Should have Local, Remote and multisession port mirroring (minimum 4 session)	
8.		Support Standard based protocols for lossless transport of real time data with dynamic QoS reservation.	



9.		Should have 8 Hardware QOS Queues per port	
10.		Should have traffic rate limiting with Configurable bandwidth granularity of 64 KBps	
11.		Should have Link Layer Discovery Protocol (802.1ab) to allow recognition of third-party network devices and LLDP MED for auto configuration	
12.		Should have MAC address tracking and notification for mac address addition, delete or movement in the Network	
13.		Should support policy-based routing and switching	
14.		Should have basic dynamic routing protocols like RIP, OSPF, PIM, VRRP on day one	
15.		Should have Configurable multicast session limit per port	
1.	Security	Local authentication database for RADIUS Authentication for 802.1x login	
2.		Should have MAC security – Lockdown & Limit and MAC address tracking with syslog & snmp notification	
3.		Should have SSH-2, SCP, SFTP for secure management	
4.		Should have dynamic arp inspection, DHCP snooping, Private VLAN, SYN attack protection, GARP protection	
5.		Should have ASIC based traffic flow analysis based on Netflow/ sFlow/ Ipfix	
6.		Should have minimum 1 K ACL entry support and Time-Based ACL or Port-based ACL	
1.	Management	Should have scheduled archiving / uploading of configuration and system log to a central server	
2.		Should support inbuilt DHCP server and Client for quick configuration of endpoints and switch	
3.		Telnet server, ssh server, Ping and traceroute over Ipv6	
4.		Should have L2 Traceroute, L2 Ping and Multicast Traceroute	
5.		Console and CLI management	
6.		Dual firmware and configuration rollback	
7.		Should be SDN capable with Open stack support and OpenFlow API support, should support IEEE P802.1Qaz	
8.		Should support Energy Efficient Ethernet 802.3az	



1.	Certification	Model should have safety and standards certifications as below:	
		IEC61000-4-6:2008/EN61000-4-6:2009, IEC61000-4-8:2009/EN61000-4-8:2010, EN 55022:2010 Class A, CISPR 22:2008 Class A, CISPR24:2010 Class A, Radiated Immunity 10V/criteria, UL60950-1 2ndEd, CE 2.0 Compliant or equivalent Indian Standards.	
2.		Seamless Integration: For Seamless Integration and Interoperability all the switches and SFP Modules should be fully compatible for smooth functioning of the system	

SAN Switch 12 port

Sr. No	Feature	Technical Specifications	Compliance (Yes/No) with comments, if any
1.	Switch Architecture	The proposed SAN Switches should have 1U form factor with minimum 24 Nos. of 32Gbps Ports or higher. Should have redundant power supplies and fans.	
2.	Fiber Channel Ports	Should be configured with 24 x 32Gbps FC Ports or higher on day one	
3.	Autosensing capabilities	The proposed ports should have autosensing capabilities to 32/16/8 Gbps FC connectivity	
4.	Trunking capabilities	The switch should support trunking with up to eight 32 Gbps ports per ISL trunk	
5.	Performance	Should support aggregate bandwidth of 768Gbps or higher	
6.	Port Types supported	Should support D_PORT (Clear Link Diagnostic Port), E_PORT, EX_PORT, F_PORT, AE_PORT	
7.	Media/Transceiver Types	Should support hot-pluggable Fiber Channel SFP+ at 32 Gbps SWL/LWL and SFP+ at 16 Gbps SWL/LWL/ELWL	
8.	USB Port	Should have at least One USB port per control processor for firmware download, support save, and configuration upload or download	



9.	Management	Should have switch management feature with support for e HTTP, SNMP v1/v3 (FE MIB, FC Management MIB), SSH; Auditing, Syslog; Command Line Interface (CLI); SMI-S compliant	
10.	Security	Should support DH-CHAP (between switches and end devices), FCAP switch authentication; HTTPS, Ipsec, IP filtering, LDAP with Ipv6, OpenLDAP, Port Binding, RADIUS, TACACS+, user-defined Role-Based Access Control (RBAC), Secure Copy (SCP), Secure RPC, Secure Syslog, SFTP, SSH v2, SSL, Switch Binding, Trusted Switch. Should also support up to 12 in-flight encryption and compression ports.	
11.	Cables	Fc cables can be provided along with SAN switches with different lengths to cater server connectivity. Or if provided along with the server	
12.	Warranty	As mentioned in RFP.	

Rack

Sr No	Specification	Minimum Requirement	Compliance (Yes/No) with comments, if any
1.	General	42 U X 600mm X 1200mm (H x W x D) rack should have metal frame supporting more than 1300 kgs of static load and more than 1000 kg of dynamic load.	
2.		Single front door and split rear door should have the perforation of more than 75% to provide the maximum airflow eliminating the need of additional FHU in the rack.	
3.		Doors shall have lift of hinges for tool less field reversibility.	
4.		Rack should have integrated hole pattern for easy installation of top panel accessories have removable opening for cable entry and shall accommodate 2000 cat 6 cables to suffice the cabling requirements.	
5.		Rack should have two pair of 19-inch EIA mounting rail with U marking on front and rear of each rail for ease of installation.	



6.	Cable Manager	Rack should have dual purpose full height depth adjustable PDU/Cable management brackets and should be mounted in the zero U space.	
7.		PDU/Cable management brackets shall have button mount keyholes throughout to accommodate the tool less mounting of rack PDU's of various heights and accessories mounting holes for toolless cable mounting accessories.	
8.	Panel	Rack should have split side panels with single locking slam latch for quick and easy installation and maintenance, single person removal and installation eliminates the manpower dependencies.	
9.	Caster & Levelling	42 U rack frame height that allows access through standard doors on four swivel casters, rack shall have the levelling feet and shall be accessible form the top of the frame for easy adjustment.	
10.	Hardware Accessories / Installation ease	Rack shall have the necessary hardware accessories ((50 each M6 cage nuts and screws), Cage nut installation tool, edge protection for top panel cable entry.	
11.		Rack shall have necessary baying brackets and the bolt down kits	
12.		Rack frame design should allow 2.5 inch more usable space in the rack for the proper equipment placement and ease of access.	
13.	Powder Coating	Rack should have the powder coated black color.	
14.	Certification	Rack shall have EIA, UL, RoHS, REACH certified	
15.	Power Distribution	Rack shall have two power distribution unit, vertically mounted on the rear of the rack to power on the devices in the rack.	
16.	Power Distribution Unit	Monitored, Unit Level, 32Amps, 230V, 1 Phase, 7.3KW, Vertical, 30 IEC C13, 6 IEC C19, Locking Sockets, 3m power Cord with 2P+E (IP44)	
17.		The PDU shall have locking outlets – cable locking mechanism so that it should not require the locking cable to secure the cables connected to the PDU	



18.		PDU shall have Input and Breaker level current monitoring. Local high visibility LED display.	
19.		PDU shall have Phase (A) Monitoring (kWh, W, VA, PF, V, A) Power Measurements Compliant with ANSI C12.1 and IEC 62053-21 at 1% Accuracy Class Requirements and Circuit / Breaker Monitoring (A)	
20.		Circuit/Breaker Current Measurements Independently Tested and Verified at 2% Accuracy.	
21.		The PDU shall support the mobile app for the power monitoring and should be easy to be shared in various formats	
22.		The PDU shall be upgrade ready so that it can be changed to monitored PDU without downtime, by simply changing the Field replaceable IMD unit.	
23.		PDU shall have button mounting option for easy toolless installation and reinstallation of the PDU's	
24.		PDU shall have colored outlets to differentiate the outlets based on the breakers.	
25.		The PDU should be CE certified.	
26.	Rack	As mentioned in RFP.	



Firewall- 3 Gig, IPS, DDos, Anti- APT, VAPT, server security- 3 GB throughput

Sr. No	Specification	Compliance (Yes/ No) with comments, if any
1	Firewall architecture should be DC grade with Data and control plane are different and should be in the Gartner Challengers/ Leaders from last 5 years and the OEM must have "Recommended" rating with min 97% Evasion proof capability and Security Effectiveness as per 2019 NSS Labs Firewall Comparative Test Report. Will be added advantage.	
2	Firewall appliance should be supplied with at least 4x40GE QSFP, 8x 10GE SFP+, 10x GE RJ45.	
3	SFP Transceivers to be populated as per solution requirement	
4	Firewall should have IPsec VPN throughput of 3 Gbps. The effective next generation firewall throughput should be 3 Gbps in real time/ Enterprise/ Application traffic mix to cater bandwidth requirement of multiple 1 Gig interface so as to ensure IDS for monitoring malicious activity or defined policy violations. It should be scalable to 4.5 Gbps in future. The Firewall must be capable to conduct operations of internal firewall with regards to application and structured data that will be residing in the DMZ.	
	The Threat prevention (FW, IPS, User identification, AVC, Antivirus, logging and Antimalware) throughput should be at least 3 Gbps on Mix / Application Mix Production traffic and should be scalable to 4.5 Gbps.	
5	Firewall should support 100K new sessions per second, from day 1	
6	Firewall should support 3 Million maximum concurrent sessions, from day 1- minimum 2 million sessions.	
7	Firewall should support 1K site-to-site VPN tunnels & 1K Client to Site VPN tunnels	
	The appliance should be secure in itself with certifications NDPP/ EAL4, FIPS/ICSA. Extra certificate will be added advantage like NEBS etc.	
8	The Firewall solution should support LLDP, ECMP, NAT64, and DNS64 & DHCPv6.	
9	The proposed system shall be able to operate on either Transparent (bridge) mode to minimize interruption to existing network infrastructure or NAT/Route mode. Both modes can also be available concurrently using Virtual Contexts. Minimum 1 Virtual Firewall licenses to be provided with the solution and should be scalable to 5 Virtual Firewalls in future	
10	The physical interface shall be capable of link aggregation, otherwise known as the IEEE 802.3ad standard, allows the grouping of	



	interfaces into a larger bandwidth 'trunk'. It also allows for high availability (HA) by automatically redirecting traffic from a failed link in a trunk to the remaining links in that trunk.	
11	High Availability: Active/Active and Active/Passive. The proposed system shall have built-in high availability (HA) features without extra cost/license or hardware component. Firewall should support ether channel or equivalent functionality for the failover control & date interfaces for providing additional level of redundancy.	
12	The proposed system should have integrated Traffic Shaping functionality. The proposed firewall shall have native network traffic classification which identifies applications across all ports irrespective of port/protocol/evasive tactics. The firewall should support QoS and Policy based routing on the basis of application.	
13	The Firewall should have integrated SSL VPN solution to cater to 1000 SSL VPN concurrent users. Tunnels (SSL, IPSec, and XAUTH) – 1K from day 1.	
14	Concurrent SSL Decryption sessions – 250000. This should be substantiated with document from public website or testing/R&D report data. Declaration on letterhead will not be accepted. The proposed firewall shall be able to identify, decrypt and evaluate SSL Tunnel traffic in an inbound and outbound connections	
15	Should support SSL decryption on Ipv6	
16	The proposed system should support	
	a) IPSEC VPN	
	b) PPTP Pass through or VXLAN inspection	
	c) L2TP VPN or GRE Tunnel and inspection of headers with 802.1Q SGT	
	d) SSL VPN	
17	The device support inbuilt hardware VPN acceleration	
18	The device shall support stateful session maintenance in the event of a fail-over to a standby unit.	
19	The management solution must have the native capability to optimize the security rule base and offer steps to create application-based rules	
20	The proposed solution must allow single policy rule creation for application control, user-based control, host profile, threat prevention, Anti-virus, file filtering, content filtering, QoS and scheduling at single place within a single rule and not at multiple locations. There must not be different places and options to define policy rules based on these parameters.	
21	Should have separate real time logging base on all Traffic, Threats, User IDs, URL filtering, Data filtering, Content filtering, unknown malware analysis, Authentication, Tunneled Traffic and correlated log view base on other logging activities	



22	Should support the report generation on a manual or schedule (Daily, Weekly, Monthly, etc.) basis, also should allow the report to be exported into other format such as PDF, HTML, CSV, XML etc.	
23	Should have built in report templates base on Applications, Users, Threats, Traffic and URLs and should create reports based on user activity	
24	Should be able to create custom report base on custom query base any logging attributes	
25	On device management service should be able to provide all the mentioned features in case of central management server failure	
26	Firewall should provide application detection and authentication for DNS, FTP, HTTP, SMTP, ESMTP,	
27	LDAP, MGCP, RTSP, SIP, SCCP, SQLNET, TFTP, H.323, SNMP	
28	The proposed solution should support the ability to create QoS policy on a per rule basis:	
	-by source address	
	-by destination address	
	-by application	
	-by static or dynamic application groups (such as Instant Messaging or P2P groups)	
	-by port and services	
	The proposed system shall have the ability to detect, log and take action against network traffic based on over 3000 application signatures	
29	Firewall should support operating in routed & transparent mode	
30	The proposed firewall must support the following routing protocols: - Static, RIP v2, OSPFv2/v3, Application based PBR, BGP v4 with graceful restart	
31	Firewall appliance should have integrated redundant hot swappable power supply and hot swappable fan tray.	
32	Proposed Firewall should not be proprietary ASIC-based in nature & should be open	
33	architecture based on multi-core CPU's to protect & scale against dynamic latest security threats.	
34	Data Leakage Prevention	
A	The proposed system shall allow administrator to prevent sensitive data from leaving the network. Administrator shall be able to define sensitive data patterns, and data matching these patterns that will be blocked and/or logged when passing through the unit.	
35	High Availability	
A	The proposed system shall have built-in high availability (HA) features without extra cost/license or hardware component	
B	The device shall support stateful session maintenance in the event of a fail-over to a standby unit.	



C	High Availability Configurations should support Active/Active and Active/ Passive	
36	Logging & reporting	
37	A dedicated appliance or management software to be proposed with the solution for logging, analysis, and reporting into a single system, delivering increased knowledge of security events throughout the network for centralized security event analysis, forensic research and reporting	
38	Event Management: There has to be a feature of Management Module/ tool to establish link with EMS platform & SIEM.	

Network Load balancer

S No.	Specifications	Compliance (Yes/No) with comments, if any
	Architecture	
1.	The Load Balancer shall distribute traffic efficiently while ensuring high application availability. It shall monitor server health to determine that application servers are not only reachable but alive. If the Load Balancer detects issues, it shall automatically remove downed servers from the server pool and rebalance traffic among the remaining servers. It shall be appliance based and shall facilitate multi-vendor, multi-application environment and shall support third-party products	
2.	The Load Balancer shall deliver the high availability required by modern Data Centers. It should support Active/Passive or Active / Active HA configurations. The Load Balancer shall automatically synchronize configurations between the pair and automatically failover if any fault is detected with the primary unit	
3.	The load balancer shall be built on high-performance hardware, designed for Data Centers. It shall deliver application traffic of all types and scalable to meet the throughput needs of the most demanding applications	
4.	The Load Balancer shall support offloading of SSL connections and should support Certificate format such as "OpenSSL/Apache, *.PEM", "MS IIS, *.PFX", and "Netscape, *.DB" etc. or better.	
5.	Should provide support for cache rules/filters to define granular cache policies based on cache-control headers, host name, file type, max object size, TTL objects etc.	
6.	The Load Balancer Shall have full traffic control and be able to route requests to servers based on region, device, browser, or a number of other factors. This enables organization to deliver customized application responses to users.	



7.	Should be high performance purpose built next generation multi-tenant hardware with NFV and SDN support. Platform should support multiple network functions including Server Load balancing, Application Security, Secure remote access and AAA network functions with dedicated hardware resources for each virtual instance.	
8.	Appliance should provide real time Dynamic Web Content Compression to reduce server load and solution should provide selective compression for Text, HTML, XML, DOC, Java Scripts, CSS, PDF, PPT, and XLS Mime types.	
	Performance	
9.	The server load balancer should deliver 5Gbps L4 Throughput from day one and scalable to 40Gbps on same hardware with license upgrade	
10.	The server load balancer should have dedicated SSL card to support Minimum 28,000 ECC TPS (ECDSA-SHA256) & 40,000 SSL TPS 2K Keys.	
11.	The sever load balancer should support Minimum 128GB RAM, 4TB HDD and should have minimum 4x1GbE copper ports, 4x10GbE SFP+ ports. Two 1G Copper dedicated management interface	
	Features required for Load Balancer	
12.	Local Application Switching, Server load Balancing, HTTP, TCP Multiplexing, Compression, Caching, TCP Optimization, Filter-based Load Balancing, Transparent Deployments, Content-based Load Balancing, Persistency, HTTP Content Modifications, QoS, Support for connection pooling to TCP request, Support for distributed denial-of-service (DDos) protection	
13.	Security features	
14.	Solution should support DDos attacks from day one like Protocol Attack: SSL invalid packet, SSL handshake attack, SSL renegotiation, HTTP invalid packet attack – Application Attacks: HTTP slow attack, HTTP flood attack, long form submission, Challenge Collapsar (CC), Hashdos, DNS NXDomain flood – Network Attacks: SYN flood, ICMP flood, Ping of Death, Smurf, IP option – HTTP & DNS ACL rules, ACL blacklist – Monitoring and Logging: PUSH/ ACK flood, FIN/RST flood, Connection flood, UDP flood – Machine learning of traffic patterns and automatic configuration of HTTP/DNS thresholds to defend against anomalous traffic	
15.	Should support machine authentication based on combination of HDD ID, CPU info and OS related parameters i.e. mac address to provide secure access to Data Center resources.	
16.	Supports SAML secure application access – Supports web single sign-on (SSO) – Serves as a SAML SP (service provider)	
17.	Solution should capable of blocking access through anonymous services (TOR, VPN, open proxies, anonymizers)	



18.	Solution Must Prevents modifying the form data and cookies on the client side by controlling their invariability between the request and the response with Cookie Signing, Form Signing and AJAX requests Signing.	
	Load Balancer Features	
19.	It should have the capability of Rate shaping & QoS Support to optimize and handle heavy Layer 4 through 7 traffic loads while delivering Latency Sensitive Applications	
20.	It should support integrated antivirus module for scanning of malicious content in files uploads and should be able to integrate with the proposed on-premise Anti-APT, SIEM, DLP solution to scan for zero-day malwares from Day 1	
	High Availability	
21.	It should have feature of Global Server Load Balancing between different Data Centers without any additional license, from Day 1.	
22.	The solution should provide comprehensive and reliable support for high availability and N+1 clustering based on stateful session failover with Active-active & active standby unit redundancy mode. Also support Single System Image for Load Balancer Function to create a single VIP (single ADC instance) out of any number of dedicated, virtualized or virtual ADV appliances to provide ultimate flexibility in scaling out.	

Miscellaneous- Virtualization, OS for servers, etc.

Virtualization Physical Servers 12

12 server Virtualization Security

Windows OS -11 Server

- 12 Physical Servers using two sockets in total 24 (12*2) quantity required for virtualization servers
- 12 physical servers using two sockets in total 24 (12*2) quantity required for security of DMZ virtualization servers

Microsoft Windows OS for Virtualization Servers

- 11 Physical Servers each having 4 VM's (Total 44 VM's). For each server we need to consider license for 40+40=80 cores (5 licenses of 16 cores)
- Windows Server Data Center Edition 64-bit latest version

Compute Virtualization			
S No.	Specifications		Compliance (Yes/ No) with comments, if any
1.	Virtualization Solution	Sits directly on the virtualization server hardware with no dependence on a general-purpose OS for greater reliability	



		& security and should be Leaders/challengers in the Gartner's Magic Quadrant latest.	
2.	Guest OS Support	Windows client, Windows Server, Linux (at least Red Hat, SUSE, Ubuntu and CentOS, Solaris x86) etc. OS vendor should provide certification and support for hypervisor.	
3.	Live Migration	Live Virtual Machine migration between different generations of CPUs in the same cluster and without the need for shared storage option and long distances from one site to another with no disruption to users or loss of services, eliminating the need to schedule application downtime or business downtime.	
4.		Live migration of VM disk from one storage array to another without any VM downtime. Support this migration from one storage protocol to another eg: FC, NFS, iSCSI, DAS.	
5.	Availability	Proactive High availability capability that utilizes server health information and migrates VMs from degraded hosts before problem occurs, should optimize power consumption by turning off hosts during the reduced demand	
6.		Migration of VMs in case one server fails all the Virtual machines running on that server shall be able to migrate to another physical server running same virtualization software.	
7.		It should support affinity and anti-affinity rules to set constraints that restrict placement of a virtual machine to a subset of hosts in a cluster and to keep virtual machines paired or separated with capability of native backup and restoration of the virtualization management server.	
8.		Solution should have single reboot to dramatically reduce the upgrade times by skipping a host reset and help to reduce patching and upgrade times by rebooting the hypervisor without rebooting the physical host, skipping time- consuming hardware initialization	
9.		Zero downtime, zero data loss and continuous availability for the applications running in virtual machines in the event of physical host failure, without the cost and complexity of traditional hardware or software clustering solutions.	
10.	Performance	Add CPU, Memory & devices to virtual machines on the fly when needed, without disruption or downtime of working VMs for both windows and Linux based VMs.	
11.		Create a cluster out of multiple storage datastores and automate load balancing by using storage characteristics to determine the best place for a virtual machine's data to	



		reside, both when it is created and when it is used over time.	
12.		Support for persistent memory, exposing it as block storage or as memory, to enhance performance for new as well as existing apps should provide configuration compliance reports/alerts/dashboards for the underlying hypervisor platform	
13.		Should be able to dynamically allocate and balance computing capacity across collections of hardware resources aggregated into one unified resource pool with optional control over movement of virtual machines like restricting VMs to run on selected physical hosts.	
14.		The Solution should offer virtual load balancers with L4-L7 load balancer with SSL offload and pass-through, server health checks	
15.		Should support network and storage QoS to ensure performance on per VM basis	
16.	Security	VM-level encryption with no modifications in guest OS to protects unauthorized data access both at-rest and live vMotion and also provides secure boot for protection for both the hypervisor and guest operating system by ensuring images have not been tampered with and preventing loading of unauthorized components.	
17.		Solution should protect every Virtual Machine with a stateful distributed firewall integrated into the host architecture and provide near line rate firewall throughput.	
18.		Solution should enable creation of security groups and security policies/ rules based on constructs like machine name, OS type, IP address, Logical Switches, Security Tags etc.	
19.		The security policies should follow the Virtual Machines as it moves within and between the virtual infrastructure so that there is no need of creation of security policies again for the applications once they move inside and across the Datacenter.	
20.		Integration of 3rd party endpoint security to secure the virtual machines with offloaded antivirus, antimalware, firewall and hips solutions without the need for agents inside the virtual machines.	
21.		Solution should support TPM 2.0 hardware modules and adds a virtual TPM device to shield guest OS from Operator or in-guest attacks	
22.		The security policies in the virtualization layer must be tied to the application, which means whenever any application	



		is moved from one virtualized server to another, even between different VLANs, the security policies should follow the application and there should be no need to redefine the security policies for the application at the new location. Also, when the application is deleted, all the security policies related to the application should also be removed.	
23.	Storage support	Support boot from iSCSI, Fcoe, and Fibre Channel SAN. Integration with Storage API's providing integration with supported third-party data protection, multi-pathing and disk array solutions. Solution should have capability similar of Virtual Volumes which enables abstraction for external storage (SAN and NAS) devices making them Virtualization aware and it should allow common management across storage tiers and dynamic storage class-of-service automation via a policy-driven control plane	
24.	Management	The solution should offer converged visibility and analytics that tie together compute, network, storage and security and provide Physical to Virtual Correlation and troubleshooting, report the amount of East-West, North-South, Internet, virtual machine to virtual machine, virtual machine to physical traffic within the datacenter Monitoring of OS level resources (CPU, disk, memory, network) for any OS and physical hardware resources of the hosts. These monitoring capabilities combined with patented analytics should extend operational visibility and proactive management capabilities across OS.	
25.		The solution should offer comprehensive flow assessment and analytics and security groups and firewall rules suggestion for the purpose of implementing a zero-trust security within the data-center, provide a converged view of virtual and physical network, provide end to end topological view of path between two virtual machines. It should support leading hardware vendors as well. The solution shall provide the ability to identify and report on over-sized, under-sized, idle and powered-off virtual workloads such that the environment can be right-sized and resources can be reclaimed	
26.	Virtual Switch	Span across a virtual Datacenter and multiple hosts should be able to connect to it. This will simplify and enhance virtual-machine networking in virtualized environments and enables those environments to use third-party distributed virtual switches.	



27.		The solution should be capable to of multisite networking (Layer 2 extension) irrespective of underlying physical topology for active active DC & DR purposes, container network and security for container to container L3 networking and micro segmentation for microservices etc.	
28.		The solution should support reduction in Recovery Time Objective when the VMs are brought up from DC to DR, without the need to redo the IP-addresses, the default gateway router should be stretched across data centers, also the firewall policy should also be applied across DC & DR automatically, so that when Virtual Machines move from DC to DR there is no need to reconfigure the firewall policies	
29.		In-built enhanced host-level packet capture tool which will provide functionalities like span, rspan, erspan and will capture traffic at uplink, virtual switch port and virtual NIC level. It should also be able to capture dropped packets and trace the path of a packet with time stamp details.	
30.		The Solution should provide distributed routing (OSPF & BGP), VXLAN based logical virtual switching, NAT function, server load balancer, Software L2 bridging to physical environments, L2 & L3 VPN, site-to-site IPSEC VPN services, distributed L2-L4 stateful firewall at vNIC level.	
31.	VM based Replication	Efficient array-agnostic replication of virtual machine data over the LAN or WAN. This Replication should simplify management enabling replication at the virtual machine level and enabling RPOs as low as 15 minutes.	
32.	Operations Management	Solution should provide integrated smart alerts for health, performance and capacity degradation to identify building performance problems before they affect end users ,should be able to collect and analyze all types of machine-generated log data, for example, application logs, network traces, configuration files, messages, performance data and system state dumps.	
33.		Solution should provide capacity analytics to identify over-provisioned resources so they can be right-sized for most efficient use of virtualized resources and “What If” scenarios to eliminate the need for spreadsheets, scripts and rules of thumb to provide automated root cause analysis and should allow connecting to data-center ecosystem components e.g., operating systems, applications, storage arrays, firewalls, network devices, etc., providing a single location to collect, store, and analyze logs at scale	



34.		It should include proactive smart alerts with self-learning performance analytics Capabilities with Customizable Dashboards, Reports and Views to provide real-time insight into infrastructure behavior, upcoming problems, and opportunities for efficiency improvements	
35.	Disaster Recovery Automation	Solution should provide DR automation solution delivered from virtualization manager console for automated failover, failback and recovery of application VMs in proper sequence to other data center with single click	
36.		Solution should provide solution to perform non-disruptive DR drill/testing of recovery plan for full and selected applications every six months without impacting production applications running in primary environment.	
37.	OEM Support	Direct OEM L1, L2, L3 24x7x365 days with unlimited incident support and 30mins or less response time including the unlimited upgrades and updates. For 5 years	

4.9 Minimum baseline for security parameters

The minimum baseline of secured environment for the envisaged system will be ensured by protection from external and internal sources with various security tools like External and internal Firewalls, DDos, Anti-APT, IPS, VAPT, Server and Application security measures, etc.

Establishing privacy and trust

Considering the secured parameters in place, it will be the prime responsibility of MSI to establish a trust for privacy policies to be adopted by every user of the system. The security parameters will be updated from time to time with effective patch management modules and training sessions will also sensitize the users for quick adoption of the updated approaches in the system to ensure safeguarding against possible threats.

Cyber Security Components in Command Center / DC & Near DRC

i. Firewall:

Firewall solution is first line of Defense and segmentation. The firewall protection for Safe City Project will be combination of traditional firewall with other Network Device filtering functionalities for the Incident, transaction data, data over HTTP, only. The appliance-based security platform should be capable of application visibility, and control, VPN functionality, intrusion preventions and advanced threat protection like deep packet inspection, etc. in a single appliance. This appliance should ideally consume 1 RU/2 RU space to utilize space in command center optimally.

- a. For better integration with other security solutions this should be based on open architecture based on multi-core CPU's to protect & scale against dynamic latest security threats.



- b. Supports multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).
- c. Denial of Service Attack (DDos) solution should be part of this FW, and DDos throughput shall be clearly mentioned in this.

ii. Internal & External Firewall with IDS and Intrusion Prevention Detection (IPD):

Firewall solution is first line of Defense and segmentation. The firewall protection of Enterprise grade for Safe City Project will be combination of traditional firewall with support of other Network Device filtering functionalities for the Incident, transaction data, data over HTTP, only.

- For better integration with other security solutions this should be based on open architecture based on multi-core CPU's to protect & scale against dynamic latest security threats.
- Supports multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).

The solution architecture at Data Center will incorporate both type of firewalls for protection against the internal and external threats. Using Firewalls and Intrusion Prevention Systems such attacks and theft should be controlled and well supported (and implemented) with the security policy. All provisions for security of field equipment as well as protection of the software system from hackers and other threats needs to be ensured. Web Application (Internet) Firewall of 2 GB will be provisioned which will cater to the DMZ security requirement at virtualization layer at the server levels.

- **External Firewall:** Unauthorized access has to be blocked; henceforth adequate capacity throughput requirement has to be handled by the external firewall to safeguard the North-South information flow with unauthorized accessibility. It will ensure a seamless throughput of SSL encrypted application and structured data.

The perimeter firewall of adequate 50 Gig throughput for passing the video feeds necessarily required for VA platform. It will be required to manage the secured sessions. The effective bandwidth requirement will be 100 Gig so as to ensure IDS for monitoring malicious activity or defined policy violations. Also, considering the capability of this aggregation firewall which will primarily handle North-West consolidated data flow, it can also be configured along with East-West firewall operations pertaining to the requirement for incidental data for DMZ.

- **Internal Firewall:** The second layer of protection of unauthorized access will be ensured by internal firewall to handle East-West traffic flow within Data Center. The internal firewall must proactively provide visibility and protection from internal threats, and it must be fast enough to keep up with the demands of internal traffic. It must ensure:
 - i. Minimizing the attack surface using micro-segmentation, which divides the network into granular zones that are secured separately
 - ii. Using intelligent automation to deploy and update security policies based on audit logs.



iii. Intrusion Prevention Detection System & VAPT

The IPS solution can be a purpose-built dedicated appliance or a subset of firewall

The IPS must be able to support granular security policy enforcement based on the following methods: Per IPS device (all segments), Per physical segment unidirectional and bidirectional.

The IPS filter must support network action set such as Block (drop packet), Block (TCP Reset), Permit, Trust, Notify, Trace (Packet Capture), Rate Limit and Quarantine & proposed IPS solution must support signatures, protocol anomaly, vulnerabilities and traffic anomaly filtering methods to detect attacks and malicious traffic & should support VA scanners to fine tune the IPS policy

The centralized management server must be an appliance based on a hardened OS shipped by-default and system shall allow the latest update to be manually, automatically or based on schedule with central management and reporting.

IPS with a throughput capacity to conduct its operation for entire stack of input feeds from cameras to be ascertained for identifying intrusion checks, session breaks, VAPT profiling for a better matured security, etc.

Vulnerability Assessment and Penetrating Testing (VAPT) must ensure series of tests on the system architectural associated IP devices throughout the network. Continual security assessments should be conducted so that the vulnerable areas are exposed and quantification and the prioritization of such instances can be done. VAPT will behave as a risk assessment tool which will ensure the following steps:

- Cataloguing assets and capabilities (resources) in a system
- Assigning a quantifiable value (or at least rank order) and importance to those resources
- Identifying the vulnerabilities or potential threats to each resource
- Mitigating or eliminating the most serious vulnerabilities for the most valuable resources

iv. Web Application Firewall:

The solution shall have web application firewall (or WAF) functionality to filter, monitor, and block HTTP traffic to and from a web application. Such data relates to the feeds and inputs coming from internet based sources which covers the inter-operability with other applications (external), communication to MCCV, Public Address Systems, Prakhar Vans, etc.

WAF shall be able to filter the content of specific web applications. By inspecting HTTP traffic, it shall prevent attacks stemming from web application security flaws, such as SQL injection, cross-site scripting (XSS), file inclusion, and security misconfigurations.

Web Application firewall is essentially required to safeguard the DMZ from threats originating through the internet exposure due to mobile interfaces and the integration of the system with other (external) data sets.



v. Other Essential security parameters

a) Anti-Virus

Anti-Virus for End Point Security (desktop & mobile users (controlling end users (clients) at C3i and C2i also through central manager)- all desktop workstations, mobile devices, etc.

E-mail is most preferred threat vector for attackers and safe city must have robust and reliable solution in place to protect their e-mail users. Solution must:

- i. Inspect all incoming and outgoing emails, and detect and protect against Spam, spoofing, virus, malware, including scanning of different file attachment types like doc, xml, txt, ods, ppt, zip etc. including compressed files.
- ii. Support for scanning of password protected files/ attachments and provide sandboxing capabilities for suspicious files.
- iii. Support for Data Loss Prevention and have the capability to define rules to protect crucial data of the organization.
- iv. Support for IPv4 and IPv6 and able to leverage telemetry feeds from threat intelligence feeds that can analyses threat sources in email, both inside and outside, as well as other sources such as Web Security, IPS, Firewall, File History, and Advanced Malware.
- v. Include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable integration with firewall, IPS, SIEM solutions, ticketing systems etc. of major OEMs.

b) Authentication Solutions for Safe Access of Digital Assets for Safe City Project:

The Safe City Project environment is different from normal IT set up where in citizens, city administrators, officers, System Integrators and other people shall be accessing various services via connecting various ways of communication. This is imperative to authorize before they connect to city network and get access to various applications and services. These users demand access to city resources using more mediums than ever before, including personal laptops, tablets, and smartphones, and from home networks and mobile networks. Henceforth, it becomes important to deploy Authorization solution which can perform following roles:

- i. Authorization, Authentication and Accounting (AAA) of network connections. Should provide risk-based context driven user authentication.
- ii. Role-based control for a user, device, or application post-authentication. This means that a given user and their device are placed into their corresponding permission and authorization algorithms.
- iii. Confidentiality and containment of intellectual property through policy enforcement
- iv. Identity and asset management considering every element of the system architecture.



- v. Should be able to perform end point posture analysis and share contextual data with vulnerability reporting in order to identify and prioritize vulnerability of end point and to take appropriate action and time bound remediation.
- vi. Solution must have very robust inbuilt context-sharing platform that should deliver deeper level of contextual data, collected by this envisaged solution for Safe City Project, to external and internal ecosystem partner solutions in order to accelerate these solutions' capabilities across the network. This solution should share data with other Network devices such as Firewalls and packet capture system solutions.
- vii. **Multi-Factor Authentication:** Safe City Project Authorities must adopt Zero Trust Model to protect application and access to these application from unauthorized users. This infrastructure is being used by variety of users such as internal employees, contractors and various other authorities such as electricity and water departments. These users will have divers set of tools to access these applications hosted in DC/DR/Cloud and may log-in from any location. This solution must have below functionalities to avoid any cyber breach:
 - Validate Users with more than their credentials by utilizing strong multi-factor authentication.
 - Validate their Device, making sure that this is trustworthy and secure.
 - Grant the minimum level of permission their workers need to do their job.

c) Public Key Infrastructure (PKI)

Considering the requirement of a certifying authority PKI has been provisioned which will complement the authorization in coordination with NAC It has been provisioned vide a VM layer.

d) Management and Reporting

- i. Organizational Asset Data source management, log retention, security alert monitoring, incident response, governance reports.
- ii. Real time digital traps based contextual solution across entire organizational assets especially covering critical assets
- iii. Real time vulnerability detection & Patch Management. Real time Compliance assessment and non-compliance fix based mitigation.
- iv. Monitoring of any privilege use activity and critical user access management
- v. Real time detection of incoming and outgoing traffic within the organization network and remediation planning
- vi. Real time glass door monitoring, analysis, Triage, Incident Mgmt. Monitoring and collating Threat Intelligence and cyber news and Security update.
- vii. Basic Security tool administration and customer requests.



- viii. Vulnerability Scanning and policy Compliance scanning.
- ix. Dashboard and Reporting.

e) Authentication and Self testing of system

All the Equipment and system should be in built provision of self-authentication and self-testing wherever possible.

vi. Network Traffic Analyzer (NTA) /Behavioral Analysis & Anomaly Detection Tool for the City Network:

The rise of unknown malware compromising internal systems, devastating DDos attacks, APTs and threats bypassing traditional security have changed the cybersecurity landscape. Building perimeter walls and relying on signature- based solutions is not enough anymore. Only a detailed awareness of network behavior and a proactive fight against cyber threats can give control over the city IT environment back to administrators.

This Solution should have but not limited to below functionalities:

a) Visibility dentity Awareness

- NTA Solution should provide the internal network visibility and actionable insight required to quickly identify and troubleshoot a wide variety of network issues. Additionally, NTA integrates user information with network traffic statistics to deliver detailed intelligence into user activity anywhere across the network.
- NTA Solution should also collect and analyse device through integration with the NAC (Network Access Control) devices.

b) Troubleshooting

NTA Solution should also offer the flexibility and capability to drill down into the end user, MAC, flows, interface utilization and a wide array of other host statistics needed for rapid incident resolution.

c) Forensics and Incident Response

By collecting, analysing and storing large amounts of flow data, NTA System provides a full audit trail of all network transactions for detecting anomalous traffic and performing more effective forensic investigations.

vii. Workload Protection in Safe City Project Environment:

- i. The secure tool should provide application insights and inventory across DC's using auto generated application discovery and dependency mapping for workloads in various Dev, Test, Pre-Prod, Prod and other DC zones. It should always provide application blueprint for continuously changing application relationships and interdependencies.
- ii. It should generate a whitelist policy based on real-time application behaviour and keep the policies up-to- date as applications evolves and more applications are added and modified. The tool should enforce that generated application whitelist



policy consistently across bare-metal, virtual and container workloads. It should track policy compliance.

- iii. It should always provide application blueprint for continuously changing application relationships and interdependencies.
- iv. The tool should have the capability to track every process executed on the server and map behaviour deviations instantaneously to malware execution patterns. It should provide high fidelity alters for both systems generated and user defined events.
- v. It should provide real time traffic search and analysis capability for tracking and monitoring application and network performance on a per flow basis between all DC and external endpoints for real time and historic traffic flow.
- vi. It should detect multiple forms of process behaviour deviations such as shellcode, raw socket creation, user Login suspicious behaviour, restricted File Access, file Access from a different user, unseen Command etc.

viii. Advance Security for End Point Detection and Remediation:

Endpoints are often entry points for advanced persistent threats (APT) and targeted attacks. Advanced persistent threats and customized targeted malware attack toolkits are intentionally bypassing traditional signature-based antivirus solutions. Endpoint detection and response solutions do traditional signature-based technologies for richer behavior-based anomaly detection and visibility across endpoints.

Anti-APT Solution for Endpoints should provide enhanced visibility, context and control to prevent attacks, so that if malware gets in, it should be detected at earliest and respond before any damage to the system. These advance solutions must use a framework of vulnerability detection engine, including one-to-one signatures, fuzzy fingerprinting, machine learning and an AV detection engine. Also, this must get integrated to sandbox solution which automatically analyzes unknown files against behavioral indicators to detect malicious files, block and quarantine.

The unidentified traffic signatures by the Firewall or IPS will be sent to Anti-APT unit which will inspect and monitor the anomaly and suspicious activity of the packet within a focused VLAN environment. All identified threats are blocked at the periphery of DC by Anti-APT unit.

ix. Web Security/ Proxy Solution:

With the emergence of Web 2.0 and social media, web has become very important threat vector for cyber criminals. The web security should be important aspect of our cyber security solution and shall have following critical features:

- Must be a hardened Web Proxy, Caching, Web based Reputation filtering, URL filtering, Antivirus and Anti-malware appliance.
- Solution should support for Anti Malware/Anti-Virus engine that can scan HTTP, HTTPS and FTP traffic for web-based threats, that can range from adware,



browser hijackers, phishing and pharming attacks to more malicious threats such as rootkits, Trojans, worms, system monitors and Key loggers

- The solution should provide Web Reputation Filters that examine every request made by the browser (from the initial HTML request to all subsequent data requests) – including live data, which may be fed from different domains to assign a web-based score to determine the likelihood that it contains URL-based malware.

x. Gateway Level Anti-Spam and Anti-Virus Security Solution:

E-mail is most preferred threat vector for attackers and Safe City Project must have robust and reliable solution in place to protect their e-mail users.

- i. Solution must inspect all incoming and outgoing emails, and detect and protect against Spam, spoofing, virus, malware, including scanning of different file attachment types like doc, xml, txt, ods, ppt, zip etc. including compressed files
- ii. Support for scanning of password protected files/ attachments and provide sandboxing capabilities for suspicious files.
- iii. Support for Data Loss Prevention and have the capability to define rules to protect crucial data of the organization.
- iv. Support for IPv4 and IPv6 and able to leverage telemetry feeds from threat intelligence feeds that can analyse threat sources in ingress and egress emails, as well as other sources such as Web Security, IPS, Firewall, File History, and Advanced Malware.
- v. Must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable integration with firewall, IPS, SIEM solutions, ticketing systems etc. of major market players.

xi. SIEM (Security Information and Event Management):

Security Information and Event Management Unit will fulcrum all security measures. Every security appliance and the policy framework, functional SoPs will converge to SIEM. The appliance will be configured for central management with modules available with every security appliance/ VM to facilitate single event management dashboard.

The SIEM solution must collect logs from security and network devices, servers and application security logs. The MSI will be expected to perform the following as part of the SIEM implementation.

- i. SIEM tool to collect logs from the identified devices/applications/databases etc.
- ii. Develop parsing and normalization rules for non-standard logs
- iii. Implement correlation rules based on inbuilt functionality of the SIEM.
- iv. SIEM solution must be integrated with a Ticketing or Incident management tool.
- v. SIEM solution must provision for all logs retention and must maintain log for mutual agreed duration.



- vi. C-DAC will ensure that the MSI must appropriately account for the log storage as part of the solution.

xii. Cyber- Security Incident Response Service:

Safe cities have opened new avenues for attackers who can indulge in disruption. There is need of comprehensive incident response plan to handle any eventuality of espionage in better and well documented manner.

Service Provider should provide the following services to Customer in the event of an information security breach or disruptive cyber incident, such as protection from a Distributed Denial of Service (“DDos”) attack occurring anywhere within the customer IT System. The services are as follows:

- i. Incident scoping.
- ii. Analysis of malware to determine nature, origin, and scope of intrusion or infection.
- iii. Review of logs (network, system, application audit, etc.).
- iv. Real time monitoring in (for example to search for threat actor activity, malicious network indicators, backdoor communications, data exfiltration).
- v. Real time corrective actions or recommendations as necessary to protect the institution.
- vi. Collaboration with UT System and / or outside legal counsel, public relations and crisis management firms.
- vii. Collection of evidence in a manner that protects the chain of custody. H. Data recovery and restoration requirements for damaged systems.
- viii. Data recovery and restoration actions required from backup systems.
- ix. Provide recommendations of process or system changes to prevent a repeat of the incident.
- x. Provide comprehensive incident reporting at the conclusion of the incident.
- xi. Provide Executive Summaries.
- xii. Provide executive level briefings.
- xiii. Work with UT internal audit staff to provide relevant points for audit plans.
- xiv. During an engagement, OEM will be required to provide:
 - a) A written status report of activities completed, findings, and planned activities no less frequently than weekly;
 - b) Provide the UT System with an inventory of all copies made of files or configurations from workstations, servers, or network devices

xiii. Privilege Identity Management: Security concerns in Identity and Access Management



Including user Authentication, Authorization implementation will also include Directory Service for Authentication and Authorization of Service User. Solution will integrate with External Directory Services and gets Token/Identity from Directory Services.

Security Platform shall have strong security mechanism such as the use of advance encryption/digital certificates/ authentication to ensure that only authorized personnel have access to critical information, prevent man-in-the-middle attacks, and that the data is kept private.

Multi-Factor Authentication (MFA) security system that verifies a user's identity by requiring multiple credentials should be accessed while dealing with the critical data from the archives. It is a critical component of Identity and Access Management (IAM).

xiv. Server Security

It should provide effective protection using: Hardware Root of Trust, signed firmware updates, secure default passwords, Persistent event logging including user activity, Secure alerting, Automatic BIOS recovery, Rapid OS recovery, System erase and supporting Spine - Leaf architecture to optimize the east - west traffic flow inside the Data Center.

xv. Security Risk Audits (Third Part Audit)

It must be ensured that ISO 27001 (ISMS) Security Audits (Third Party) must be conducted as mentioned in this RFP to mitigate risk in regular operations and to stay compliant.

xvi. Privacy Protection

Since the envisaged data would be captured and analysis of sensitive data pertaining to residents and citizens will happen. Henceforth, privacy protection and ethical use of personal data must be ensured as per Data Protection Bill/ Act.

The logical depiction for the same is shown in the diagram below: -

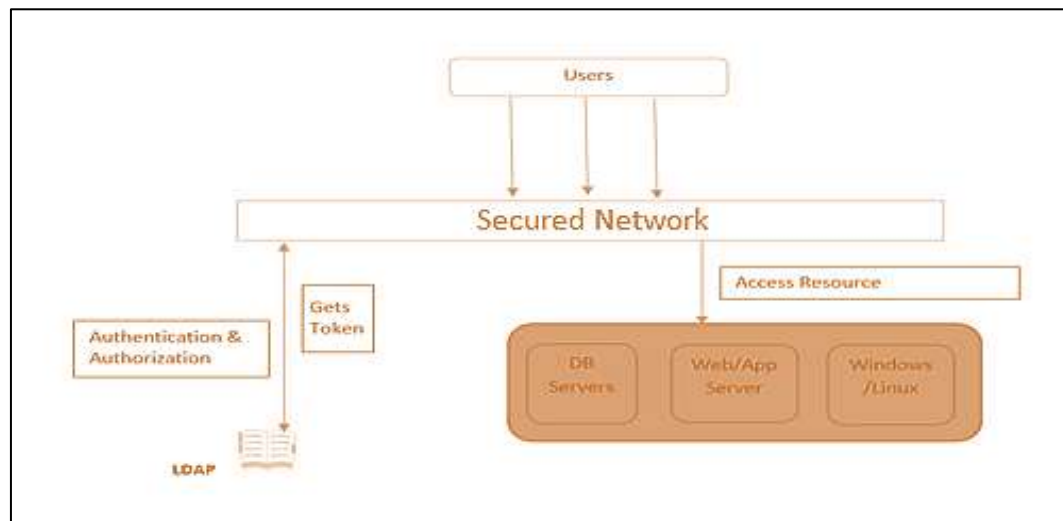


Figure: Privacy Protection Layout

xvii. Application security

- a. The security policies in the virtualization layer must be tied to the Surveillance application, which means whenever any application is moved from one virtualized server to another, even between different VLANs, the security policies should be followed throughout the application migration and there shouldn't be any need to redefine the security policies for the application at the new location. Also, when the application is deleted, all the security policies related to the application should also be removed.
- b. Detailed visibility into specific application processes and their associated network connections.
- c. Single console to configure Network & Security policies across a heterogeneous environment where application can run on hypervisor, virtualised server and containers (apply stateful layer 4 firewall at the edge to protect traffic flow between external and internal application and databases which will reside on virtualisation layer sitting directly on the hardware not on the guest OS).
 - Security Policy Management
 - a. Report the amount of East-West, North-South, virtual machine to virtual machine, virtual machine to physical traffic within the data center
 - b. Provide a converged view of virtual and physical network, provide end to end topological view of path between two virtual machines. It should support leading hardware vendors as well.

i. Edge device security

- a. Be able to control and manage your edge devices (edge systems/gateways and things)
- b. Extend IT security standards to the edge infrastructure with granular visibility and control for all connected devices, applications and networking.



- c. Rapidly configure and securely deliver updates/patches to firmware and software with fine grained control over approvals, scheduling, activation and installation

xviii. Work Flow- secured Management

- i. The system must be equipped with mobile application platform to enable sharing triggers to the field/ beat officer, SHO, DCP on real time of incident occurrence.
- ii. Along with the triggers, the concerned officer must be able to get the snapshot of the incident along with the access to mobile interface of the real time multi-cast video stream of the camera at incident location.
- iii. All the mobile devices for access to the system will be registered and whitelisted in the system, mac-binded over private VPN network.
- iv. Any attempt for unauthorized access to the system will be immediately tracked and the connection, if established will be terminated. The mobile gateway will send an immediate SMS to all the officers mapped in a pre-defined escalation matrix.

xix. Safeguarding, Anti-vandalism and anti-tampering mechanisms for edge devices:

Effective and suitable mechanisms to be ensured for monitoring upon the vandalism, tampering, etc. with the field device' operations like Central Policy Manager at DC for infrastructure and network monitoring, installation of vandalism proof cameras.

xx. Other security parameters:

- a) The message exchange between various applications in the Safe City Project should be fully encrypted and authenticated. Any application outside the Data Center (DC) should talk to the applications hosted in the data center only through predefined APIs and via encrypted channel.
- b) The Safe City Project architecture should be capable of managing heterogeneous data, which would be continuously communicated through numerous devices following different protocols. In order to ensure that the flow of data between devices does not run into latency issues, appropriate protocols need to be deployed so as to minimize latency. The following communication protocols could be used for the different layers for data flow;
- c) Between applications and back end systems: HTTP, SQL, FTP, HLS, SNMP, SOAP, XML, SSH, SMTP
- d) Between back end systems and field devices: Message Queue Telemetry Transport (MQTT), xMPP, RESTful HTTP, Constrained Application Protocol (CoAP), SNMP, IPv4/6, BACnet, LoNworks, Low Power Wide Area Network (LoRa), Fixed, 4G/5G, Wi-Fi, WiMax, 2G/3G
From field devices: ZigBee oLP, ETSI LTN, IPv4/6, 6LoWPAN, ModBus, Wi-Fi, 802.15.4, enocean, LoRA, RFID, NFC, Bluetooth, DashT' Fixed, ISM & short-range bands.



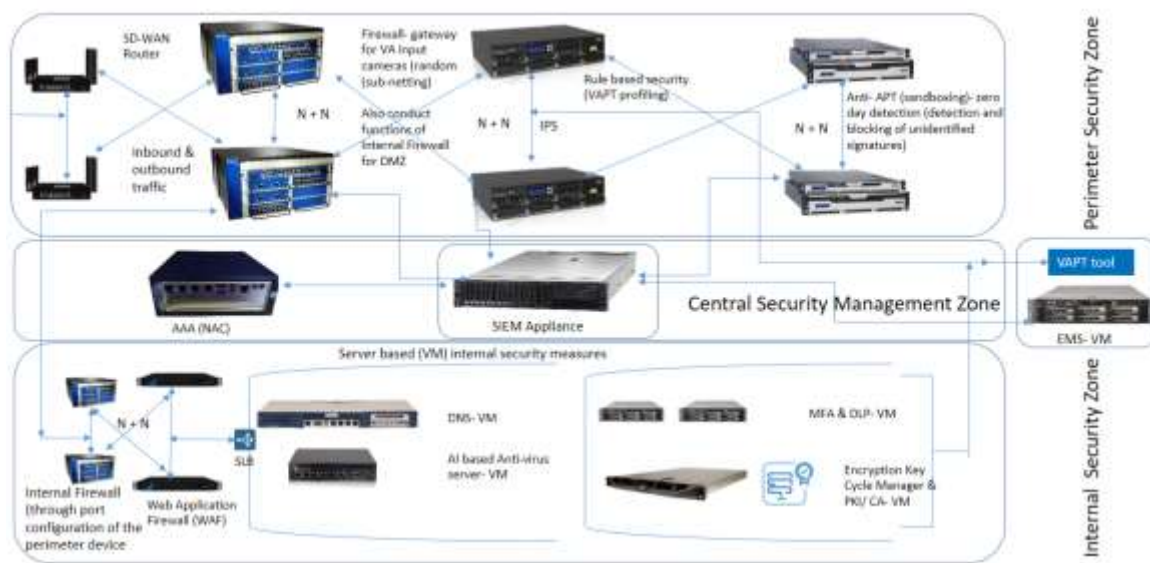
- e) From a network security perspective all information that flows on the network should be encrypted to ensure safety and privacy of confidential data. The devices at each endpoint of the network should be authenticated (using mechanisms based on attributes one of which could use passwords). The authentication system so used on these endpoint devices should ensure that only authorized users are sending data over the network, and there is no rogue data that is sent to the control systems to generate false alarms or sabotage the systems
- f) All the mobile, external devices as required in the system to use data from the Data Center for effective Decision Support System by the stakeholders will be MAC bound and proper authentication through login credentials will be provided to access the encrypted database.
- g) 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.
- h) 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.
- i) Open Standards - Systems should use open standards and protocols to the extent possible.
- j) 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 status of their applications
- k) Support for Public Key Infrastructure (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).
- l) The Security solution will build a zero-trust security architecture where appropriate security controls are available for every Surveillance workload/application.
- m) Solution will protect every Surveillance application/ workload with a state full distributed in firewall.
- n) Security solution should protect workload at the NIC level with a full stateful firewall engine at a very granular level based on constructs such as MAC, IP, ports, objects and tags, active directory groups, Security Groups, etc.
- o) The network will provide distributed routing (OSPF & BGP), virtual switching, NAT



function, Software L2 bridging to physical environments, L2 & L3 VPN services.

- p) The solution should be capable to provide agentless guest introspection services like Anti-Malware etc. and Network introspection services like IPS/IDS, edge load balancing, multi-site networking (Layer 2 extension) irrespective of underlying physical topology for active - active DC & DR purposes, container network and security for container to container L3 networking and micro segmentation for micro-services etc.
- q) Solution provide traffic visibility, end point monitoring for visibility up to layer 7 for network monitoring and automating application security rules, firewall planning & management, network virtualization operations & troubleshooting tools.
- r) Solution will support reduction in Recovery Time Objective when the failover / fall back are brought up from DC to DR, without the need to redo the IP-addresses, the default gateway router should be stretched across data centers, also the firewall policy should also be applied across DC & DR automatically.
- s) Each gateway connected to Edge devices uses authorised Access Control Lists for ongoing communicating with the server to reduce spoofing and device sessions use an HMAC-based authentication token for continued communication with the server and should detect anomalies by monitoring configurable device metric thresholds and initiate remediation actions with rule-based alerts and API based integrations with 3rd party tools.

Security zone- Perimeter & Internal (HA) Architecture



Security Parameters- Technical Requirements and Compliance Sheet for MSI (to provide compliance report with the bid)

Firewall

S No.	Specifications	Compliance (Yes/ No) with comments, if any
1.	Firewall architecture should be DC grade with Data and control plane are different and Gartner quadrant from last 5 years shall be preferred.	
2.	Firewall appliance should be supplied with at least 4x100GE QSFP28/40GE QSFP+, minimum 10x 10GE SFP+, 2x GE RJ45 and scalable. SFP Transceivers to be populated as per solution requirement	
3.	Next Generation Firewall Throughput should be at least 100 Gbps for Enterprise Mix / Application mix production traffic and should be scalable to 150 Gbps in Future	



4.	Firewall should have IPSec VPN throughput of 50 Gbps. The effective next generation firewall throughput should be 100 Gbps in real time/ Application/Enterprise traffic mix to cater bandwidth requirement of 100 Gig interface so as to ensure IDS for monitoring malicious activity or defined policy violations. It should be scalable to 100 Gbps or better The Firewall must be capable to conduct operations of internal firewall with regards to application and structured data that will be residing in the DMZ. Also, it should facilitate the coordinative flow of 2 Gig SSL data (traffic) to IPS.	
5.	Firewall should support 5K site-to-site VPN tunnels & 10K Client to Site VPN tunnels	
6.	The appliance should be secure in itself with certifications NDPP/ EAL4, FIPS/ICSA. Extra certificate will be added advantage like NEBS etc.	
7.	The Firewall solution should support LLDP, ECMP, NAT64, DNS64 & DHCPv6.	
8.	The proposed system shall be able to operate on either Transparent (bridge) mode to minimize interruption to existing network infrastructure or NAT/Route mode. Both modes can also be available concurrently using Virtual Contexts. Minimum 10 Virtual Firewall licenses to be provided with the solution and should be scalable to 225 Virtual Firewalls in future	
9.	The physical interface shall be capable of link aggregation, otherwise known as the IEEE 802.3ad standard, allows the grouping of interfaces into a larger bandwidth 'trunk'. It also allows for high availability (HA) by automatically redirecting traffic from a failed link in a trunk to the remaining links in that trunk.	
10.	The Firewall should have integrated SSL VPN solution to cater to 5000 SSL VPN concurrent users.	
11.	The proposed device should minimally attain Common Criteria and Internet Computer Security Association (ICSA) Certification.	
	The proposed system should support	
	a) IPSEC VPN	
	b) SSL VPN	
	c) GRE, VX LAN inspection	
	d) SSL and SSH decryption for both inbound and outbound apart from video streaming Data	
12.	The device support be open based and not on the basis of proprietary Application specific integrated circuit.	
13.	The Firewall Threat Prevention (FW + AVC + IPS+ Antivirus +Anti Malware) throughput should be 60 Gbps for Enterprise Mix / Application mix production traffic and should be scalable to 100 Gbps in Future	
14.	FIREWALL solution should have capability to protect against Denial of Service (DOS) and DDOS attacks. Should have flexibility to configure threshold values for each of the Anomaly. DOS and DDOS protection should be applied and attacks stopped before firewall policy look-ups.	



15.	FIREWALL should have a configurable action like terminate a TCP session by issuing TCP Reset packets to each end of the connection, or silently drop traffic in addition to sending a alert and logging the incident	
16.	Antivirus	
17.	The threat prevention (FW + AVC + IPS + Antivirus +Antimalware) throughput should be at least 60 Gbps on Enterprise Mix / application Production traffic	
18.	The proposed system should be able to block, allow or monitor only using AV signatures and file blocking based on per firewall policy based or based on firewall authenticated user groups with configurable selection of the following services:	
19.	HTTP, HTTPS, SMTP, SMTPs, POP3, POP3s, IMAP, FTP etc.	
20.	The proposed system should be able to block or allow oversize file based on configurable thresholds for each protocol types and per firewall policy.	
21.	The FIREWALL solution should not have any wireless code in the offered device or its family in hardware or software and should be able to integrate with the proposed on-premise Anti-APT solution to scan for zero-day malwares from Day 1	
22.	Application Control	
23.	The proposed system shall have the ability to detect, log and take action against network traffic based on over 3000 application signatures	
24.	The application signatures shall be manual or automatically updated	
25.	The administrator shall be able to define application control list based on selectable application group and/or list and its corresponding actions and should also support policy-based routing on the basis of application.	
26.	Data Leakage Prevention	
27.	The proposed system shall allow administrator to prevent sensitive data from leaving the network. Administrator shall be able to define sensitive data patterns, and data matching these patterns that will be blocked and/or logged when passing through the unit.	
28.	High Availability	
29.	The proposed system shall have built-in high availability (HA) features without extra cost/license or hardware component	
30.	The device shall support stateful session maintenance in the event of a fail-over to a standby unit.	
31.	High Availability Configurations should support Active/Active and Active/ Passive	
32.	Logging & reporting	
33.	A dedicated appliance with minimum 10TB or more storage RAID 1/5/6 to be proposed with the solution for logging, analysis, and reporting into a single system with 500 device licenses from day-1, delivering increased knowledge of security events throughout the network for centralized security event analysis, forensic research and reporting	



WAF (QTY No.2 in HA)

S No.	Specification	Compliance (Yes/ No) with comments, if any
1	The proposed appliance should provide minimum 2Gbps WAF (HTTPs) throughput	
2	The proposed appliance should have:	
3	Traffic ports: 6 x 10G QSFP+ and 6 x 10G SFP+ ports and 4TB HDD	
4	Should support 25M HTTP Request Per Second 100000 SSL TPS with RSA2K Key and 75000 with ECC	
	Device should have Sub Millisecond Latency	
5	Should support 25 Million HTTP request per second & 10 Million L7 request per second	
6	The proposed appliance should have 32GB RAM and scalable upto 512GB RAM	
7	The proposed appliance should have virtual administrative domains feature that support multiple tenant environments.	
	The proposed device should have 5 Virtual Instances from Day 1 and scalable upto 20 Virtual Instances.	
8	WAF should have the flexibility to be deployed and perform in the following modes: Active mode, passive mode, Transparent mode, proxy mode, Sniffer and Forensic mode. - Reverse proxy - Out of Path (OOP) support	
9	The WAF should be able to bypass the traffic in case of its failover.	
10	The proposed solution should support standard VRRP (RFC – 2338) or equivalent for High Availability.	
11	The WAF should support the following escalation modes:	
	a) Active,	
	b) Bypass,	
	c) Passive	
12	Should support custom signatures	
13	Provide ability to allow/deny URL access	
14	The device should support for Ipv4 and Ipv6 traffic	
15	Auto Policy Optimization and learning	
	• Zero Day Attack Blocking – Extended Mode	
	• Security Filter Auto Policy Generation	
	a) Full Auto	
	b) Auto Enabled	
	c) Auto Refinements	
	• Auto Discovery	



16	Should have the capability to Auto-Learn Security Profiles required to protect the Infrastructure.	
17	Should provide a statistical view on collected application traffic	
18	Policies must be automatically generated from auto learn results	
19	WAF should continue to provide protection even while in learning mode.	
20	Following Threats should be protected by the proposed WAF solution:	
	Parameters Tampering	
	Cookie Poisoning	
	SQL Injection	
	Session Hijacking	
	Buffer Overflow Attacks	
	Cross-Site Scripting (XSS)	
	Brute Force Attacks	
	Cross Site Request Forgery (CSRF)	
	Path (directory) Traversal	
	Malicious file upload	
21	The proposed WAF should support the Activity Tracking.	
22	WAF should support the Historical Security Reporting from Day 1	
23	Ability to identify and notify system faults and loss of performance	
24	Should support Log Aggregation	
25	Should support multiple log formats such as CSV, Syslog, TXT, etc..	
26	Should support inbuilt Reporting and sending the report via E-Mail	
27	Should support report formats in PDF/HTML/WORD/RTF, etc..	
28	Reports should be customizable.	
29	Report Distribution Automatically via email	
30	Event Management: There has to be a feature of Management Module/ tool to establish link with EMS platform & SIEM.	
31	The solution must be able to handle OWASP Top 10 attacks, Anti-Bot Mobile DDos protection and application layer encryption and API authentication and API Gateway protection	
32	The proposed solution should have capability of BOT detection and Protection beyond signatures and reputation to accurately detect malicious and benign bots using client behavioural analysis, server performance monitoring, and escalating JavaScript/ CAPTCHA challenges/Device Fingerprinting	
	The solution must protect against FTP, SMTP, HTTP, HTTPS and Application layer Dos and DDOS attacks including stress-based DOS and Heavy URL attacks.	



	WAF should support inbuilt capability or via integration with 3rd party solution to protect against the mobile/tablet application-based attacks through Anti-Bot Mobile SDK which whitelist establish trust based on an embedded software package within the application code and corresponding cookie verification to protect application against attacks generated from mobile	
33	The solution must support integration with third party DAST tool to perform virtual patching for its protected web applications. The solution must support integration with leading DAST solutions like WhiteHat, QualysGuard, and IBM etc. to virtually patch web application vulnerabilities	
	The proposed solution should support below services to protect and manage access to applications: • Identity Federation and SSO – Creates a single point of policy-based access for cloud and on premise/private applications with MFA support. • Client and Web-based SSL VPN Access – Policy-based access to network VPN service through web-plugins or clients on mobile and desktop operating systems. • Web Portal Access to Applications – Open web applications to users instead of opening up your network. • Desktop Application and VDI Support – Policy-based access to virtualized applications through a single, consolidated gateway along with native VDI support and a customizable, web portal. • Secure Web Gateway Proxy Services – Provides web-based malware protection and URL filtering through Secure Web Gateway Services	
	Offered solution should be EAL or NDPP (Network Device Protection Profile) certified under Common Criteria Program for security related functions.	
34	OEM of WAF product should be ISO-9001, ISO-27001 certified	

Anti-APT

S No.	Specification	Compliance (Yes/ No) with comments, if any
1	The solution should be able to communicate bi-directionally with the proposed FIREWALL solution for automatic blocking/threat update	
2	The solution should support deep packet inspection of SSL encrypted traffic (including HTTPS) for both incoming and outgoing	
3	The solution should provide detection, analysis and remediation capability against APT & SSL based APT attacks.	



4	The solution must employ an on premise (not on cloud) analysis engine using virtual execution to detect zero day and unknown threats and must not be signature based. But should have option to work in hybrid mode if required.	
5	The proposed solution should be able to detect and prevent advanced Malware, Zero-day attack, spear phishing attack, drive by download, watering hole and targeted Advanced Persistent Threat without relying on just Signature database.	
6	The proposed solution should perform dynamic real-time analysis of advanced malware to confirm true zero-day and targeted attacks. No file should be sent to third party systems or cloud infrastructure system for analysis and detection of Malware	
7	The proposed solution should automatically detect and confirm multistage zeroday malware and targeted attacks without prior knowledge of the malware.	
8	The proposed solution should utilize a state-full attack analysis to detect the entire infection lifecycle, and trace the stage-by-stage analysis of an advanced attack, from system exploitation to outbound malware communication protocols leading to data exfiltration.	
9	The proposed solution should analyze advanced malware against a cross-matrix of different operating systems and various versions of pre-defined applications.	
10	The solution must support pre-populated Licensed copies of Operating systems and applications/software's (like Microsoft Office). There should be no requirement for the customer to buy additional license.	
11	The proposed solution should have the ability to analyse, detect and block malware in common file formats including but not limited to executables, JAVA, PDF, MS Office documents as per the OEM policy, links in email and ZIP/RAR/7ZIP/TNEF archives to prevent advanced Malware and Zeroday attacks and should be able to convert unknown to known in 300 seconds post detection and should be mentioned on public website.	
12	The proposed solution should be able to analyse email attachments and malicious links for static and dynamic analysis	
13	The solution should provide reports in (but not limited to) PDF/CSV formats.	
14	The solution should support for SIEM log integration.	
15	The solution should be able to schedule reports and also provide the flexibility to generate on-demand reports like daily/weekly/monthly/yearly/specific range (day and time) etc.	
16	Minimum number of Interfaces – 4x GE RJ45 ports	
17	Number of VM's should be at least 25 on Day1, scalable to 50 VMs	
18	The APT appliance should be able to process minimum of 150000 files/month and scalable to 3,00,000 files/month (either web or mail or both)	



19	High Availability & Maximum Scalability up to 20 devices in cluster	
20	The solution should have dual AC power supply fully populated (within box) and 2 TB in RAID 1 from day one and should have at least 4 extra bays for future scalability	

Intrusion Prevention System (IPS)

S No.	Specification	Compliance (Yes/ No) with comments, if any
1	The IPS solution must be a purpose-built dedicated appliance or a subset of proposed firewall appliance should be capable handling seamless throughput of 50 Gbps scalable to 100 Gbps	
2	The device must have separate dedicated interface for management and device must have inbuilt internal Redundant Power Supply (RPS) and redundant hot swappable fan trays	
3	Intrusion Prevention solution should have in built or external zero-day threat protection with customize simulation environment and should integrate with the asked APT solution.	
4	The device must have functionality of hardware-based fail-open or option to disable software features. NIPS must also have fail-open feature, in built or external which must allow traffic to pass through uninterrupted when power failure occur on the NGIPS.	
5	The device must accurately detect intrusion attempts and discerns between the various types and risk levels including unauthorized access attempts, pre-attack probes, suspicious activity, DoS, DDos, vulnerability exploitation, brute force and zero-day attacks.	
6	The IPS must protect against the following categories: - Exploits, Identity Theft/Phishing, Reconnaissance, Security Policy, Spyware, Virus, Vulnerabilities and should support inspection of headers with 802.1Q for specific Layer 2 security group tag (SGT) values and drop the packet based on Zone Protection profile	
7	The proposed IPS must be able to support granular security policy enforcement based on the following methods: Per application (all segments), Per physical segment unidirectional and bidirectional.	
8	The IPS filter must support network action set such as Block (drop packet), Block (TCP Reset), Permit, Trust, Notify, Trace (Packet Capture), Rate Limit & proposed IPS solution must support signatures, protocol anomaly, vulnerabilities and traffic anomaly filtering methods to detect attacks	



	The IPS should have native protection against credential theft attacks (without the need of endpoint agents) with ability to prevent the theft and abuse of stolen credentials.	
9	The centralized management server must be an appliance based on a hardened OS shipped by-default and system shall allow the latest update to be manually, automatically or based on schedule with central management and reporting.	
10	Must have 4 x 10 G interface, 2 X 100 Gbps and 8 x 1 G copper port. IPS Should have bypass capability considering internal issues i.e. memory hang, firmware crash etc.	
11	The single device must have minimum Inspected throughput of 60 Gbps scalable to 120 Gbps for all kinds of real world/ enterprise mix/ application mix traffic in Active-Active or Active-Passive mode.	
12	The proposed IPS must be able to control the known bad host such as spyware, botnet C2 server, spam and so on based on country of origin, exploit type and the reputation score	
13	The solution must use prevention techniques and provide zero-day protection against worms, Trojans, spyware, key loggers, and other malware from penetrating the network.	
14	Latency must be <50 microseconds considering variable size of data packet sizes in concurrent sessions. Must support 4000,0000 concurrent sessions scalable to 6000,0000	
15	NIPS solution should have inbuilt or external zero-day threat simulation and then create IOC's within 5 minutes post detection and revert back to inline device to block threats on real time.	
16	The NIPS solution should be able to categorized traffic based on geo-location.	
17	The NIPS solution should be able to filter (restrict/allow) traffic based on application protocol, web application, client application & server application.	
18	The centralized management server if provided as separate from asked Firewall management, should provide dashboard for various summary i.e. top attackers, top targets, categories of attack, categories of traffic based on geolocation/application protocol/os	
19	The centralized management server should have facility to generate reports such i.e. events reports, intrusion events, malware events etc. and same should be exported to excel and pdf.	
20	The centralized management server should have ability to monitor its & NIPS health.	
21	The solution should have facility to schedule the reports	
22	The solution should have facility to rollback update and should not impact the environment.	
23	The NIPS Should support Ipv6 from day one.	
24	All features should be fully functional from day one and should be loaded with all necessary license required.	



25	Accurately detects intrusion attempts and discerns between the various types and risk levels including unauthorized access attempts, pre-attack probes, suspicious activity, DoS, DDos, vulnerability exploitation, brute force, hybrids, and zero-day attacks.	
26	The NIPS solution should be able to prioritizes risky hosts and users, including active botnets, through the identification of anomalous network behavior	
27	Event Management: There has to be a feature of Management Module/ tool to establish link with EMS platform & SIEM.	

DDos

S No.	Specification	Compliance (Yes/ No) with comments, if any
1	DDos mitigation solution should be a dedicated appliance (not a part of Router or IPS or Next Generation firewall solution). Also, IPS, Next Generation firewall and Anti-DDos should be from different OEM for better security purpose	
2	Dedicated appliance based DDOS Mitigation solution with: i) Legitimate throughput handling of 100Gbps with 100 Million concurrent connections ii) Mitigation Capacity of 80 Gbps ii) Inspection Ports supported: 4 x 40G QSFP+ and 16 x 10G SFP+ ports	
3	Dedicated appliance-based solution with DDos flood prevention rate/ Syn Cookies per second of 200 Million and support of handling 100000 SSL-CPS on RSA 2K Key and 75000 SSL-CPS on ECC with 50Gbps of SSL throughput.	
4	BEHAVIORAL ANALYSIS using behavioral algorithms and automation to defend against threats, including Mirai DNS Water Torture, Burst and Randomized attacks, should provide DNS based DDos attack protection for individual record type like A, AAAA, CNAME, PTR, MX, NS and TXT	
5	POSITIVE SECURITY MODEL should have advanced behavior-analysis technologies to separate malicious threats from legitimate traffic	
6	ZERO DAY ATTACK PROTECTION should be provided by behavior-based protection with automatic signature creation against within seconds of unknown, zero-day DDos attacks.	
7	CUSTOM TAILORED HARDWARE must be proposed using dedicated DoS Mitigation platform which off-loads high volume attacks, inspecting without impacting user experience.	



8	Behavioral DoS (Behavioral Denial of Service) Protection should defend against zero-day network-flood attacks, detect traffic anomalies and prevent zero-day, unknown, flood attacks by identifying the footprint of the anomalous traffic. Network-flood protection should include: • TCP floods—which include SYN Flood, TCP Fin + ACK Flood, TCP Reset Flood, TCP SYN + ACK Flood, and TCP Fragmentation Flood • UDP flood • ICMP flood • IGMP flood	
9	All layer 3, 4, and 7 DoS/DDos threats including flood/sweep with Src/Dst IP address awareness, UDP/DNS/HTTP/TCP/SIP/SYN/ACK/RST/FIN using sub-second detection, network behavior analysis, 120+ DDos vectors, application anomaly detection, dynamic filtering, protocol analysis, source tracking, control policies, and more.	
10	Should have inbuilt advance and Hardware accelerated purpose-built TLS stack for Key exchange and bulk inspection; RC4, DES, 3DES, AES-CBC, AES-GCM, AES-GMAC, RSA, DSA, DH, ECDSA, ECDH, MD5, SHA, SHA2 ciphers	
11	The proposed appliance should support Geo-location blocking feature	
12	OEM has to provision for knowledgeable and specialized security experts to provide 24x7, TAC services for the network facing denial-of-service (DoS) attack in order to restore network and service operational status.”	
14	Centralized Monitoring and Reporting solution should be provided from Day 1	
15	Event Management: There has to be a feature of Management Module/ tool to establish link with EMS platform & SIEM.	
16	The proposed solution shall meet following DNS protection functionality: • Should support DNSSEC • DNS DDos threshold alerting • DNS query limit for individual record type like A, AAAA, CNAME, PTR, MX, NS • DNS NX-Domain attack protection • DNS TCP active authentication	



Data- Leakage Prevention

S No.	Specification	Compliance (Yes/ No) with comments, if any
1.	Must offer comprehensive customer/server security by protecting enterprise networks which includes virus protection, spyware, rootkits, bots, grayware, adware, malware and other computer borne threats or mixed threat attacks or any emerging cyber-attacks or zero-day attack protection.	
2.	Solution must clean computers of file-based and network viruses plus virus and worm remnants (Trojans, registry entries, viral files)—through a fully-automated process.	
3.	Must be able to reduce the risk of virus/malware entering the network by blocking files with real-time compressed executable files.	
4.	Must include capabilities for detecting and removing rootkits	
5.	Must provide Real-time spyware/grayware scanning for file system to prevent or stop spyware execution	
6.	Must have Assessment mode to allow first to evaluate whether spyware/grayware is legitimate and then take action based on the evaluation	
7.	To address the threats and nuisances posed by Trojans, the solution should be able to do the following but not limited to:	
	a) Terminating all known virus processes and threads in memory	
	b) Repairing the registry	
	c) Deleting any drop files created by viruses	
	d) Removing any Microsoft Windows services created by viruses	
	e) Restoring all files damaged by viruses	
	f) Includes Clean-up for Spyware, Adware etc.	
8.	Must be capable of cleaning viruses/malware even without the availability of virus clean- up components. Using a detected file as basis, it should be able to determine if the detected file has a corresponding process/service in memory and a registry entry, and then remove them altogether.	
9.	Must provide Outbreak Prevention to limit/deny access to specific shared folders, block ports, and deny write access to specified files and folders on selected customers in case there is an outbreak	
10.	Behavior Monitoring:	
11.	a) Must have behavior monitoring to restrict system behavior, keeping security related processes always up and running	
12.	b) Enable certification that a software is safe to reduce the likelihood of false positive detections or equivalent	



13.	Must provide Real-time lock down of customer configuration allow or prevent users from changing settings or unloading/uninstalling the software	
14.	Users with the scheduled scan privileges can postpone, skip, and stop Scheduled Scan.	
15.	CPU/memory (physical or virtual) usage performance control during scanning:	
16.	a) Checks the CPU usage level configured on the Web console and the actual CPU consumption on the computer	
17.	b) Adjusts the scanning speed if: The CPU usage level is Medium or Low	
18.	c) Actual CPU consumption exceeds a certain threshold	
19.	Should have a manual outbreak prevention feature that allows administrators to configure port blocking, block shared folder, and deny writes to files and folders manually	
20.	Should have Integrated spyware protection and clean-up	
21.	Should have the capability to assign a customer the privilege to act as a update/master relay agent for rest of the agents in the network	
22.	Shall be able to perform different scan Actions based on the virus type (Trojan/ Worm, Joke, Hoax, Virus, other)	
23.	shall be able to scan only those file types which are potential virus carriers (based on true file type)	
24.	Should be able to detect files packed using real-time compression algorithms as executable files.	
25.	shall be able to scan Object Linking and Embedding (OLE) File	
26.	Must provide Web threat protection by the following ways:	
27.	a) Must be able to protect the endpoints from Web threats by blocking access to and from malicious sites based on the URL's reputation ratings	
28.	b) Must extend Web threat protection to the endpoints even when they disconnect from the network, i.e. regardless of the location	
29.	c) Must have the capabilities to define Approved URLs to bypass Web Reputation policies	
30.	d) Must provide real-time protection by referencing online database with millions of rated Web domains	
31.	e) Configure Web reputation policies and assign them to individual, several, or all end users' machine.	
32.	Must be capable of uninstalling and replacing existing customer antivirus software and to ensure unavailability of any residual part of the software.	
33.	Security Compliance should leverage Active Directory services to determine the security status of the computers in the network	
34.	Must provide File reputation service	



35.	a) Must be able to check the reputation of the files hosted in the internet	
36.	b) Must be able check the reputation of the files in webmail attachments	
37.	c) Must be able to check the reputation of files residing in the computer	
38.	Must protect customers and servers on the network, high performance network virus scanning, and elimination.	
39.	Must provide the flexibility to create firewall rules to filter connections by IP address, port number, or protocol, and then apply the rules to different groups of users	
40.	Must have smart feedback to enable feedback from the customer agents to the threat research Centers of the vendor.	
41.	Uses any alternate method other than the conventional pattern-based scanning with the following features:	
42.	a) Provides fast, real-time security status lookup capabilities in the cloud	
43.	b) Reduces the overall time it takes to deliver protection against emerging threats	
44.	c) Reduces network bandwidth consumed during pattern updates. The bulk of pattern definition updates only need to be delivered to the cloud or some kind of repository and not to many endpoints	
45.	d) Lowers kernel memory consumption on endpoints. Consumption increases minimally over time.	
46.	Should be able to deploy the Customer software using the following mechanisms:	
47.	a) Customer installation Package (Executable & Installer Package Format), should support silent installer, unmanaged customers, specific installer for servers	
48.	b) Web install page	
49.	c) Login Script Setup	
50.	d) Remote installation	
51.	e) From a customer disk image	
52.	Must provide a secure Web-based management console to give administrators transparent access to all customers on the network	
53.	The management server should be able to download updates from different source if required.	
54.	Must reduce network traffic generated when downloading the latest pattern by downloading only incremental patterns.	
55.	Must have the flexibility to roll back the Virus Pattern and Virus Scan Engine if required via the web console	
56.	Should have role-based administration with active directory integration.	
57.	a) To create custom role type	



58.	b) To add users to a predefined role or to a custom role	
59.	Should have integration with the Active directory 2008/2012 or higher	
60.	Shall support grouping of customers into domains for easier administration & Endpoint security solution should provide vulnerability protection, which should scan the machine and provide CVE number visibility and accordingly recommend rule for virtual patch against vulnerability.	
61.	Establish separate configuration for internally versus externally located machines (Policy action based on location awareness)	
62.	Should have a monitoring feature which sends a customized alert message to specified recipients when log counts from customer IPS, customer firewall, and/or network virus logs exceed certain thresholds, signaling a possible attack.	
63.	Must be able to send a customized notification message to specified recipients when firewall violations exceed certain thresholds, which may signal an attack	
64.	Should perform Boot & Rootkit scan and cleaning, Endpoint security solution should have capability of AV, Vulnerability protection, HIPS, Firewall, Device control, virtual Patching and integrated DLP with pre and post machine learning execution for malware analysis.	
65.	Virus definition files should be lighter so that same can be transmitted to remote locations having minimum of 64kbps link or the update pattern size should be less than 200Kb	
66.	AV should be seamlessly implemented on all the variants of the Operating System.	
67.	System should be configured in such a way that at no case no endpoints/remote agents will be able to communicate with OEM cloud for obtaining updates through internet.	
68.	In case of bot infection, bot removal tools also to be facilitated to clean the infected machine	
69.	The solution should have latest machine learning technology in built from day one.	
70.	The solution should have the option of the endpoint vulnerability shielding in the network.	
71.	The solution should have ransomware protection in built.	
72.	Event Management: There has to be a feature of Management Module/ tool to establish link with EMS platform & SIEM.	



VAPT

S No.	Specification	Compliance (Yes/ No) with comments, if any
1	Vulnerability Assessment and Penetrating Testing (VAPT) must ensure series of tests on the system architectural associated IP devices throughout the network.	
2	Continual security assessments should be conducted so that the vulnerable areas are exposed and quantification and the prioritization of such instances can be done.	
3	Accurately detect vulnerabilities through rapid network mapping and regular, scheduled scans across all of your devices	
4	Test for and identify emerging network vulnerabilities to prevent external agents from accessing them	
5	Proactively discover vulnerabilities in web and mobile applications using authenticated and un-authenticated scanning, protecting the system from unauthorized access.	
6	VAPT will behave as a risk assessment tool which will ensure the following steps:	
A.	Cataloguing assets and capabilities (resources) in a system	
B.	Assigning a quantifiable value (or at least rank order) and importance to those resources	
C.	Identifying the vulnerabilities or potential threats to each resource	
D.	Mitigating or eliminating the most serious vulnerabilities for the most valuable resources	
7	Event Management: There has to be a feature of Management Module/ tool to establish link with EMS platform & SIEM.	

SIEM Appliance (Should work in HA Mode)

S No.	Description	Compliance (Yes/ No) with comments, if any
1.	The SIEM solution should provide a dedicated appliance with provision of scaling up with distributed architecture and should have minimum 100 TB of built-in/DAC storage capable of processing 20000 EPS with scalability to 30000 EPS in future. And 1Gbps capture rate scalable to 5GBPS without appliance change. The solution should have no limitation of number of devices for integration.	



2.	The SIEM solution must be able to store both the raw event log as well as the parsed event log/normalized data. Storage should be sized to provide 1-year online log storage at central site. Both raw logs and normalized logs should be made available with minimum 100 TB usable of storage expandable to 200 TB provided by OEM on the same appliance.	
3.	SIEM solution should maintain minimum 90 days of logs (both raw and normalized) in an uncompressed format to allow for fast searching, threat hunting, and investigation. Data beyond 90 days should be compressed with minimum 50% or better compression to save storage requirement. All the data should be available online for min 1 year	
4.	The SIEM & Log Monitoring solution should be from a different OEM other than the Prevention Security solutions like F/W, IPS, HIPS, AV, DLP. So that it can detect threats missed by other existing tools using the security defense in depth strategy.	
5.	The solution must have the ability to capture live network traffic at 1 Gbps and import PCAP files using the same infrastructure and it must be able to detect malicious payload in network traffic • Detect and reconstruct files back to its original type • Detect hidden or embedded files • Detect and flag out renamed files • Complete session reconstruction with support for HTTP/2 protocol	
6.	The solution should be a purpose-built OEM appliance-based system with following dedicated components: a. Management & Reporting b. Normalization and Indexing c. Integrated Correlation Engine for logs and packets. d. Data Management	
7.	The SIEM should provide a unified analytics interface that allows the same query language to Analyse both log data and raw packet data. Both raw, parsed and enriched data must be passed to the SIEM solution from the collectors. Processing of event data should be performed by parsers on the system. All parsers should be able to be modified and customized.	
8.	Devices can be monitored without agents via SSH, telnet WMI, JMX and PowerShell. Solution should support more than 350 integrations out of the box for monitoring the complete environment. Kindly provide documentation for the same.	
9.	Ability to integrate with Threat Intelligence (TI) feeds with support for STIX/TAXII	
10.	The solution should provide out of the box reports, at no additional charge, for PCI-DSS, HIPAA, SOX, NERC, FISMA, ISO, GLBA, GPG13, and SANS critical controls	



11.	The solution should have the ability to export and import dashboards, reports and rules. Also, solution should be able to create custom reports and dashboard as per requirement with role-based access control.	
12.	SIEM solution should support Single Sign On, SAML 2.0 and AD for enterprise authentication with role-based access control.	
13.	The solution should provide an integrated SOC dashboard and Incident analysis system that could provide a single view into all the analysis performed across all the different data sources including but not limited to logs, endpoint and packets. The Tool should have role-based access control mechanism and handle the entire security incident lifecycle.	
14.	Solution should analyze following application types: a. Web pages: HTML, HTTP--GET, HTTP--POST, HTTP--RESP b. Email and attachments: EML c. Document files: DOC, DOCX, XLS, XLSX, PPT, PPTX, PDF, WPD d. Images: JPG, BMP, GIF, PNG e. Config, system files: REG, DLL, CONF, CPP, ELF, EXE f. Compressed archives: ZIP, GZIP, RAR	
15.	Should be able to provide complete packet-by-packet details pertaining to one or more session of interest including Session replay, page reconstruction, image views, artefact & raw packet and object extractions.	
16.	Should store RAW packet DATA and normalized packet data and correlate that with logs in the correlation engine to find threats such as: 1) Payload based attacks 2) Encrypted tunnels 3) Extract exe/pdf/JavaScript/malicious files for analysis 4) Full session reconstruction 5) Uncompress http payload and detect malicious content on the fly	
17.	Should support data obfuscation and data privacy requirements. The solution should support to identify PII/sensitive information in popular protocols to detect data exfiltration. Also, the appliance should support data at rest encryption capabilities to mitigate theft risk.	
18.	The proposed solution should automatically resolve the unsupported device events by extracting known / key meta [IP Address, Username, Email address etc.] of an event without having to write the parser.	
19.	The Solution should have a centralized management for various components from a single GUI.	



AAA Server (NAC)

S No.	Specifications	Compliance (Yes/ No) with comments, if any
1.	Dedicated redundant Hardware Appliances. Should be supplied with 20000 AAA (Endpoint licenses)	
2.	Should be able to integrate with all makes of manageable network devices which are capable of supporting open standards-based protocols required for NAC operation	
3.	Must provide Network Access Control and visibility in single pane of glass for the entire infrastructure from day 1 spread across multiple Network Locations / Zones	
4.	Must allow system-level operations such as device discovery, event management, logging and application maintenance to be performed centrally.	
5.	Must provide the capabilities to modify, filter, and create your own flexible views of the network.	
6.	Must allow for graphing or viewing in table format and multiple OIDs that are user selectable.	
7.	Must allow scheduled events or tasks that the user can perform behind the scenes or schedule an event for another time in the future.	
8.	Must provide a utility to view and select MIB objects from a tree-based representation and include a compiler for new or third-party MIBs.	
9.	Must support RADIUS and LDAP Authentication for users/devices of the application.	
10.	Must have SNMP MIB compile capability to integrate any SNMP compliant device	
11.	When integrated with security devices such as IDS it must be able to isolate and quarantine the attacker without disruption to other users, applications and business critical systems	
12.	When integrated with security devices such as IDS it must be able to dynamically deny, limit or change the characteristics of the user's access to the network	
13.	Must provide a web interface that contains reporting, dashboards, troubleshooting and monitoring tools.	
14.	Must enable diagnosis of network issues and performance through real-time NetFlow analysis.	
15.	Must provide port level analysis capability	
16.	Must provide customizable reports	



17.	Solution should have capability to integrate with IoT solutions	
18.	Should have the capability to integrate with 3rd party vendors	
19.	If required, solution should be deployable in a distributed mode with different units for Different Locations for ease of management, Authorization and Policy Control. All individual Units should be integrated to one central Control Unit with hierarchical management access or role-based access like admin, operator etc.	
20.	Solution must utilize standards-based authentication mechanisms enabling non-intelligent devices the ability to connect to the network and receive the proper network services.	
21.	Should be able to gather Detailed identity and access information with OS and device fingerprinting for Blackberry, iOS, Android, Windows, Linux and more	
22.	Should be able to perform posture check for compute end points (Windows & MAC) for OS health for parameters like Registry Keys, allowed process, AV or Firewall Enabled etc. Should include licenses towards posture check for the above mentioned no. of devices.	
23.	Detect and protect any device with IP address without the need for a client application on each endpoint including detection of VoIP phones, printers, wireless devices, machinery, cameras, sensors etc.	
24.	Support event logging of Device Access and Activity Time Stamp	
25.	Device search functionality by attributes such as user name / OS type / IP- MAC address / System Name	
26.	Must support automated onboarding and self-registration of all IP end points. Must also offer the option of sponsorship capabilities to validate guest registration without involvement of IT staff.	
27.	Must Support location-based Registration portals to redirect Users entering through common location to different portals for different Network Zones	
28.	Must support automated context-based policy provisioning of network services for mobile devices	
29.	Solution must support User Validation as well as device Validation for two factor security against an AD or LDAP database. Support integration with multiple LDAP / AD servers	
30.	Ipv6 support for NAC implementation in networks with Ipv6 end systems- preferred.	
31.	Support Management Access Authentication and Authorization for Network Device Access	
32.	Support Manipulation of Radius Attributes for Authentication as well as Radius Accept	
33.	Must be able to create correlated topology based on LLDP, SNMP, L2 and L3 protocol connectivity hierarchy	



34.	Must allow system-level operations such as device discovery, event management, logging and application maintenance to be performed centrally.	
35.	Must support RADIUS or LDAP Authentication for users of the application.	
36.	Must be able to define policies to rate-limit bandwidth, throttle the rate of new network connections, prioritize based on Layer 2 or Layer 3 QoS mechanisms, apply packet tags, isolate/quarantine a particular port or VLAN, and/or trigger pre-defined actions.	
37.	Must provide a tool to search and locate the physical location of connected devices and end users, quickly and easily.	
38.	Must allow IT administrators to easily define a number of pre-configured network policies, and designate select personnel to activate/deactivate these policies as appropriate	
39.	Must be able to provide a centralized history of firmware and configuration changes and other inventory management operations made to a device.	
40.	Must be able to download text-based (ASCII format) configuration templates to one or more devices.	
41.	Must provide capability to bind together the username, IP address and MAC address, and physical port of each endpoint for forensic analysis	
42.	Must provide an interface with troubleshooting and monitoring tools (Ping / Traceroute, SSH, Telnet, Http/s)	
43.	Must provide event logs for the entire infrastructure of Network devices	
44.	Must enable diagnosis of network issues and performance through real-time Flow analysis (sflow / Netflow / jFlow)	
45.	Must provide user customizable reports creation	
46.	Must be able to interact with network security devices and push template based automated response to security events and thus remediating real time threats	
47.	Must provide open XML APIs for integration with third party applications.	
48.	Must support the ability to monitor end-system events and view the health results from an end-system's latest assessment scan.	
49.	Must provide easy-to-use dashboards and detailed views of the health of the end systems attached or trying to attach to the network.	
50.	Must provide the ability for analysts to be able to easily tailor the dashboard views to present the information in their preferred format.	



51.	Should be capable of reporting for historical and real-time data. Should be equipped with Custom report designer to meet the needs of specific data attributes and periodic email of the same to relevant Administrative team.	
52.	VLAN steering via RADIUS IETF attributes and VSAs	
53.	VLAN steering and port bouncing via SNMP	
54.	Ability to perform caching of MAC address post guest authentication to avoid the need for guest to re-authenticate during the period of their visit (3G like user experience after first authentication via captive portal).	
55.	Policy model should support incorporation of several contextual elements including identity, endpoint health, device, authentication method & types, and conditions such as location, time, day, etc.	
56.	AAA framework must allow for the complete separation of Authentication and Authorization sources. For example, authentication against Active Directory but authorize against an external SQL database.	
57.	All external facing interfaces are programmable, which means APIs are available to extend the system to support different authentication protocols, identity stores, health evaluation engines and port and vulnerability scanning engines.	
58.	The solution Must be an easy-to-deploy hardware platform that utilizes identity-based policies to secure network access and includes an integrated set of capabilities bundled under one policy platform:	
	• Built-in guest management and device/user onboarding	
	• Web based management interface with Dashboard	
	• Reporting and analysis with custom data filters	
	• Data repository for user, device, transaction information	
	• Rich policies using identity, device, health, or conditional elements	
	• Deployment and implementation tools.	
59.	Must support flexible licensing model based on required functionality (i.e. Profile, Onboard, Posture, Guest Access).	
60.	Correlation of user, device, and authentication information for easier troubleshooting, tracking etc.	
61.	Platform must be deployable in an out-of-band model and support for clustering with N+1 redundancy model.	
62.	Flexibility to operate all features/functions on any appliance in the cluster.	
63.	Web-based, interface that includes several productivity tools such as a configuration wizard and preconfigured policy templates.	



64.	Support any type of networking equipment (wired, wireless, VPN) and a variety of authentication methods (802.1X, MAC auth, Web auth).	
65.	Ability to take advantage of a phased implementation approach by starting with one element of access management (role based) and later incorporating added security measures (endpoint health).	
66.	Must incorporate a complete set of tools for reporting, analysis, and troubleshooting. Data from access transactions can be organized by customizable data elements and used to generate graphs, tables, and reports. Must correlate and organize user, authentication, and device information together.	
67.	Solution must have fully integrated support for Microsoft NAP allowing health and posture checks on Windows endpoints without the need to install an agent.	
68.	Agent-based enforcement – bouncing a managed interface and sending custom messages. Also, control access to different networks via whitelist and blacklist. License as per requirement.	
69.	Must be able to join multiple Active Directory domains to facilitate authentication.	
70.	Event Management: There has to be a feature of Management Module/ tool to establish link with EMS platform & SIEM.	

Network load balancer

S No.	Specifications	Compliance (Yes/ No) with comments, if any
A	Architecture	
1	The Load Balancer shall distribute traffic efficiently while ensuring high application availability. It shall monitor server health to determine that application servers are not only reachable but alive. If the Load Balancer detects issues, it shall automatically remove downed servers from the server pool and rebalance traffic among the remaining servers. It shall be appliance based and shall facilitate multi-vendor, multi-application environment and shall support third-party products	
2	The Load Balancer shall deliver the high availability required by modern Data Centers. It should support Active/Passive or Active / Active HA configurations. The Load Balancer shall automatically synchronize configurations between the pair and automatically failover if any fault is detected with the primary unit	
3	The load balancer shall be built on high-performance hardware, designed for Data Centers. It shall deliver application traffic of all	



	types and scalable to meet the throughput needs of the most demanding applications	
4	The Load Balancer shall support offloading of SSL connections and should support Certificate format such as “OpenSSL/Apache, *.PEM”, “MS IIS, *.PFX”, and “Netscape, *.DB” etc. or better.	
5	Should provide support for cache rules/filters to define granular cache policies based on cache-control headers, host name, file type, max object size, TTL objects etc.	
6	The Load Balancer Shall have full traffic control and be able to route requests to servers based on region, device, browser, or a number of other factors. This enables organization to deliver customized application responses to users.	
7	Should be high performance purpose built next generation multi-tenant hardware with NFV and SDN support. Platform should support multiple network functions including Server Load balancing, Application Security, Secure remote access and AAA network functions with dedicated hardware resources for each virtual instance.	
8	Appliance should provide real time Dynamic Web Content Compression to reduce server load and solution should provide selective compression for Text, HTML, XML, DOC, Java Scripts, CSS, PDF, PPT, and XLS Mime types.	
	Performance	
9	The server load balancer should deliver 160Gbps L4 Throughput	
10	The server load balancer should have dedicated SSL card to support Minimum 76,000 ECC TPS (ECDSA-SHA256) & 110,000 SSL TPS 2K Keys.	
11	The sever load balancer should support Minimum 512GB RAM, 4TB HDD and should have minimum 16x10GbE SFP+ ports, 4x40GbE QSFP+ ports. Two 1G Copper dedicated management interface	
B	Features required for Load Balancer	
12	Local Application Switching, Server load Balancing, HTTP, TCP Multiplexing, Compression, Caching, TCP Optimization, Filter-based Load Balancing, Transparent Deployments, Content-based Load Balancing, Persistency, HTTP Content Modifications, QoS, Support for connection pooling to TCP request, Support for distributed denial-of-service (DDos) protection	
	Security features	
13	Solution should support DDos attacks from day one like Protocol Attack: SSL invalid packet, SSL handshake attack, SSL renegotiation, HTTP invalid packet attack – Application Attacks: HTTP slow attack, HTTP flood attack, long form submission, Challenge Collapsar (CC), Hashdos, DNS NXDomain flood – Network Attacks: SYN flood, ICMP flood, Ping of Death, Smurf, IP option – HTTP & DNS ACL rules, ACL blacklist – Monitoring and Logging: PUSH/ ACK flood, FIN/RST flood,	



	Connection flood, UDP flood – Machine learning of traffic patterns and automatic configuration of HTTP/DNS thresholds to defend against anomalous traffic	
14	Should support machine authentication based on combination of HDD ID, CPU info and OS related parameters i.e. mac address to provide secure access to Data Center resources.	
15	Supports SAML secure application access – Supports web single sign-on (SSO) – Serves as a SAML SP (service provider)	
16	Solution should capable of blocking access through anonymous services (TOR, VPN, open proxies, anonymizers)	
17	Solution Must Prevents modifying the form data and cookies on the client side by controlling their invariability between the request and the response with Cookie Signing, Form Signing, AJAX requests Signing.	
C	Load Balancer Features	
18	It should have the capability of Rate shaping & QoS Support to optimize and handle heavy Layer 4 through 7 traffic loads while delivering Latency Sensitive Applications	
19	It should support integrated antivirus module for scanning of malicious content in files uploads and should be able to integrate with the proposed on-premise Anti-APT, SIEM, DLP solution to scan for zero-day malwares from Day 1	
D	High Availability	
20	It should have feature of Global Server Load Balancing between different Data Centers without any additional license, from Day1.	
21	The solution should provide comprehensive and reliable support for high availability and N+1 clustering based on stateful session failover with Active-active & active standby unit redundancy mode. Also support Single System Image for Load Balancer Function to create a single VIP (single ADC instance) out of any number of dedicated, virtualized or virtual APV appliances to provide ultimate flexibility in scaling out.	

Multi-Factor Authentication (with Finger print biometric and hard token devices) at all workstations

Miscellaneous- Virtualization, OS for servers, etc.

Virtualization licensing socket Base -

- 77 Physical Servers using two sockets in total 154 (77*2) quantity required for virtualization servers
- 18 physical servers using two sockets in total 36 (18*2) quantity required for security of DMZ virtualization servers

Microsoft Windows OS for Virtualization Servers



- 73 Physical Servers each having 4 VM's (Total 308 VM's). For each server we need to consider license for 40+40=80 cores (5 licenses of 16 cores)
- Windows Server Data Center Edition 64-bit latest version

The proposed virtualization solution should support mobile device management of minimum 320 devices i.e. mainstream versions of Windows CE, Windows 10, Android, iOS along with zero day support for any new Windows, Android, iOS OS upgrade versions.

Police Department should be able to centrally push all policies and send notifications to all devices and should provide capability to support multiple active directories, exchange, and other integration services as required by department.

Compute Virtualization			
S No.	Specifications		Compliance (Yes/ No) with comments, if any
1.	Virtualization Solution	Sits directly on the virtualization server hardware with no dependence on a general-purpose OS for greater reliability & security and should be Leaders/challengers in the Gartner's Magic Quadrant latest.	
2.	Guest OS Support	Windows client, Windows Server, Linux (at least Red Hat, SUSE, Ubuntu and CentOS, Solaris x86) etc. OS vendor should provide certification and support for hypervisor.	
3.	Live Migration	Live Virtual Machine migration between different generations of CPUs in the same cluster and without the need for shared storage option and long distances from one site to another with no disruption to users or loss of services, eliminating the need to schedule application downtime or business downtime.	
4.		Live migration of VM disk from one storage array to another without any VM downtime. Support this migration from one storage protocol to another eg: FC, NFS, iSCSI, DAS.	
5.	Availability	Proactive High availability capability that utilizes server health information and migrates VMs from degraded hosts before problem occurs, should optimize power consumption by turning off hosts during the reduced demand	
6.		Migration of VMs in case one server fails all the Virtual machines running on that server shall be	



		able to migrate to another physical server running same virtualization software.	
7.		It should support affinity and anti-affinity rules to set constraints that restrict placement of a virtual machine to a subset of hosts in a cluster and to keep virtual machines paired or separated with capability of native backup and restoration of the virtualization management server.	
8.		Solution should have single reboot to dramatically reduce the upgrade times by skipping a host reset and help to reduce patching and upgrade times by rebooting the hypervisor without rebooting the physical host, skipping time- consuming hardware initialization	
9.		Zero downtime, zero data loss and continuous availability for the applications running in virtual machines in the event of physical host failure, without the cost and complexity of traditional hardware or software clustering solutions.	
10.	Performance	Add CPU, Memory & devices to virtual machines on the fly when needed, without disruption or downtime of working VMs for both windows and Linux based VMs.	
11.		Create a cluster out of multiple storage data stores and automate load balancing by using storage characteristics to determine the best place for a virtual machine's data to reside, both when it is created and when it is used over time.	
12.		Support for persistent memory, exposing it as block storage or as memory, to enhance performance for new as well as existing apps should provide configuration compliance reports/alerts/dashboards for the underlying hypervisor platform	
13.		Should be able to dynamically allocate and balance computing capacity across collections of hardware resources aggregated into one unified resource pool with optional control over movement of virtual machines like restricting VMs to run on selected physical hosts.	



14.		The Solution should offer virtual load balancers with L4–L7 load balancer with SSL offload and pass-through, server health checks	
15.		Should support network and storage QoS to ensure performance on per VM basis	
16.	Security	VM-level encryption with no modifications in guest OS to protects unauthorized data access both at-rest and live vMotion and also provides secure boot for protection for both the hypervisor and guest operating system by ensuring images have not been tampered with and preventing loading of unauthorized components.	
17.		Solution should protect every Virtual Machine with a stateful distributed firewall integrated into the host architecture and provide near line rate firewall throughput.	
18.		Solution should enable creation of security groups and security policies/ rules based on constructs like machine name, OS type, IP address, Logical Switches, Security Tags etc.	
19.		The security policies should follow the Virtual Machines as it moves within and between the virtual infrastructures so that there is no need of creation of security policies again for the applications once they move inside and across the Datacenter.	
20.		Integration of 3rd party endpoint security to secure the virtual machines with offloaded antivirus, antimalware, firewall and hips solutions without the need for agents inside the virtual machines.	
21.		Solution should support TPM 2.0 hardware modules and adds a virtual TPM device to shield guest OS from Operator or in-guest attacks	
22.		The security policies in the virtualization layer must be tied to the application, which means whenever any application is moved from one virtualized server to another, even between different VLANs, the security policies should follow the application and there should be no need to redefine the security policies for the application at the new location. Also, when the application is deleted, all the security policies	



		related to the application should also be removed.	
23.	Storage support	Support boot from iSCSI, FcoE, and Fibre Channel SAN. Integration with Storage API's providing integration with supported third-party data protection, multi-pathing and disk array solutions. Solution should have capability similar of Virtual Volumes which enables abstraction for external storage (SAN and NAS) devices making them Virtualization aware and it should allow common management across storage tiers and dynamic storage class-of-service automation via a policy-driven control plane	
24.	Management	The solution should offer converged visibility and analytics that tie together compute, network, storage and security and provide Physical to Virtual Correlation and troubleshooting, report the amount of East-West, North-South, Internet, virtual machine to virtual machine, virtual machine to physical traffic within the datacenter Monitoring of OS level resources (CPU, disk, memory, network) for any OS and physical hardware resources of the hosts. These monitoring capabilities combined with patented analytics should extend operational visibility and proactive management capabilities across OS.	
25.		The solution should offer comprehensive flow assessment and analytics and security groups and firewall rules suggestion for the purpose of implementing a zero-trust security within the data-center, provide a converged view of virtual and physical network, provide end to end topological view of path between two virtual machines. It should support leading hardware vendors as well. The solution shall provide the ability to identify and report on over-sized, under-sized, idle and powered-off virtual workloads such that the environment can be right-sized and resources can be reclaimed	



26.	Virtual Switch	Span across a virtual Datacenter and multiple hosts should be able to connect to it. This will simplify and enhance virtual-machine networking in virtualized environments and enables those environments to use third-party distributed virtual switches.	
27.		The solution should be capable to of multisite networking (Layer 2 extension) irrespective of underlying physical topology for active-active DC & DR purposes, container network and security for container to container L3 networking and micro segmentation for micro services etc.	
28.		The solution should support reduction in Recovery Time Objective when the VMs are brought up from DC to DR, without the need to redo the IP-addresses, the default gateway router should be stretched across data centers, also the firewall policy should also be applied across DC & DR automatically, so that when Virtual Machines move from DC to DR there is no need to reconfigure the firewall policies	
29.		In-built enhanced host-level packet capture tool which will provide functionalities like span, rspan, erspan and will capture traffic at uplink, virtual switch port and virtual NIC level. It should also be able to capture dropped packets and trace the path of a packet with time stamp details.	
30.		The Solution should provide distributed routing (OSPF & BGP), VXLAN based logical virtual switching, NAT function, server load balancer, Software L2 bridging to physical environments, L2 & L3 VPN, site-to-site IPSEC VPN services, distributed L2-L4 stateful firewall at vNIC level.	
31.	VM based Replication	Efficient array-agnostic replication of virtual machine data over the LAN or WAN. This Replication should simplify management enabling replication at the virtual machine level and enabling RPOs as low as 15 minutes.	
32.	Operations Management	Solution should provide integrated smart alerts for health, performance and capacity degradation to identify building performance problems before they affect end users, should be able to collect and analyze all types of	



		machine-generated log data, for example, application logs, network traces, configuration files, messages, performance data and system state dumps.	
33.		Solution should provide capacity analytics to identify over-provisioned resources so they can be right-sized for most efficient use of virtualized resources and “What If” scenarios to eliminate the need for spreadsheets, scripts and rules of thumb to provide automated root cause analysis and should allow connecting to data-center ecosystem components e.g., operating systems, applications, storage arrays, firewalls, network devices, etc., providing a single location to collect, store, and analyze logs at scale	
34.		It should include proactive smart alerts with self-learning performance analytics Capabilities with Customizable Dashboards, Reports and Views to provide real-time insight into infrastructure behavior, upcoming problems, and opportunities for efficiency improvements	
35.	Disaster Recovery Automation	Solution should provide DR automation solution delivered from virtualization manager console for automated failover, failback and recovery of application VMs in proper sequence to other data center with single click	
36.		Solution should provide solution to perform non-disruptive DR drill/testing of recovery plan for full and selected applications every six months without impacting production applications running in primary environment.	
37.	OEM Support	Direct OEM L1, L2, L3 24x7x365 days with unlimited incident support and 30mins or less response time including the unlimited upgrades and updates. For 5 years	

4.10 Field Devices

Functional requirements and essential needs

A. Cameras and sensors

- a) The camera layer will behave to help the city administration gather information about the ambient city and monochrome city conditions or capture information from the edge level devices.



- b) The cameras will serve as the eye of policing across the Delhi NCT. The cameras must ensure faster convergence, stable network, utilizing multipath, Quality of experience and handover of traffic to multiple users, segregation of different users / Police Stations at network layer.
- c) The cameras need to work on 24 Hours throughout the year during all weather conditions and shall also provide continuous multi-cast seamless feeds from the installed locations with wide Field of View to capture all coverage in the Data Center.
- d) Each camera will work on high bandwidth (average 5 Mbps per camera approximately with H.265 compression) with robust infrastructure to provide stable and sharp streaming at the video wall layer.
- e) The output of the camera feeds will be stored directly at the Data Center through redundant connectivity measures adopted over multiple ring and mesh topologies to connect all locations.
- f) The multi-casted field cameras will pool in the entire lot of feeds on a multi-cast enables MPLS cloud of the identified cloud and broadcast the streams at all Police Stations, District Offices and PHQ, based upon the respective jurisdictions defined in an operational rule-based network engine.
- g) The cameras will be the combination of 6121 Fixed Box cameras (4 MP), 2246 Pan-Tilt-Zoom cameras (4 MP) and 1622 Automatic Number Plate Recognition Cameras with IR illuminators (2 MP).
- h) The fixed box cameras should have sharp, instant and concentrated Field of View as desired. It should have Max Image Resolution 2688 X 1520 or better and Lens 2.8 to 12mm lens, Auto/DC/P-IRIS, or better varifocal motorized.
- i) FB Camera should have more than 120dB Wide Dynamic Range to get better visibility in extremely bright and dark environments. The camera should be effectively eliminating glares and managing over-exposure conditions.
- j) The monochrome city conditions during night must be captured within minimum 100m distance with supreme night visibility. The illumination should have capability of varied angle long range. Which automatically adjust IR lighting intensity to ensure better identifications during night. The quality of the feeds must maintain with the desired H.265 codec compression at 25/30 FPS.
- k) The PTZ cameras must have adequate widespread Field of View, which will be regulated and controlled from the C4i. The PTZ cameras must have Optical Zoom 30X or better and Digital Zoom 16X or better. There will be provision of PTZ cameras to be deployed for entry/exits of public places, dark areas in consultation with Delhi police.
- l) The ANPR- Vehicle Surveillance cameras must ensure highly reliable results of min 90% + capture and OCR accuracy min 90% in both day and night. The ANPR- Vehicle Surveillance camera has to conduct H.265 codec compression at 25/30 FPS. There will be provision of external IR illuminator with required accessories.



- m) All cameras must be equipped with capabilities to monitor and provide alert during instances of vandalism, theft, etc. The housing should be vandal-proof with IP-67 weather-proof and IK 10 enclosure.
- n) The cameras will be equipped with embedded cyber security measures and should not be classified with GB28181, GB/T28181-2011 standards which primarily facilitate the OEM to access the camera from anywhere globally and ingest outside videos in the network.
- o) The camera should be capable to manage smart of the moving objects to minimize the effective bandwidth requirement and reduce storage space requirement.
- p) The camera should have the capability to rotate the aspect ratios to adjust the image from x:y to y:x formats as required for the Video Wall.
- q) Safe city Logo and Delhi Police logo will be embossed/etching (in colour) in each camera

B. Civil and Hardware

Supply & Installation of Camera Infrastructure:

Based on detailed field survey as mentioned above, MSI will ensure the supply, install and commission the surveillance and monitoring systems at the identified locations and also undertake necessary work towards its testing. MSI will ensure the industry leading practices during the implementation phase w.r.t positioning and mounting the cameras, poles and junction boxes. MSI will ensure that, check-points that need to be adhered by the MSI while installing / commissioning cameras are as follows:

- a) Ensure that surveillance and monitoring objective is met while positioning the camera such that the required field of view is being captured as finalized in field survey
- b) Ensure that camera is protected from on field challenges of weather, physical damage and theft.
- c) Make proper adjustments so as to have the best possible image / video captured.
- d) Ensure that the pole is well placed for vibration resistance adhering to the road safety norms.
- e) Deployment of Collisions preventive barriers around the junction box & pole foundation in case it's installed in collision prone place.
- f) Deployment of Appropriate Safe City logo of Delhi Police on poles and junction boxes, to warn mischief mongers against tampering with the equipment at the junction.
- g) Appropriate unique code is to be given to each pole, which will be painted on respective pole.



C. Installation of Poles/Cantilevers

- a) The MSI will ensure that all installations are done as per standards with final check & satisfaction of the Delhi Police. For installation of CCTV Cameras, PTZ Cameras, Public Address System, etc. MSI will ensure that they shall provide appropriate poles & cantilevers and any supporting equipment.
- b) MSI to supply, install, configure and integrate surveillance cameras at the identified locations and thereafter undertake necessary work towards their commissioning.
- c) MSI will ensure that the poles erected to mount cameras are good, both qualitatively and aesthetically (the drawings have to be pre-approved by the Delhi Police).
- d) MSI will ensure the industry leading practices while positioning and mounting the cameras and ensure that the pole / mast implementation is vibration resistant. Arrangements for bird scare spikes on top of camera shall be made to prevent birds from sitting on top of camera box.
- e) The poles shall be installed with base plate, pole door, pole distributor block and cover.
- f) MSI will ensure the base frames and screws shall be delivered along with poles and same will be installed.
- g) MSI will ensure, in case the cameras need to be installed beside or above the signal heads, suitable stainless-steel extensions for poles need to be provided and installed, so that there is clear line of sight.
- h) MSI will be responsible to undertake required structural analysis regarding the regulated load conditions and considering the respective wind load while installing the poles / cantilevers for cameras
- i) MSI will provide structural calculations and drawings for the approval of Competent Authority. The design shall match with common design standards as applicable under the jurisdiction of Delhi Police.
- j) MSI will make sure that component-wise certifications by Competent Authorities (for safety security, IT and Non-IT parameters) for ensuring adequate performance levels for the project.
- k) MSI will ensure that the OEM will be required to provide Manufacturing Authorization Form/ Certificate with the Country of Origin details for every product being provided as a part of Project requirement.
- l) MSI will ensure that OEM will submit Factory Acceptance Certification for all its products.
- m) The certification of the field equipment like poles for successful installation in terms of seismic strength, durability, etc. and the building floor strength a third-party inspection can be conducted through Government/ PSU Authorized Institutions/agencies like CPWD, IIT- Delhi, IIT-Powai, IIT-Kharagpur, PDIL, EIL, RITES etc. Certifications for project components are incorporated in **para 4.17 for Chapter 4 of this RFP**.



- n) MSI will coordinate with concerned authorities / municipalities for installation to expedite the work.
- o) Poles and cabinet shall be so designed that all elements of the field equipment could be easily installed and removed.
- p) MSI will ensure the physical look of the installation area returns to neat & tidy conditions after installation of poles, cantilevers etc. The placement shall be designed keeping in mind the normal flow of vehicular traffic and pedestrian movement is not disturbed.
- q) The indicative drawing of pole and cantilever with foundation work is provided below:

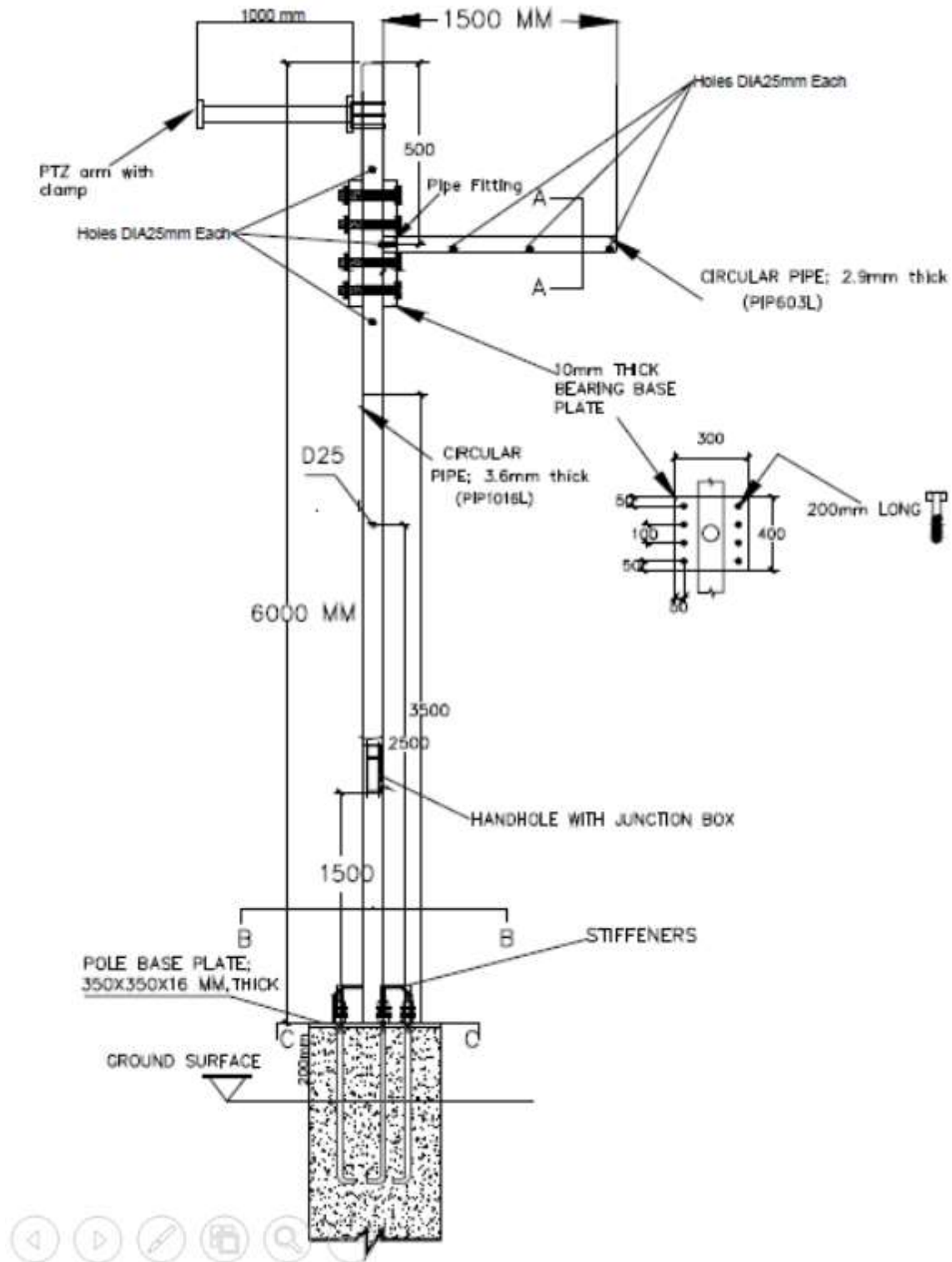


Figure: Indicative drawing of pole and cantilever

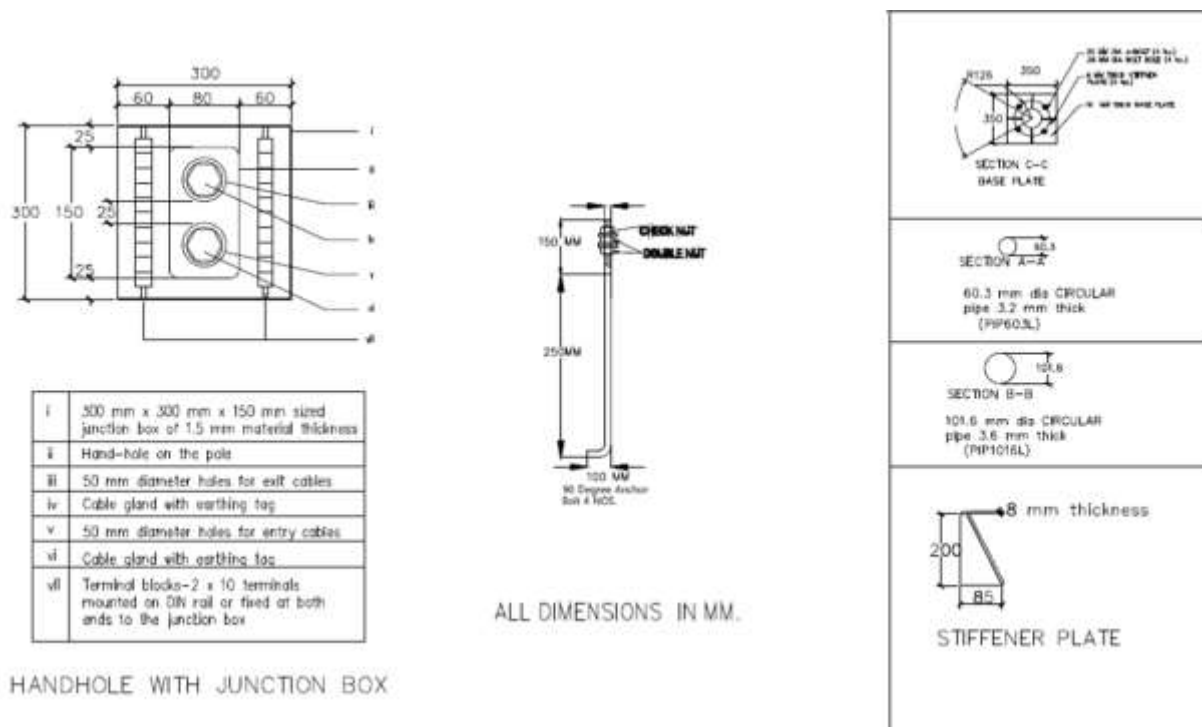


Figure: Top View of Pole on Field

D. Outdoor Cabinets / Junction Boxes

- Each location shall be fitted with outdoor cabinets dimensioned to host all equipment necessary to operate surveillance systems in this project.
- MSI will reserve additional room in the location controller cabinet to accommodate the future system requirements.
- The size of outdoor cabinet / Junction Boxes shall be sufficient to house all the system components, which may be installed at the location or nearby. Ingress Protection should be Outdoor – IP55 or better for Junction Box to be dustproof and impermeable to splash-water. It shall be suitable for Delhi's environmental conditions and it shall have provision for two types of cabinet as follows:
 - Power cabinet:** This cabinet shall have the provision to house the electricity meter and the redundant power supply system
 - Control cabinet:** This cabinet shall house the controllers for all the field components at that particular location e.g. ANPR, PTZ, Fixed cameras etc.
- Internal cabinet cabling shall be designed for an easy connection and disconnection of the equipment and power
- The cabinets shall be of robust construction and shall include 3-point spring loaded locking mechanism with Pad lock and protective cover (Allen key) to prevent unauthorized access to the field equipment
- Temperature and Humidity Control: All enclosure compartments shall be equipped with a natural convection air circulation system via provision of air circulation filters that shall not require maintenance and shall allow free circulation of air inside the enclosures to prevent overheating as well as the build-up and effects of humidity and heat, without permitting the entry of elements that might endanger system operation



- g) MSI will ensure to place all the hardware inside the junction boxes that could withstand temperatures prevalent in Delhi throughout the year
- h) MSI will ensure security of Junction Box from vandalism & theft by using complete welded structure with fixed rear and side panels.

E. Civil and Electrical Works

- a) MSI will be responsible for carrying out all the civil & Electrical work executed and setting up all the field components of the system including:
 - Preparation of concrete foundation for MS-Poles & cantilevers
 - Laying of GI Pipes (B Class) complete with GI fitting
 - Hard soil deep digging and backfilling after cabling
 - Soft soil deep digging and backfilling after cabling with added rocks/ coarsen
 - Chambers with metal cover at every junction box, pole and at road crossings
 - Concrete foundation from the Ground for outdoor racks, if required
- b) MSI will provide distance from junction box to the cameras through the aggregation point. Since this component has dependency on approval from local authorities, MSI will also plan this requirement well in advance & submits the application to the concerned electricity City distribution agency with requisite fees, as applicable
- c) MSI will carry out all the electrical work required for powering all the components of the system
- d) Electrical installation and wiring shall be under standard guidelines to the electrical codes of India
- e) MSI will make provisions for providing electricity to the cameras (ANPR, PTZ, and Fixed) via SJB (Surveillance Junction Box), housing the UPS/SMPS power supply, with minimum backup in coordination with Delhi Police and the Electrical Department. The power will be fetched from the nearby transformer as guided by the Electrical Department.
- f) For the Fixed Box cameras, MSI will provision for drawing power through PoE+ (Power over Ethernet) and for the ANPR cameras MSI will provision for drawing power through POE, POE+, while PTZ cameras shall be powered through dedicated power cable laid separately along with STP/SFTP cable if additional power is required.
- g) Registration of electrical connections at all field sites shall be done in the name of the Delhi Police.
- h) Electricity meters will reside inside the power cabinet as per BSES/NDPL guidelines.



- i) The power connections (electrical meters) charges will be paid by MSI and the recurring power charges will be borne by the Delhi Police from Go-Live phase respective to each phase. Appointed MSI will coordinate the execution of connections with Electrical Department.

F. Earthing and Lightning Proof Measures

- a) MSI will comply with all the Technical Specifications taking into account lightning-proof and anti-interference measures for system structure, equipment type selection, equipment earthing, power and signal cable laying. MSI will describe the planned lightning-proof and anti- interference measures in their Technical Bid.
- b) Corresponding lightning arrester shall be erected for the entrance cables of power line, video line, data transmission cables
- c) All interface board and function board, interfaces of equipment shall adopt high speed photoelectric isolation to reduce the damage to integrated circuit CMOS (Complementary metal-oxide-semiconductor chip due to the surge suppression
- d) Install the earthing devices for the equipment, including lightning earthing, protection earthing and shielded earthing. All earthing shall meet the related industry standards
- e) The earthing cable shall be installed in a secure manner to prevent theft and shall be rust proof. Earthing down lead and the earthing electrode shall be galvanized.

G. UPS for field devices

- a) As an acute necessity of the power backup arrangement for uninterrupted operations of field devices such as switches, cameras Gun-shot detection sensors, etc. the provision of adequate capacity UPS is recommended.
- b) The UPS should be capable to provide 60 min. of power backup in field which will be placed inside the Junction Box with the set of batteries.
- c) A UPS of 1 KVA, 2 KVA load for every pole mounted and floor mounted Junction Box respectively is considered.

A. Field Devices- Technical Requirements and Compliance Sheet for MSI (to provide compliance report with the bid)

A. Outdoor Fixed Camera - 4MP

Sr. No	Parameter	Specification	Compliance (Yes/No) with comments, if any
1.	Image sensor	1/3"Progressive Scan CMOS or better	
2.	Max Image Resolution	2688 X 1520 or better	
3.	Lens	2.8 to 12mm lens, Auto/DC/P-IRIS, or better varifocal	
4.	True Day and Night	Yes	
5.	Wide Dynamic Range	True WDR of 120dB or better	
6.	Minimum Illumination / Light Sensitivity	Color: 0.01Lux @f/1.6 or better, B/W: 0.05Lux @f/1.6(IR on) or better	



	IR Filter		
7.	IR Filter	Automatic Built in IR Cut filter	
8.	IR Distance	IR distance-50 Mtr. Or better	
9.	Shutter Speed	Auto/Manual, 1/3~1/ 30000s or better	
10.	Video Compression	H.264, H.265 (Dynamic group of pictures) or better	
11.	Resolutions and frame rates (H.265)	Minimum 4MP with 25/30fps or Better	
12.	Video Streams	Individually configurable minimum 03 video streams	
13.	Streaming Method	Unicast, Multicast, Broadcast support along with multi stream support	
14.	Local storage	SD Card Slot with 128 GB or better Support with provided 128 GB card	
15.	Image Settings	Colour, Brightness, Sharpness, Contrast, White balance, Backlight compensation, Image Mirroring, Text and image overlay, BLC/HLC/ AGC required	
16.	Supported Protocol	HTTP, HTTPS/SSL/TLS, TCP, ICMP/RTSP, RTP, UDP, IGMP, RTCP, SMTP, FTP, DHCP, UPnP/ARP/DNS, SMTP, Ipv4/Ipv6.	
17.	Ethernet Port	RJ-45 (10/100Base-T) Mbps or Better	
18.	ONVIF	Profile S, G / Profile S, G, T	
19.	Operating Temp	-30 °C ~ 60 °C, Up to Humidity 90%	
20.	HLC, BLC	Aut	
21.	IR – Internal/External	IR 50 meters to be considered Internal or external	
22.	Housing	IP 67 Rated IK 10 rated for outdoor use	
23.	Certifications	CE, FCC, UL/cUL, BIS, NEMA 4X	
24.	Power Requirement	POE+	
25.	Mounting Accessories	For pole and surface mount with L/C Brackets	
26.	EMI EMC	Surge test (Level 4) as per IEC:61000-4-5(Level 4)	
27.	Audio	1 Channel Audio IN/ 1 Channel Audio Out or Built In MIC/ 1 Channel Audio Output, Support two-way audio (Optional)	
28.	MTBF	Min 100000 Hours or better	
29.	Defogger	Digital defogger/Defogger	



30.	Misc.	The Camera to be provided by the OEM/bidder should not be complying to GB28181, GB/T28181-2011 standards and there should be no option to activate or deactivate GB/T 28181 standards in the camera web page/settings.	

B. Outdoor PTZ Camera - 4MP, 30x Optical Zoom and Joystick control operations

Sr. No	Parameter	Specification	Compliance (Yes/No) with comments, if any
1.	Image sensor	1/3-in. CMOS & Minimum 4 MP	
2.	NUMBER OF PIXELS	2592 × 1520 (4MP)	
	(H × V)	30X or better	
3.	Optical Zoom	30X or better	
4.	Digital Zoom	16X or better	
5.	Min. Illumination	Color: 0.01 lux @f1.6 or better B/W: 0.05 lux (with IR on) @f1.6 or better	
6.	WDR	True WDR 120 db or better	
7.	Focal Length	4.5 mm – 135 mm or 4.3 mm - 129 mm or 4.8 mm - 144 mm or 6mm -180 mm	
8.	Max Aperture	F1.6 – F5.0	
9.	IR Distance	150 m or better	
10.	Defog	On/Off	
11.	PAN Travel	360° endless	
12.	TILT Travel	0 to 90°, auto flip 180°	
13.	Manual PAN Speed	Up to 180°/s or better	
14.	Manual TILT Speed	Up to 120°/s or better	
15.	Preset Speed	Pan: 240°/s; Tilt: 200°/s or better	
16.	Presets	256 or better	
17.	Image Rotation	Flip	
18.	Language support	English	
19.	Compression	H.264, H.265 or better	
20.	Streaming Capability	Individually configurable minimum 03 video streams (multicasting)	
21.	Frame Rate	25/30 FPS	
22.	Day and Night	Automatic, Color, Mono	
23.	White Balance	Auto / Manual /ATW/Indoor/Outdoor/Daylight lamp/Sodium lamp	
24.	Ethernet	RJ-45 (10/100Base-T)	



25.	Protocols	IPv4/IPV6, HTTP, HTTPS, FTP, SMTP, UPnP, SNMP, DNS, DDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, ICMP, DHCP	
26.	Streaming Method	Unicast, Multicast, Broadcast support along with multi stream support	
27.	Local Storage	SD Card Slot with 128 GB or better Support with provided 128 GB card	
		In the event of failure of connectivity to the central server the camera shall record video locally on the SD card automatically.	
28.	Power	24 VAC, 3 A ($\pm 10\%$), PoE+ (802.3at)/POE+	
29.	Mount	Wall / Pole Mount	
30.	Working Temperature	-30 °C ~ 60°C, up to Humidity 90%	
31.	ONVIF	Profile S, G /Profile S, G, T	
32.	Certifications	CE, FCC, UL/cUL, BIS, NEMA 4X	
33.	Mounting Accessories	For pole and surface mount with L/C Brackets	
34.	EMI EMC	Surge test (Level 4) as per IEC:61000-4-5(Level 4)	
35.	Housing	IP 67 Rated IK 10 rated for outdoor use	
36.	Audio	1 Channel Audio IN/ 1 Channel Audio Out or Built In MIC/ 1 Channel Audio Output, Support two-way audio (Optional)	
37.	HLC, BLC	Auto	
38.	MTBF	Min 80000 Hours or better	
39.	Defogger	Digital defogger/Defogger	
40.	Misc.	The Camera to be provided by the OEM/bidder should not be complying to GB28181, GB/T28181-2011 standards and there should be no option to activate or deactivate GB/T 28181 standards in the camera web page/settings.	

C. Outdoor Fixed ANPR Camera with IR Illuminator- 2MP

S.No.	Specification	Compliance (Yes/No) with comments, if any
1.	ANPR 2 Mega pixel camera / Sensor (True day and night): one per lane to be used to capture all vehicles including 2 wheelers. All types of number plates reflective type and standard type should be captured. Vehicle image also should be captured under all conditions. Image compression JPEG. Connectivity Ethernet.	



2.	Camera resolutions as needed by the solution to achieve highly reliable results of min 90% + capture and OCR accuracy min 90% in both day and night.		
3.	Color images for day, monochrome images for night		
4.	Global shutter sensor or rolling shutter sensor with Image stabilization		
5.	Lens: True Mega pixel or better, Day & night, IR corrected, lens.		
6.	Flash power should be sufficient to capture vehicle images also at night which can help ANPR Camera to capture retro reflective and non-reflective number plates.		
7.	Cameras should be able to detect Number plates of Vehicle upto 120 Kmph without any distortion in image.		
8.	Image sensor	1/2" Progressive Scan CMOS Sensor 2.0 megapixel or better CMOS.	
9.	Max Image Resolution	1920x1080 or better	
10.	Lens	C/CS or inbuilt with 5- 50 mm or better	
11.	True Day and Night	Yes	
12.	Wide Dynamic Range	True WDR of 120dB or better	
13.	Minimum Illumination / Light Sensitivity	Color: 0.001Lux @f/1.6 B/W: 0.001Lux @f/1.6 Or better	
14.	IR Filter	Automatic Built in IR Cut filter	
15.	IR Distance	IR distance- 80 Mtr. Or better; Inbuilt or External IR	
16.	Shutter Speed	1-1/30000s or better; slow & auto shutter operations	
17.	Video Compression	H.264, H.265 or better	
18.	Resolutions and frame rates (H.265)	All resolution streams with 25/30fps or Better	
19.	Video Streams	Individually configurable minimum 03 video streams or more	
20.	Streaming Method	Unicast, Multicast, Broadcast support along with multi stream support	
21.	Local storage	SD Card Slot with 128 GB or better Support provided with 128 GB card	
22.	Image Settings	Colour, Anti-glare Brightness, Sharpness, Contrast, White balance, Backlight compensation, Image Mirroring, Text and image overlay, HLC, 3D DNR, Defog, EIS, ROI, AGC, bmp format,	
23.	Supported Protocol	HTTP, HTTPS/SSL/TLS, TCP, ICMP/RTSP, EAP-TLS, EAP-MD5, RTP, UDP, IGMP, RTCP, SMTP, FTP, DHCP, UPnP/ARP/DNS/ DynDNS, SMTP, Ipv4/Ipv6.	



24.	Ethernet Port	RJ-45 (10/100Base-T) Mbps or Better	
25.	ONVIF	Profile S, G / Profile S, G, T	
26.	Operating Temp	-30 °C ~ 60 °C, Humidity 90% or less (non-condensing)	
27.	HLC, BLC	Auto	
28.	IR – Internal/External	IR 80 meters to be considered Internal or external or better	
29.	Input / Output	Min 2/2 or better	
30.	Housing	IP 67 Rated IK 10 rated for outdoor use;	
31.	Certifications	CE, FCC, UL/cUL, BIS, NEMA 4X	
32.	Power Requirement	Power Over Ethernet (P.O.E.), POE+	
33.	Mounting Accessories	For pole and surface mount with L/C Brackets	
34.	EMI EMC	Surge test (Level 4) as per IEC:61000-4-5(Level 4)	
35.	Audio	1 Channel Audio IN/ 1 Channel Audio Out or Built In MIC/ 1 Channel Audio Output, Support two-way audio (Optional)	
36.	MTBF	Min 100000 Hours or better	
37.	Defogger	Digital defogger/Defogger	
38.	Misc.	The Camera to be provided by the OEM/bidder should not be complying to GB28181, GB/T28181-2011 standards and there should be no option to activate or deactivate GB/T 28181 standards in the camera web page/settings.	

D. Poles - for Cameras with 1 mtr ARMs for Fixed & PTZ

Sr.No.	Parameter	Technical Specifications	Compliance (Yes/No) with comments, if any
1.	General Requirement	Hot dip galvanized pole with silver coating of 86 micron as per IS:2629 with suitable bottom and top thick HT plate along with base plate and suitable arm bracket and with J type foundation bolts. Fabrication in accordance with IS 2713 (1980), Ground based security GI MS pole with accessories to mount the PTZ and bullet/fixed cameras	
2.	Material	Mild Steel (M.S) Tubular Pipe (B-Class) as per IS-1239 (Part-1)-193 or Mild Steel hot dip galvanized with Yellow Painted with two layered.	
3.	Diameter and Thickness	Outer diameter 125mm or better Thickness 3.96 mm +- 5% tolerance	



4.	Base Plate	MS hot dip galvanized 15 mm thick (300 mm by 300 mm) with four MS hot dipped 20 mm dia. foundation bolts	
5.	Foundation	Pole would be fixed on an adequate and strong Foundation to withstand city weather conditions and wind speed of 180 km/hr. Foundation – RCC blocks with 10 mm tor steel size 500 mm by 500mm by 1800mm. foundation bolts (4 no's ,16mm dia. ,700 mm length) precasted in RCC block. Casting of civil foundation with foundation bolts to ensure vibration free (video feed quality should not be impacted due to wind in different climatic conditions)	
6.	Height	Height of the pole shall be as per requirement of the location varying from 6m or higher.	
7.	Arm / Overhang	If required System Integrator can provide around 1 mtrs. ARM	
8.	Lighting Protection	Copper lighting arrestor at top of the pole 14mm diameter.	
9.	Earthing	Chemical/salt earth pit with depth of 10 feet.	
10.	Seismic dampeners, anti-corrosion warranty, Load Capacity, Wind Velocity capacity	Seismic dampeners required as per Delhi seismic zone. Warranty of anti-corrosion of min 10 years or better Wind velocity = Min 180 KMPH (pole mounted at ground level). Required structural certificated based on the loading etc. Load capacity = ONE PTZ with two bullet cameras and one junction box of 12U (if pole mount) and 16 U (if floor mount) Wind loads as per IS: 875	
11.	Design Standard and Design life	IS: 800-2007 and min 10 years life or better	
12.	Accessories like Washer, Screws, Nut Bolts and other required accessories	As per the final drawings and with approval by recognized institution. Metal Climb blocker need to be installed on every pole, conceal cabling & wiring should be there	



E. Poles - Cantilever Poles for ANPR camera

Sr.No.	Parameter	Technical Specifications	Compliance (Yes/ No) with comments, if any
1.	General Requirement	Hot dip galvanized pole with silver coating of 86 micron as per IS:2629 min 10 cm diameter pole and suitable bottom and top thick HT plate along with base plate suitable for wind speed 50 m/sec with suitable arm bracket and with J type foundation bolts. Fabrication in accordance with IS 2713 (1980) with accessories to mount four to six bullet /ANPR cameras	
2.	Material	Mild Steel (M.S) Tubular Pipe (B-Class) as per IS-1239 (Part-1)-193 or Steel E350 grade or Mild Steel hot dip galvanized with Yellow Painted with two layered.	
3.	Diameter and Thickness	Outer diameter 125mm or better Thickness 3.96 mm +- 5% tolerance	
4.	Base Plate	MS hot dip galvanized 16 mm thick (400 mm by 400 mm) with four MS hot dipped 20 mm dia foundation bolts.	
5.	Foundation	Pole would be fixed on an adequate and strong Foundation to withstand city weather conditions and wind speed of 180 km/hr. Foundation – RCC blocks with 10 mm tor steel size 500 mm by 500mm by 1800mm. foundation bolts (4 no's ,16mm dia. ,700 mm length) precasted in RCC block. Casting of civil foundation with foundation bolts to ensure vibration free (video feed quality should not be impacted due to wind in different climatic conditions)	
6.	Height	Height of the pole shall be as per requirement of the location varying upto 6m	
7.	Arm / Overhang/Cantilever	Upto 5 mtr. with guy rope with extension arm dia. of 73 mm /3.05 mm thickness GI	



		-MS pole attached with main pole via fledge joint/fledge thickness 14mm.	
8.	Lighting Protection	Copper lighting arrestor at top of the pole 14mm diameter or better.	
9.	Earthing	Chemical/salt earth pit with depth of 10 feet.	
10.	Design Standard and Design life	IS: 800-2007 and minimum 10 years of life or better	
11.	Seismic dampeners, anti-corrosion warranty, Load Capacity, Wind Velocity capacity	Seismic dampeners required as per Delhi seismic zone. Warranty of anti-corrosion of min 10 years or better Wind velocity = Min 180 KMPH (pole mounted at ground level). Required structural certificated based on the loading etc. Load capacity = four to six bullet cameras and one junction box of 12 U (if pole mount) and 16 U (if floor mount). Wind loads as per IS: 875	
12.	Accessories like Washer, Screws, Nut Bolts and other required accessories	As per the final drawings with approval by recognized institution. Metal Climb blocker need to be installed on every pole, conceal cabling & wiring should be there	

F. Network Access Switches - 8 or more ports

Sr. No	Type:	Layer 2 Manageable Industrial Grade switch.	Compliance (Yes/No) with comments, if any
1.	Ports	Minimum 8 x of 10,100,1000 RJ45 interfaces with POE+ Supporting IEE 802.3af and 802.3 at standards and 4 x 1G SFP interface and 2x1G single mode optix on day one. Simultaneous active port count should be 12 or more. Support EEE on all copper ports	
2.	Performance and Reliability	It should be industrial grade switch which should operate at wider temperature range (-10 to 60 deg) or better withstands greater shock, vibrations, temperature and EMI/EMC tests. It should have non-blocking wire-speed architecture. It should be architected to support real time applications like voice, video, data by having distributed architecture. Should support IP 30 rating. MTBF value not less than 20/25 years	



3.	Power	POE Budget – 240 watts.	
4.	VLAN support	a. Minimum 1024 active VLANS b. Dynamic VLAN with VTP / MVRP /PIM c. IP subnet VLAN d. 802.1v e. 802.1ad (q-in-q) f. Private VLAN	
5.	Security	a. 802.1x support b. MAC-based Authentication c. DHCP Server ipv4 & ipv6, Client, Relay, Snooping, option 82/Relay, d. ACL based on L2, L3, L4 rules e. IP source Guard f. Storm Control for unicast, broadcast and multicast. g. Cable diagnostics to measure cable length h. Ipv4 & ipv6 sFlow Agent	
6.	Surveillance Traffic handling Features	a. 8K MAC table b. 8 QoS queues per port, DSCP remarking c. NTP over IPv6. D. Bandwidth control rate limit, Per VLAN port mirror e. Ring Protocol for fast failover. Link loss recovery < 50ms f. IGMP snooping - v1, v2, v3, MLD snooping, MVR/PIM	
7.	Management	a. GUI - should be supplied with software for mass configuration of switches. b. IP v6 compatible and management with support for SSH, Telnet, SNMP, RMON c. Support Syslog for alarm d. Dedicated Management port with industry standard CLI - e PoE management - Scheduling of Power Delivery, Power limit by device type and Power delivery prioritization f. Switch Port Analyzer per VLAN g. RADIUS (Authentication and Accounting), TACACs+ 3.0 , RMON I and II, DNS Server, Client and Proxy, Configurable LLDP-MED values h. Support for RFC 2544 or better	
8.	Certification	a. EN 61000-4-5 Surge b. EN 60950c c. RoHS and WEEE compliant d. NEMA- TS2	



9.	Operating conditions	temperature -10° ~ 60°C, humidity 5% to 95% (Non-condensing)	
10.	Accessories:	Should be supplied with mounting bracket, DIN rail, power cord, console cable and installation guide with each switch.	
11.	Warranty and Support	As mentioned in RFP with support and OS upgrade	
12.	Seamless Integration	Seamless Integration: For Seamless Integration and Interoperability all the switches and SFP Modules should be fully compatible for smooth functioning of the system	

G. Junction Box - Floor placed and Pole mounted (including last mile passive networking, Earthing, etc.)

S.No	Parameter	Specifications	Compliance (Yes/No) with comments, if any
1.	Ingress Protection	Outdoor – IP55 or better, Floor mount Dimension -16U (800 W x (16U) x 800 D), Pole Mount -12U (600Wx(12U)x600D (in mm)	
2.	Cooling	Force Cooling Thorough Fan with filter provisions. Fan and filter housing unit min 02 (top/side mounted) or better. The final number of fans will be decided by thermal calculations of actual load.	
3.	Mounting	Both Pole & Floor Mount Pole/ Floor mounting arrangements with support bracket and other accessories like Nut bolts, washers etc. as required	
4.	Material	Galvanised Iron (GI) Sheet - 120GSM, Galvanised Iron (GI) sheet gauge for Floor mount JB- 1.6 mm or better Pole Mount JB- 1.2- 1.5 mm Surface treatment PP Coating 80-120 Micron Nano ceramic coated, electro-phoretic (EC) dip coat primed and then powder coated	
5.	Temperature	Inside cabinet temperature should be maintained between 0 to 40°C or better	
6.	Locking	3-point spring loaded locking mechanism with Pad lock and Allen key with anti-rusting metal protective cover	



		Opening leaver/handles should be made of metal	
7.	Weight	Weight bearing capacity should be Min 90 Kg for floor mount, for Pole Mount 65 Kg	
8.	Service & Maintenance	Professional and Prompt	
9.	Anticorrosion Warranty & JB Life	Minimum 10 years or better from date of installation at site	
10.	Others	Removable high-quality EPDM gasket for IP rating Rain canopy 75 mm on top with front projection of the enclosure such that rain water or water lodging should not penetrate in Junction Box Horizontal/Vertical PDU Caging for security of Junction Box from vandalism and theft	
11.	Design	The design of the JB both Pole and Surface to be submitted.	
12.	Safe City Logo & DP Logo	Safe city Log and Delhi Police logo will be embossed/etching (in color) in each JB	

H. Gun Shot solution-200 No

a. Functional requirement

Gunshot application should be provisioned in order to capture the instances threatening severe crimes related to bullet fire. The application should be capable enough to capture the Gun shot sound in the noisy conditions of roads in Delhi. It is to be considered that the Gun-shot application would be operated for the camera locations where the Police Administration has firm trends of such probable crimes only considering the low accuracy of the solution in the current demographics of Delhi NCT.

This solution should be capable for analyzing the object movement speed, sound transfer rate, thermal effect, etc. considered for better success rate of the application.

Key result areas:

- Gunshot detectors which are large acoustic needs to be positioned across 200 poles out of all envisaged locations covering more criminal prone areas across the city. They form an expansive geographic network that cover whole neighbourhoods.



- b. Gunshot detectors sense several unique characteristics of gunshots to recognize the sound of a bullet blast, the “crack” of a projectile moving at supersonic speeds, and a visible muzzle flash.
- c. When someone fires a gun, multiple sensors must detect the noise and record the precise moment of the sound reached the sensor. The volume of the shot and tiny differences in the time it took the sound to reach the sensor must be able to establish the distance of the shot from each detector. The system must be capable to use this information to triangulate the location of the shooter.
- d. Gunshot detection- Technical Requirements and Compliance Sheet for MSI (to provide compliance report with the bid)

Sr. No	Specification	Compliance (Yes/No) with comments, if any
1.	Built using AI that runs entirely on the edge	
2.	Up to 80% accurate at up to 200 feet; AI technology enables increased accuracy over time in an environment	
3.	AI allows the system to detect a broad range of gunshot types	
4.	Up to 1000 feet of localizable acoustic range	
5.	Receive real-time acoustic alerts sent via email and text	

I. Public Address System + loudspeaker

At $182(c2i) + 16(c3i) + 2(c4i) + 100(\text{loudspeaker in field}) = 300$ identified spots (locations) centrally regulated at C4i

a. Functional Requirements

The network PA works very much similarly to computer networks where packets of data are transmitted from one node to another with each of them having a unique IP address in the network system. The nodes will then only pick up the packets that solely addressed to them. The network PA can also be integrated with other building services or subsystems that are TCP/IP compliant like PA system at C2i can be instructed from C4i/C3i and other building management system to provide instantaneous voice assisted response and feedback from each system. The PA system should have at least featured like:

- i. All the elements of the system are IP compatible.
- ii. PS/Districtwide announcements based on the selection of channel and all call emergency announcements can be made through the PA system.
- iii. This IP based P A system can be accessed from anywhere and everywhere and forward required messages. It 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

- iv. PA system shall be connected at C2i, C3i and C4i level. In addition to this PA system for Mobile Command Control Vehicle (MCCV) can also be provided in order to have the connectivity centrally.

b. PAS - Technical Requirements and Compliance Sheet for MSI (to provide compliance report with the bid)

S No.	Public Address System (PAS)	Compliance (Yes/ No) with comments, if any
1.	The Public Address System (PA) shall be capable of addressing citizens at specific locations from the ICCC.	
2.	The proposed system shall contain an IP-based announcing control connected to the ICCC.	
3.	Public Address system shall be used at intersections, public places, market places or those critical locations as identified by Delhi Police to make important announcements for the public.	
4.	The system shall contain an IP based amplifier and uses PoE power which shall drive the speakers (If amplifier required more power supply should be provided externally through junction box provisioning). The system shall also contain the control software which shall be used to control/ monitor all the components of the system which include Controller, Calling Station & keypad, Amplifier (Mixing & Booster).	
5.	It shall be able to broadcast messages across all PA systems or specific announcement could be made to a particular location supporting single zone / multi zone operations.	
6.	The system shall also deliver pre-recorded messages to the loud speakers attached to them from CD/DVD Players & Pen drives for public announcements.	
7.	The system shall contain an IP-based amplifier and uses PoE power that could drive the speakers. The system shall also contain the control software that could be used to control/monitor all the components of the system that includes Controller, Calling Station & keypad, Amplifier (Mixing & Booster).	
8.	PA system's master controller shall have function keys for selecting the single location, group of locations or all locations, simple operation on broadcasting to any terminal or separated zones.	
9.	PA system's master controller should facilitate multiple MIC inputs and audio inputs.	



10.	Scope of Work	
11.	The broad scope of work to be covered under this sub module will include the following, but is not limited to:	
12.	MSI will install IP based Public Address System as part of the information dissemination system at 200 locations (the location details will be shared & finalized with the successful MSI) in the city. These systems shall be deployed at identified junction to make public interest announcements.	
13.	The system deployed shall be IP based and have the capability to be managed and controlled from the ICCC	
14.	MSI, in consultation with Delhi Police can propose alternate locations apart from the locations mentioned in this RFP for installing the PA system where their effectiveness in communicating information about traffic conditions in Delhi Police will be maximized.	
15.	Delhi Police shall review and approve the proposed locations. MSI will install the PA system on the approved locations.	
16.	Should have the capability to control individual PAS i.e. to make an announcement at select location (1:1) and all locations (1: many) simultaneously.	
Public Address System Technical Parameters		
S No.	Parameter	Compliance (Yes/ No) with comments, if any
1.	Should have the capability to control individual PAS i.e. to make an announcement at select location (1:1) or multiple locations (1: many). The PAS should also support both, Live and Recorded inputs	
2.	Field Side Equipment	
3.	IP amplifier with minimum 50 Watts, Class D.	
4.	Native IP connectivity, no convertors to be used	
5.	0 to 55 C Temperature rating for Amplifier	
6.	Automatic Volume Control	
7.	Frequency Response: 50Hz to 15000 Hz for Amplifier	
8.	2Inputs and 1 Output relay contacts in Amplifier	
9.	Speaker: Minimum 2 Speakers 20 W capacity	
10.	Frequency Response of Speaker 350 -10,000Hz	
11.	Line Monitoring Facility for speakers	



12.	IP 55 Housing for amplifier	
	Control room Side Equipment	
1.	Central Software based server application capable of working on virtual environment/cloud with 100% redundancy for DC & nDR	
2.	Access control mechanism would be also required to establish so that the usage is regulated.	
3.	Integration with VMS and Command & Control center or any other component if required	
4.	PA Master Controller to have facility for multiple mic inputs, direct dialing buttons, LCD screen	
5.	Software Client for making Calls to PA and ECB	
6.	Automatic Volume Control, Call recording of all PA announcements with date and time	
7.	Transmission bandwidth 16000 KHz.	
8.	Operating temperature for control desk 0 to +60C	

J. UPS (60 Minutes backup)- 1KVA, 2KVA with 60 mins. Backup on 80% Load

Sr. No	Parameter	Specifications	Compliance (Yes/ No) with comments, if any
1.	Capacity	1.0 KVA / 900 W, 2.0 KVA / 1600 W (It will be placed in field so required rigid UPS)	
2.	Technology	IGBT (Rectifier & Inverter both); ECO Mode required	
3.	Wave form & Freq converter	Pure Sine wave & shall have frequency converter mode	
4.	Display	LCD	
5.	Input power factor correction	0.99 at 100% Linear load	
6.	Input configuration	1Ph, L-N+PE (176 to 300Vac) +/- 3% on full load & shall support upto 110Vac for 60% load).	
7.		UPS Shall have inbuilt OVCD protection. OVCD shall be capable to withstand 430 VAC for minimum 24 Hours. (OVCD is Over Voltage Cut Off Device)	
8.	Frequency (Input)	45 to 55 Hz frequency (or 54 to 66 Hz for 60Hz Output)	



9.	Frequency (output)	50Hz or (selectable to 60Hz)	
10.	Output Voltage	200/208/220/230/240Vac shall be available with +/-1% regulation	
11.	V threshold / Output Voltage Distortion	< = 2% max full linear load	
12.	Output Power factor	0.9	
13.	Crest factor	3:1 or better	
14.	AC-AC Efficiency	Online Mode: Greater than or equal to 88% @ Full Rated Load & Battery Fully charged ECO Mode: greater than or equal to 97% @ Full Rated Load & Battery Fully charged	
15.	Transfer time Main-Battery	0	
16.	Transfer time Inverter-Bypass	4 msec	
17.	Output Connection	Minimum 10Amps X 4 Nos. – C13 Type inbuilt to the UPS back.	
18.	Monitoring software for UPS	Shall be provided for monitoring of UPS from remote along with SNMP Card	
19.	Communication	SNMP Card	
20.	Port	RS 232	
21.	Battery Type	12V SMF	
22.	Battery backup	1KVA UPS with 1 Hr battery backup at 80% load using 30 minutes (Min VAH 775)	
23.	Charger	Shall be minimum 10% of the offered Battery AH	
a	Environmental Parameter		
1.	Operating temperature range	0-40 deg C or better. It should sustain in Delhi Environment, conformal coating for PCB Boards Fire Retardant material to be used for PCB Assemblies used in making the UPS	
2.	Other	Indication required -> Over Temperature, Load on Battery, Battery low, Mains ON	



3.	Humidity	0% to 95% no-condensing	
4.	Noise Level	52 dBA max	
5.	Mounting	Tower type /Rack Mount type (preferably standard 19-inch Rack mount)	
6.	EPO	Shall be available	
24.	Protection	IP20	
25.	LCD Display		
25.a	Measurements (On LCD)	Input & Output Voltage, Input & Output Frequency, Bypass: Voltage & Frequency, Remaining time & Battery Level Indicator, Load Level indicator, Fault codes, UPS alarm enable or disable.	
26.	Manufacturer	Manufacturer -> ISO 9001, ISO 14001, OEM Plant should have water & air pollution control clearance certificate from respective govt. agency. UPS OEM should have registered office in India from last 10 years (certificate of incorporation to be provided)	
27.A	Product	BIS certification	
28.	Management Supports /Software	Windows® 2000/ 2003 /XP/Vista/ 2008, Windows® 7 / 8, Linux, Unix	

K. Mobile hand held devices for Police Officials

S No.	Features	Minimum Specifications	Compliance (Yes/ No) with comments, if any
1.	Technology	GSM	
2.	Processor core	Octa core	
3.	Processor speed (in GHz) Minimum	2.3	
4.	Operating system	Android 8.x Oreo GMS certified	
5.	Chipset	Qualcomm / Mediatek / Exynos / Snapdragon / Spreadtrum	
6.	RAM Size (in GB) Minimum	8	
7.	Internal Storage (in GB)	128 or better	
8.	Storage Expandable up to (in GB)	512	
9.	Display size (in inch)	6.3 inch or better	
10.	Display type	LCD Touch Screen / LED Backlit Touch Screen / Amoled Touch	



		Screen / Retina / Retina HD / IPS Touch/Super Amoled Touch Screen	
11.	Display Resolution (Horizontal x Vertical) (Pixel)	FHD (Minimum 1920 x 1080)	
12.	Sun light readability (Nits) - Minimum	400	
13.	Display protection	Corning Gorilla Glass 4 or better and equivalent	
14.	Rear Camera Resolution (Mega Pixel) - Minimum	24	
15.	Front Camera Resolution (Mega Pixels) - Minimum	24	
16.	SIM Card Slots	Dual SIM slot with separate memory card slot	
17.	OTG support	Yes, with cable	
18.	Connectivity	4G VoLTE	
19.	Wi-fi Connectivity	802.11a/b/g/n/ac	
20.	Bluetooth Connectivity	4.3 or higher	
21.	GPS	GPS with AGPS	
22.	Battery Capacity (mAH) Minimum	4000	
23.	Type of Battery	Lithium-ion or better	
24.	Accessories: One wall charger with USB charging and Data transfer cable	Yes	
25.	Accessories: One ear phone	Yes	
26.	The tool to manage devices data security push device policies push custom apps reports management of applications and devices for example white list or blacklist applications URLs control device functionality as camera Bluetooth WIFI,4G Enabled, Private APN for SIM	Yes	
27.	Admin portal to manage smart mobile phones remotely to enroll u- enroll deploy and configure all mobile devices applications and security policies	Yes	
28.	Onsite Service and warranty	As mentioned in RFP	



4.11 Mobile Command Control Vehicle

A. Chassis and Interior

S No.	Technical Specifications	Compliance (Yes/No) with comments, if any
A.	Chassis	
1.	Air-Conditioned Bus shall be from a reputed vendor	
2.	Wheelbase: approx. 4200 mm wheelbase	
3.	Ground Clearance: minimum 190mm	
4.	Overall Length: minimum 7000mm or more	
5.	Steering: Power Steering	
6.	Brakes: Airbrake or better	
B.	Engine	
1.	Compliant to present vehicle standards	
2.	Emission: As per the registration criteria in Delhi	
3.	Fuel: CNG	
C.	Vehicle Interior	
1.	The vehicle shall accommodate: Two Operator Consoles with 32" Display One ICS Console Seating arrangement for 2 Operators and 1 ICS person Seating arrangement for 1 Supervisor and a mini seating area Mast for PTZ Camera LED Flood Lights Generator for Electronics Air Conditioning for Operations Area Minimum 5 KVA UPS with 60min Power backup Roof Mounted PA Speakers Shock mounted rugged 19" rack with storage space	
2.	Integrated Operator Console with 32" Display shall be provided separately for two operators. The chairs with swivel and fastened to the floor of the section.	
3.	The monitors for the surveillance computers shall be mounted in such a manner that it is convenient for viewing by the seated surveillance personnel.	
4.	Static electronic equipment shall be housed in a 19" rack with the necessary power sockets. The electronic equipment shall be housed such that it is safely fastened when the vehicle is moving and does not fall out. The rack shall 19" with shock & vibration isolators for safety of electronic equipment.	



5.	The vehicle body shall be strong enough to support a mast mounted PTZ camera.	
6.	The vehicle shall be air-conditioned with a 1 Ton Split Air Conditioner of reputed OEM	
7.	Vehicle shall be provided with rear parking camera and sensors. There shall be 2 cameras installed on the sides of the vehicle to monitor vehicle security	
8.	There shall be storage for stationary and other electronic equipment when not in use.	
9.	Vehicle External Painting shall be done based on Police's recommendation.	
10.	LED Lights to be provided in the Driver, Power and Operator area. Each cabin to have one smaller LED Light powered by Vehicle Battery. Balance to be powered by UPS.	
11.	The mast would be deployed only when the vehicle is stationary and would be retracted when vehicle starts moving. The mast should be self-supporting, having a head load of 25 Kgs or more and should be able to operate in wind speeds of 50 Kmph	
D.	Electrical	
1.	The electrical sub-system in the vehicle shall allow power to be drawn from the generator or external raw power available at operations site. Accordingly, MCBs, change-over switches, and other equipment shall be installed to make this possible. Industrial Raw AC Power socket to be supplied and installed externally.	
2.	The vehicle shall have electrical cabling to power computer systems, telecommunications equipment, networking equipment, and surveillance equipment. Concealed ducting needs to be provided in the vehicle body, for electrical and network cabling. The duct panels should be easily accessible by a technician, for maintenance purposes.	
E.	Lighting	
1.	Each workstation area should be well-lit. LED Lights shall be provided in the Driver, Mast and Operations Cabin. Each cabin to have one smaller LED Light powered by Vehicle Battery. Balance to be powered by UPS.	
F.	Power Generation	
1.	The power generation shall happen through the 7.5 KVA petrol genset unit installed inside the vehicle or when available the power shall be drawn from the raw power available at the site.	
2.	The power to the electronic equipment shall be given thru the UPS and Stabilizer. The generator power should be routed through the UPS, for charging the batteries. The UPS and the generator should be accommodated inside the van	



B. 5KVA UPS System with Batteries for 1 hour backup

S No.	Technical Specifications	Compliance (Yes/No) with comments, if any
A.	UPS	
1.	Pure Sinewave UPS: To supply power to the electronic equipment in the Vehicle for up to 60 minutes.	
2.	1 phase input – 1 phase output UPS	
3.	LCD panel information	
4.	Rating: 5 KVA or better	
5.	Peak Efficiency: > 80%	
6.	ISO Certified	
B.	UPS Battery	
1.	SMF batteries with deep discharge technology	
2.	Battery type: SMF	
3.	Powers 5 KVA UPS for up to 60 minutes	
4.	Fully sealed construction	
5.	Nominal Voltage: 12V	

C. 7.5 KVA Silent Petrol Generator Set or better

S No.	Technical Specifications	Compliance (Yes/No) with comments, if any
A.	Generator Set Silent Type	
1.	Generator-set to power the electronic equipment, accessories, and lighting	
2.	Starting System: Recoil / Electric or better	
3.	Rated output (50 Hz): 7.5 KVA or better	
4.	Rated voltage @ 50 Hz: 230 or better	
5.	Continuous Operating Time: minimum 4 hrs. at full capacity or better	
6.	Fuel Tank Capacity: 16 Ltr. (minimum) or better	
7.	ISO Certified	

D. PC for Operator / Industrial PC based Network Video Recorder

S. No.	Classification	Description	Compliance (Yes/No) with comments, if any
1.	Processors	10th Generation Intel Core i7-10510U Processor	
2.	Memory	16GB DDR4@2666 MHz Non-ECC Memory or better	



3.	Graphics	NIVDIA Quadro K620 2GB or better	
4.	Hard Drives	8 TB SATA HDD 7200RPM	
5.	Standard i/o Ports	4 - USB 2.0 1 - VGA 1 - RJ45 1 - Audio line-in / microphone 1 - Audio line-out	
6.	Operating System	Windows 8 Prof. or better	

E. Vehicle Mast mounted PTZ Camera with Keyboard and Joystick

S. No.	Classification	Description	Compliance (Yes/No) with comments, if any
1.	General	1/1.9" Progressive Scan CMOS or better	
		Optical zoom: 23X; Digital zoom: 16X or better	
		Resolution: 1920x1080. 2MP or better	
		ONVIF, CGI, PSIA	
		IP66 or better Compliant	
		Up to 80m IR Light Source	
2.	Focal Length	5.9-135.7mm, 23X or better	
3.	Angle of View	59.8°-3.0°(Wide-Tele) or better	
4.	Min. Working Distance	10-1500mm (Wide-Tele) or better	
5.	Camera Function	Auto iris, Auto focus, Auto white balance, Backlight compensation and auto day & night switch Min. Illumination: Color : 0.002Lux @ (F1.5, AGC ON), B/W : 0.0002Lux @ (F1.5, AGC ON)	
6.	Smart Functions	Image processing: shall support defog, HLC/BLC Smart codec: low bit rate, ROI	



7.	Network Functions	H.265,H.264,MJPEG video compression H.264&H.265 encoding with Baseline/Main/High profile ROI(Region of Interest) encoding Built-in Web server Multiple network protocols supported: IPv4/Ipv6, HTTP, HTTPS, 802.1X, QoS, FTP, SMTP, UPnP, SNMP, DNS, DDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, ICMP, DHCP, PPPoE	
8.	Video Resolution	PAL: CIF (704×576)/2CIF (704×288)/CIF (352×288)/QCIF (176×144) NTSC: 30fps; PAL: 25fps	
9.	Connections	Network Connection: 10/100M self- adaptive Ethernet port	
		Network Protocols: ATP, Telnet, ODP, TCP, IP, HTTP, IGMP, ICMP, ARP, SNMP, ONVIF	
10.	Pan & Tilt Functions	PT Movement Range: Pan: 360° endless, Tilt: +90°~-90° or better	
		PT Movement Speed: Pan: 0.1°-80°/s, Tilt: 0.1°-40°/s or better	
		PT Number of Preset: 300	
		PT Patrol: 8 patrols, up to 32 presets per patrol	
		PT Pattern: 4 patterns, with the recording time not less than 10 minutes per pattern	
11.	Power	DC12V, Max. 40W	
12.	IR	Up to 150m IR Light Source	
		Automatically adjusted, depending on the zoom ratio	
13.	Housing	IP67 rated IK10 rated for outdoor unit	
14.	Certifications	CE, FCC, UL/cUL, BIS, NEMA 4X	
15.	Misc.	The Camera to be provided by the OEM/bidder should not be complying to GB28181, GB/T28181-2011 standards and there should be no option to activate or deactivate GB/T 28181 standards in the camera web page/settings.	



F. Vehicle mounted full HD Bullet Cameras

S. No.	Classification	Description	Compliance (Yes/No) with comments, if any
1.	Resolution	2 MP Full HD 1080p or better	
2.	Camera Type	Fixed	
3.	Video compression	H.264,H.265 or better	
4.	Frame rate	Min. 25 fps	
5.	Image Sensor	1/2.8" progressive scan CMOS or better	
6.	Minimum Illumination	Colour: 0.05 lux, B/W: 0.01 lux @F1.6	
7.	S/N Ratio:	≥ 50dB	
8.	Day/Night Mode	Colour, Mono, Auto	
9.	Wide Dynamic Range	True WDR	
10.	Auto adjustment	Color, brightness, sharpness, contrast, white balance, exposure control, backlight compensation, Gain Control, Electronic Image Stabilization	
11.	Protocol	HTTP, HTTPS, FTP, SNMP, DNS, NTP, RTSP, RTP, TCP, UDP, RTCP, DHCP, ONVIF	
12.	Housing	IP67 rated IK10 rated for outdoor unit	
13.	Certifications	CE, FCC, UL/cUL, BIS, NEMA 4X	
14.	Misc.	The Camera to be provided by the OEM/bidder should not be complying to GB28181, GB/T28181-2011 standards and there should be no option to activate or deactivate GB/T 28181 standards in the camera web page/settings.	



G. Video Management System

S. No.	Classification	Description	Compliance (Yes/No) with comments, if any
1.	User Management	Unlimited Users & Roles - Custom defined roles: a.) Individual camera access, b.) View/Delete video Clips, c.) Administration access	
		Detailed user activity logging	
		Lost password retrieval	
2.	Video Viewing	Min. 16 Camera Flow View, a.) Live View Displays, Native Resolution, b.) Split Screen, c.) Full Screen	
		Live Video Patrols, a.) Select Cameras/Time to Display, b.) Highlight on Motion Detection, c.) Play Audio Alert on Motion	
		Digital Pan, Zoom and Tilt	
		Video Viewing shall be possible from Android based smart phone.	
3.	Video Recording & Playback	Record Video and Images, a.) On Demand, b.) On Motion Detection, c.) On Scheduled Day and Time, d.) 24x7x365	
4.	Scheduling	Schedule Types, a.) Video Recording, b.) Alerts, c.) Backups	
5.	Camera Settings	Compression (H.264, H.265)	
		Brightness	
		Sharpness	
		Saturation	
		Iris	
		Frame Rate (5-30fps)	
		Bit Rate (64kbps-4.6mbps)	
		Auto Low Light Mode	
		Environment Settings	
		Flicker Settings	
6.	Back-up & Storage	External Backup, a.) NAS	
		Backup, a.) On Demand, b.) On Custom Schedule, C.) By Media Type	
		Automatic Purge, a.) By Number of Days, b.) By % of HDD Capacity	
7.	Supported Devices	Windows PC, IE Web Browser (v7.0+)	



8.	Analytics	The minimal analytics features should be part of the VMS for the cameras. Performance degradation due to the placement of cameras would be acceptable.	

H. Standalone Mobile Hand Held Device

S. No.	Features	Minimum Specifications	Compliance (Yes/ No) with comments, if any
1.	Technology	GSM	
2.	Processor core	Octa core	
3.	Processor speed (in GHz) Minimum	2.3	
4.	Operating system	Android 8.x Oreo GMS certified	
5.	Chipset	Qualcomm / Mediatek / Exynos / Snapdragon / Spreadtrum	
6.	RAM Size (in GB) Minimum	8	
7.	Internal Storage (in GB)	128 or better	
8.	Storage Expandable up to (in GB)	512	
9.	Display size (in inch)	6.3 inch or better	
10.	Display type	LCD Touch Screen / LED Backlit Touch Screen / AMOLED Touch Screen / Retina / Retina HD / IPS Touch/Super AMOLED Touch Screen	
11.	Display Resolution (Horizontal x Vertical) (Pixel)	FHD (Minimum 1920 x 1080)	
12.	Sun light readability (Nits) – Minimum	400	
13.	Display protection	Corning Gorilla Glass 4 or better and equivalent	
14.	Rear Camera Resolution (Mega Pixel) – Minimum	24	
15.	Front Camera Resolution (Mega Pixels) – Minimum	24	
16.	SIM Card Slots	Dual SIM slot with separate memory card slot	
17.	OTG support	Yes with cable	
18.	Connectivity	4G VoLTE	
19.	Wi-fi Connectivity	802.11a/b/g/n/ac	
20.	Bluetooth Connectivity	4.3 or higher	
21.	GPS	GPS with AGPS	



22.	Battery Capacity (mAH) Minimum	4000	
23.	Type of Battery	Lithium-ion or better	
24.	Accessories: One wall charger with USB charging and Data transfer cable	Yes	
25.	Accessories: One ear phone	Yes	
26.	The tool to manage devices data security push device policies push custom apps reports management of applications and devices for example white list or blacklist applications URLs control device functionality as camera Bluetooth WIFI, 4G Enabled, Private APN for SIM	Yes	
27.	Admin portal to manage smart mobile phones remotely to enroll u- enroll deploy and configure all mobile devices applications and security policies	Yes	
28.	Onsite Service and warranty	As mentioned in RFP	

I. Interoperable Communication System (ICS)

S. No.	Classification	Description	Compliance (Yes/ No) with comments, if any
1.	System Capacity	The system should be able to support up-to 4 radio interfaces. The system shall be scalable to support one operator position operating in a fixed or mobile environment and accessing a small number of communications resources in an integrated dispatch or call-taking environment and accessing multiple resources	
2.	System Architecture	The console dispatch system shall employ an end-to-end digital architecture from the resource interfaces to the operator workstations that is capable of integrating	



		in a single switch all radio and telephone voice communications.	
3.	Dispatch workstation and User Interface	Dispatch workstations shall consist of an operator control unit to manage all audio communications between the operator position and the switching equipment, and a Windows-based personal computer (PC) to provide operators access to and control of system resources and functions. Workstation PCs shall run under the Microsoft Windows operating system Each workstation shall be equipped with a touch panel-based display, keyboard, mouse or trackball, external or embedded speakers, and associated input and control devices (headsets, handsets, microphones, footswitch, dual jack boxes, etc.) as described elsewhere in this tender document	
4.	Radio Interface Support	The system shall support various trunking and wireless interfaces.	
5.	Signaling Protocols	The system shall support various signaling protocols.	
6.	Telephony Protocols	The system shall support various telephony protocols including 2-wire POTS and PSTN/PABX and GSM Modems	
7.	Instant Recall Recorder	Each dispatch workstation shall be capable of being equipped with hardware and/or software-based instant recall recorders (IRR). A software-based IRR shall be a Windows application capable of recording all operator audio in standard WAV file format and offering immediate playback and short-term storage of operator audio communications. It shall be possible to store audio WAV files on the workstation PC, network server, and/or on a network storage device (e.g., CD-RW). The ability to play back a call shall not be limited by the availability of the network or a system-wide recording device.	
8.	Dispatch Console User Interface	The console dispatch system shall include a Windows-based user interface (UI) application that gives operators access to and control of system resources and	



		functions. The UI application shall run on the workstation PC and shall be configurable to provide the specific functionality needed for an operator to perform his/her duties.	
		The UI shall present the various line and function controls using icons representing traditional screen-based buttons whose appearance can be configured according to location on the screen, size, color, labeling (font style and color), and image (bitmap). In addition, operators shall be able to access multiple screens presenting different line and function controls simply by clicking on tabs that, when selected, present new resource views. The appearance (color, font, three dimensional effects) of buttons will change as required to indicate the state of the line or function to the operator (e.g., selected line, activity on a channel, etc.).	
		The UI shall include embedded windows that allow operators to access and display intranet and/or internet HTML pages and to navigate Web-based resources, subject to administrative control.	
9.	Channels	The Integrated Dispatch Console System shall support 4 Radios (APCO-P25/UHF/DMR/GSM) connection.	
10.	System Diagnostics & Reporting	The console dispatch system shall provide the means to monitor system diagnostics via the configuration software. In addition, LEDs on the DSU will supply diagnostic information.	
11.	Configuration Software	Configuration software shall be provided that runs on a Windows-based PC that can be interfaced to the electronics directly. The software shall be used to configure the system and to monitor the status of system alarms.	
12.	Accessories	Operator Display Pedal PTT Speakers PTT Desk Mic	



13.	Interfacing	The proposed ICS should accommodate up-to 4 communication media. These would be provided for installation on MCCV along with all accessories. The communication media would be of following type : One DMR Radio One UHF Radio One APCO P25 Radio One GSM SIM (DMR, UHF & APCO P25 Radio would be provided by Delhi Police)	

J. 4 SIM based 4G Aggregator Device with Dongles

S. No.	Description	Compliance (Yes/No) with comments, if any
1.	4G Aggregator device shall have following features: 3G/4G/LTE Downlink & Uplink Bonding in Peer mode Dynamic DNS Load Balancing Support for 4 Nos of USB LTE Dongles Shall have Virtual interfaces with WAN and Traffic Management Shall support LAN, WAN & USB Ports Max Throughput of 1 Gbps at the receiver end Cloud based, SNMP & Remote Syslog based Device Management Internet Bonding Receiver Box for the Control Room shall also be proposed with Static IP and Internet Broadband Connectivity	

K. 24 Port GigE Switch

S. No.	Classification	Description	Compliance (Yes/No) with comments, if any
1.	Switch	24 X 10/100/1000 Mbps Gigabit ports	
		2 SFP Port	
		Auto MDI/MDIX cross-over for all ports	
		Secure store-and-forward switching scheme	
		Full/half-duplex for Ethernet/Fast Ethernet speeds	
		IEEE 802.3x Flow Control	



		Plug-and-play installation	
		Patch cables should be provided to connect the surveillance equipment as per the network diagram	

L. LED Flood Lights with 120-degree coverage (Mast Mounted)

S. No.	Description	Compliance (Yes/ No) with comments, if any
1.	Total System Wattage (W) – 120	
2.	Application: Outdoor	
3.	Dispersion Angle in degrees: 120	
4.	LED Type: High Power LED	
5.	Input Voltage in Volts: (90V to 300 V): 230 VAC	
6.	Weight: Max 5Kg	
7.	IP Rating: IP65 Compliant	

M. First-Aid Box

S. No.	Description	Compliance (Yes/ No) with comments, if any
1.	- Plastic Transparent Box SJF P5 :1 - Adhesive Plaster 19 X 72mm :10pcs - Adhesive Plaster 25 X 72mm :5pcs - Adhesive Plaster Round :3pcs - Microporous Tape 1.25x5mt :1pcs - Wound Cleaning Swabs: ALC :5pcs - Antiseptic Wipes :5pcs, Electrolyte Powder :3pcs - Sterile Burn Dressing 5cm :2pcs, Gauze Bandage 5cmx3mtr :1pcs - Sterile Gauze Swab 10 Cm :1pcs, Sterile Gauze Swab 7.5cm :1pcs - Burn Dressing Medium 10cm :1pcs, Sterile Adhesive Plaster 6x10cm :1pcs, Sterile Eye Pad Oval :2pcs, Elastic Gauze Bandage 6x1m :1pcs - Absorbent Cotton 15gms :1pcs, Scissor 7cm :1pcs - Dusting Powder 10g :1pcs, Antiseptic Cream 10gms :1pcs - Safety Pin :10pcs, Antiseptic Solution 50ml :1pcs - Tweezer Plastic :1pcs, Tincture Iodine 20ml :1pcs	



	• First Aid Book :1pcs, Sugar Sachet :3pcs • Common Salt Sachet :3pcs	

N. Fire Extinguisher

S. No.	Description	Compliance (Yes/ No) with comments, if any
1.	• Gross Weight: 2.3 Kg or more • Empty Weight: 1.3 Kg or more, • Can Height: 298MM or more, • Diameter: 86.5MM or more Discharge time: Minimum 8 Secs, • Discharge Mechanism: Controllable, • Range: Minimum 2 Meters, • Applicable on: Class A, B, C and electrically started Fire, (A Rating: 1A, B Rating: 8B,) • Can Construction: Deep drawn & CO2 Mig welded, Valve • Construction: Forging & Machining, • Internal Coating of Can: Epoxy Powder coating, • External Coating of Can : Epoxy Polyester Powder coating, • Certification: ISI Approved	

4.12 Network- Connectivity Backbone

The Networking infrastructure and the associated bandwidth measures to operate the entire infrastructure on field for video stream dissemination from field devices to Data Center, integration with external Govt. datasets and conduction of Post Analytical Operations with all security parameters in place will be the responsibility of the Internet Service Provider (ISP). The ISP will be the Networking Agency, who will be appointed through a distinct Competitive Bid Process.

There will be a tri- partite /quad partite mutual agreement, which will facilitate the field works related to network establishment for Project requirement in a conducive and speedy execution with respect to coordination with various Municipal bodies/ agencies across the NCT and the MSI.

A. Planning & Execution

The MSI will ensure all coordination help to the ISP to execute list of activities for laying of fiber cables for installation of the network backbone work to ensure desired last mile Connectivity starting from site survey of respective locations, laying and installation of various cables, hardware, UAT, Testing and signoff. All the ISP dependencies on the MSI for final stitching of the solution requirement to operationalize the system will be addressed pro-actively with the objective that the project does not suffer towards the tailing stages of the project.



The following essential activities to be coordinated by the MSI as per the requirement (if any) to enable ISP for execution of implementation activities and services to ensure time bound completion of under mentioned infrastructure laying targets:

- i. ROW application to be submit in various Municipal and Development Offices.
- ii. ROW demand note received from authority.
- iii. DD/BG preparation.
- iv. DD/BG submission to authority for permission.
- v. Liasioning with authority for ROW permission
- vi. Liasioning with authority for vehicle entry permission of HDD machine shifting.
- vii. Pits digging to start HDD machine
- viii. Manual digging or with HDD machine depends the track is hard rock/concrete/simple track.
- ix. Duct laying started post ROW receive
- x. Cable laying started post ducting
- xi. Fiber termination work post cable laying
- xii. Splicing work of fiber.
- xiii. Pits Closer
- xiv. Chamber installation
- xv. Route marker installation
- xvi. AT offering and clearance by fiber project team
- xvii. Ensure the availability of space and power at each node.
- xviii. ISP material installation & commissioning.
- xix. Termination and integration of fiber.
- xx. SFP installation
- xxi. Patch cord installation
- xxii. Node integration & RFS certificate for media provisioning.
- xxiii. Testing the circuit in presence of customer.
- xxiv. UAT at sites in presence of customer.
- xxv. Signoff after successful completion of testing.
- xxvi. Circuit Hand over

Total bandwidth estimation for the envisaged network in centralized Architecture

B. Bandwidth estimated requirement

S. No.	Type of Cameras	Bitrate (Mbps)	Frame Rate	Compression	Qty.	Police Stations (C2i)	DHQs (C3i)	Total bandwidth with average 30% viewing at C2i and 10% viewing at C3i
1.	Fixed Cameras – 4 MP	5	25	H.265,	6121	182	16	Average consumption of 80 Mbps for viewing at a time at each Police Station
2.	PTZ Cameras – 4 MP	5	25	H.265,	2246			



3.	ANPR Cameras – 2 MP	3	25	H.265	1622			
Total Cameras					9989	17270 Mbps considering 16 cameras viewing on a Workstation screen at a moment (keeps on moving for cyclic set of view frames for all cameras).		
Total bandwidth								

Following are the other factors for bandwidth calculation:

Other Factors for Bandwidth Calculations

S No.	Bandwidth category	Requirement (Mbps)
1	Total bandwidth required for the architecture (N)- new cameras at 182 C2i (Police Stations) 30% Viewing and at 16 C3I (DHQ)- 10% Viewing	17270
2	Total bandwidth required for the architecture (N)- new cameras at C4i and DC - 10% viewing	46756
3	Total Bandwidth required between DC and Near DR	2048
4	Total Bandwidth required for integration of cameras under different existing schemes	3500
5	Total bandwidth requirement	69574

Total bandwidth estimation is 69.5 Gig considered per year after the declaration of Go-live of phase-I. This provision will enable the live uninterrupted broadcasting (multi-casting) streaming at PHQ, DHQ and Police Station levels and parallel retrieval/ extraction of the transactional data from the Data Center at DHQ on the same infrastructure network. There will be provision of 1 Gig internet bandwidth.

4.13 Service Level Agreement for Project Implementation for MSI

Service Levels

Service Level Agreement (SLA) shall become the part of Agreement between Authority and the MSI. SLA defines the timely delivery of the deliverables and the correctness of the same based on the agreed Performance Indicators as detailed in the RFP scope. The MSI must comply with Service Levels requirements to ensure adherence to Project timelines, quality and availability of services.

The purpose of this Service Level Agreement (hereinafter referred to as SLA) is to clearly define the levels of service which shall be provided by the MSI to Authority for the duration of this Agreement.

The MSI must supply software/automated tools to monitor all the SLAs mentioned below.



The Service Level agreements have been logically segregated in the following categories:

Service Level Agreement (SLA)

SLA would be applicable in the Implementation, operations and maintenance phase of the project.

SLA would be applicable on:

- a. Implementation phase related performance levels
- b. C4i, C3i, C2i and City surveillance related performance levels
- c. Helpdesk SLA for O&M phase
- d. Data center activities

Definitions

For the purposes of this service level agreement, the definitions and terms are specified in the contract along with the following terms shall have the meanings set forth below:

- a. "Uptime" shall mean the time for the specified services / components with the specified technical service standards are available to the user department. Uptime, in percentage, of any component (Non - IT & IT) can be calculated as:
$$\text{Uptime} = \{1 - [(\text{Downtime}) / (\text{Total Time Maintenance Time})]\} * 100$$
- b. "Downtime" shall mean the time for which the specified services / components with specified technical and service standards are not available to the user department and excludes downtime owing to Force Majeure & Reasons beyond control of MSI.
- c. "Incident" refers to any event like non availability of services/partial availability of the services/performance downgrades which leads to disruption in normal operations of the entire System.
- d. "Helpdesk" shall mean the 24x7x365" support centre which shall handle Fault reporting, Trouble Ticketing and related enquiries during this contract.
- e. "Resolution Time" shall mean the time taken to resolve /fix the reported incident. This shall include resolving by means of diagnosing, troubleshooting, fixing and escalating to the next level. The details or reports of the outcome shall be informed to the next higher levels

Measurement of SLA

The SLA metrics provided specifies performance parameters as baseline performance, lower performance and breach. All SLA calculations will be done on quarterly basis. The SLA also specifies the penalties for lower performance and breach conditions.

Payment to the MSI is linked to the compliance with the SLA metrics. The matrix specifies three levels of performance, namely,

- The MSI will get 100% of the Contracted value (Net Project Cost) if all the baseline performance metrics are compiled and the cumulative credit points are 100
- The MSI will get lesser payment in case of the lower performance. (For e.g. if SLA point score is 80 then the MSI will get 20% less on the quarterly payment)
- If the performance of the MSI in respect of any parameter falls below the prescribed lower performance limit, debit points are imposed for the breach.

The credit (+) points earned during the quarter will be considered for computing penalty. The quarterly payment shall be made after deducting the penalties as mentioned above.



The SLA parameters shall be measured as per the individual SLA parameter requirements and measurement methods, through appropriate SLA Measurement tools to be provided by the MSI and manual calculation on the sample data on the basis the SLA measurement methodology approved and audited by the Authority or its appointed Consultant for accuracy and reliability.

The Authority shall also have the right to conduct, either itself or through any other MSI as it may deem fit, an audit/revision of the SLA parameters. The SLAs defined, shall be reviewed by the Authority on an annual basis after consulting the MSI, Project Management Consultants and other experts. All the changes would be made by the Authority after consultation with the MSI and might include some corrections to reduce undue relaxation in Service levels or some corrections to avoid unrealistic imposition of penalties, which are noticed after project has gone live.

Total penalties to be levied on the MSI shall be capped at 10% of the Total Project Cost. However, the Authority would have right to invoke termination of the contract in case the overall penalties equals 10% of Total Project Cost. Penalties to be levied during Post Implementation period shall be capped at 10% of the Total Project Cost. The Authority would also have right to invoke termination of contract in case cumulative debit point (breach points) are above 30 in two consecutive quarters.

Penalties

- Performance Penalty for not meeting a measurement parameter
- Time delivery of the Scope of Work

Definition	Timely delivery of deliverables would comprise entire Bill of Quantity and the application systems, and as per successful User Acceptance Test (UAT) of the same
Service Level Requirement	All the deliverables defined in the contract has to be submitted On-time on the date as mentioned in the contract with no delay
Measurement of Service Level Parameter	To be measured in Number of weeks of delay from the timelines mentioned in the section "Project Timelines"
Penalty for non-achievement of SLA Requirement	Penalty in percentage mentioned below para specified in the subsequent SLA tables as per various activities under the SLA norms.



Measurements & Targets

a. Implementation phase related performance levels

Sr. No.	Measurement	Definition	Target	Severity level	Penalty Amount per instance of non-compliance/ fault
1	Team mobilization and commencement of work	MSI must mobilize its complete project team as expected.	Within 7 days	—	1) Delay beyond 7 calendar days = 0.5% of the contract value 2) Delay beyond 15-30 calendar days = 0.6% of the contract value 3) Delay beyond 30 days = 0.7% of the contract value per week or may lead to Termination of the Contract at the discretion of TSP (C-DAC).

Data Center and Surveillance related Performance Levels/ Camera Feed and Quality:

The SLA metrics provided specifies performance parameters as baseline performance, lower performance and breach. All SLA calculations will be done on quarterly basis. The SLA also specifies the liquidated damages for lower performance and breach conditions. Payment to the MSI is linked to the compliance with the SLA metrics for various components involved. The matrix specifies three levels of performance namely,

- The MSI will get 100% of the Contracted value if all the baseline performance metrics are compiled and the cumulative credit points are 100.
- The MSI will get lesser payment in case of the lower performance.
 - If SLA point score is 80 then the MSI will get 15% less on the quarterly payment
 - If SLA point score is 70 then the MSI will get 20% less on the quarterly payment
 - If SLA point score is 50 then the MSI will get 25% less on the quarterly payment

The calculation of the credit score based on different line items as per SLA requirement can be seen in table given below.

If the performance of the Agency in respect of any parameter falls below the prescribed lower performance limit, which is 'breach' category, 50% penalty will be imposed on the quarterly SLA for the breach or termination of the contract in case of 2 consecutive 'breach' performance.



Table 1: SLA Performance Level

S. No	Performance Area	Baseline		Lower Performance		Breach	
		Metric	Poi nts	Metric	Poi nts	Metric	Poi nts
1. Camera, Video Feed Uptime and Quality							
1	Uptime per camera (live feed available irrespective of bandwidth or last mile issues, which are in control of MSI)	97%	15	>= 92% to <97%	10	< 92%	-10
2	Viewing center at police station shall display live camera feed available from selected cameras for viewing) at any given time	97%	14	>= 92% to <97%	4	< 92%	-13
3	Quality of Video feeds (Bad feeds due to Video Jitter, dim, blurred, unfocused, obstructed, non-aligned feeds	98%	10	>= 94% to <98%	3	< 94%	-8
5	Video stream Latency refers to the average time required for transmission of video feed from one point to another	=> 40ms	5	> 40-50 ms	3	>50 ms	-5
2. Application Performance							
1	Overall application(s) availability at Police Station & Command & Control Center	99%	6	>= 96% to <99%	2	< 96%	-6



S. No	Performance Area	Baseline		Lower Performance		Breach	
		Metric	Poi nts	Metric	Poi nts	Metric	Poi nts
2	Maximum time for User Login at Command Center	< 2 sec	1	2.01 – 4.0 secs	0.5	> 4 sec	-1
3	Maximum time for Surveillance Application(s) opening, this includes any application deployed for the project at Command Center	< 5 sec	1	5.01 – 10.0 secs	0.5	> 10 sec	-1.5
4	Menu Navigation, Window/Screen Opening, Screen Navigation (Average) at Command Center	<2 sec	1	2.01 – 5.0 secs	0.5	>5 secs	-1
5	Retrieval of video feeds at Command Center	<4 sec	2	4.01 – 6.0 secs	0.5	>6 secs	-1
6	Reports Generation Response Time (Alerts/MIS/Logs etc.)	Simple query - < 5secs Medium complexity query - <30 secs High Complexity query - < 1min	1	Simple complexity Query = 5.01 – 10 secs Medium complexity query = 10.01 – 15 secs High Complexity query = < 15.1 sec – 1 min	0.5	Simple complexity Query = > 10 secs Medium complexity query = > 15 secs High Complexity query = > 1 min	-1
7	PTZ Lag time (movement at keyboard/joystick and actual moving indication through video feed viewed	< 3 sec	1	3.01 – 5.0 secs	0.5	>5 secs	-1



S. No	Performance Area	Baseline		Lower Performance		Breach	
		Metric	Poi nts	Metric	Poi nts	Metric	Poi nts
8	Maximum time for successful camera settings modification (in online mode)	< 5 sec	0.5	5.01 – 10.0 secs	0.25	>10 secs	-0.5
3. Video Analytics Performance							
1	ANPR for Standard Roman Number plates (3 wheelers & above)	80%	1.5	79.99% to 70%	0.5	< 70 %	-1
2	ANPR for Non-Standard Roman Number plates (3 wheelers & above)	60%	1.5	49.99% to 60%	0.25	< 60 %	-1.3
3	ANPR for Standard Roman Number plates (2 wheelers)	70%	0.3	69.99% to 60%	0.15	< 60 %	-0.3
4	ANPR for Non-Standard Roman Number plates (2 wheelers)	50%	0.2	49.99% to 40%	0.1	< 40 %	-0.2
4. End-User Equipment Uptime							
1	Monitoring workstations at Command Center & Viewing Center	99%	3	>= 97 % to <99%	1	< 97 %	-3
2	Video wall	99%	3	>= 97 % to <99%	1	< 97 %	-3
5. Underlying IT Infrastructure Uptime/Availability at Data Center							
1	Production Servers Uptime	99.982%	4	>= 99.5 % to <99.982%	2	< 99.5 %	-10
2	Storage System Uptime	99.982%	3	>= 99.5 % to <99.982%	1.5	< 99.5 %	-8
3	Physical Security	Fully compliant	1	Lacunae shown in compliance procedures	0.5	For every Noncompliance instance	-2
4	CCTV surveillance of Data Center area	99%	1	97%-99%	0.5	< 97%	-1
5	DG,HVAC,UPS,WLD, Electrical system	99.982%	1	>= 99.5 % to 99.982%	0.5	< 99.5%	-1



S. No	Performance Area	Baseline		Lower Performance		Breach	
		Metric	Poi nts	Metric	Poi nts	Metric	Poi nts
	including panels ,Fire detection and suppression system etc.- uptime						
6. Security /Patch Services for IT Infrastructure							
1	Security rules update within 2 hours of approved change management request	0 violations of service parameters	1	1-4 violations	0.25	> 4 violations	-1
2	Anti-virus, Anti-spyware, Anti-spam updates within 24 hours of request	0 violations of service parameters	1	1-4 violations	0.25	> 4 violations	-1
3	Critical Patches – within 48 hours of patch release.	0 violations of service parameters	0.5	1-4 violations	0.25	> 4 violations	-0.5
4	Non Critical Patches – within 15 days of patch release	Up to 1 violations of service parameters	0.5	2-5 violations	0.25	> 5 violations	-0.5
7. Technical Helpdesk, Issue Resolution							
1	Average Speed of Answer	<= 10 secs	1	10 to 14 secs	0.25	> 14 sec	-1
2	Average Call Lost Rate	0 – 0.5	1	0.5 – 2 %	0.5	> 2 %	-1
3	Resolution of Critical Issue (that impacts more than one production services & higher mgmt. call)	60 minutes	2	60.01 to 120 min	1	>120 min	-2
4	Resolution of Medium Level Issue (that does not impact production services)	120 minutes	1.5	120.01 to 240 min	0.75	>240 min	-1



S. No	Performance Area	Baseline		Lower Performance		Breach	
		Metric	Poi nts	Metric	Poi nts	Metric	Poi nts
			10 0		50		- 10 0

Note: During post-implementation period, in case the pole /outdoor cabinets or any other field equipment is damaged by a vehicular Accident (or due to any other reason outside the control of MSI) and needs repair/replacement, then the corresponding equipment to be replaced by MSI as per the SLAs defined in this section. **In such cases, damages are to be borne by MSI** through proper comprehensive insurance for all the equipment during contract period.

SLA Matrix of Spares for Maintenance and Attendance

The detailed escalation matrix for the entire project needs to be provided by MSI (Phase wise)

S. No	Measurement	Definition	Target	Severity Level
Spares and Maintenance				
1	Repair / replacement of infrastructure equipment including: a. Cameras b. Network Equipment c. Server d. Storage Devices e. Workstations f. UPS (field Unit) g. All other field devices	MSI should keep minimum 5% spare at any given point of project execution. Infrastructure equipment should be replaced or repaired after complaint logging from purchaser officials Measurement Tool: System generated call log at Helpdesk	Within 24 business hours of logging complaints	
			>1 to <=2 calendar days of logging complaint	INR 250 per day for each component
			More than 2 calendar days of logging complaint	INR 1000 per day for each component
Helpdesk availability				
2	Availability of Resources for IT Help Desk at location	[(Total number of man days available for a month) / (Agreed Total number of man days in a month)] *100 There shall be no instance when all the resources for IT Helpdesk are unavailable. This may lead to Severity Level 8 penalty at The discretion of the Purchaser.	>=98 % calculated on monthly basis	
			<= 96% to >98% up time measured on monthly basis	2
			<= 90 % to >96% up time measured on monthly basis	3
			<90.0% up time measured on a	4



		Measurement Tool: SLA Monitoring tool for Online attendance		

Security Breach SLA

Note: This SLA for Security Breach is applicable over and above the SLAs mentioned in above table

Definition	Security of the video feeds and the overall system is quite important and MSI shall be required to ensure no compromise is done on the same. Security Breach types considered for this SLA are • Availability of Video feeds to any other user than those authorized by Delhi Police Department, and provided passwords • Availability of any report / data to any other user than those authorized by the Police Department and provided passwords • Successful hacking of any active component on the network by any unauthorized user • Or any other privacy rule is broken as per Govt. of India guidelines
Service Level Requirement	Security compliance of the system should be 100%
Measurement of Level Service Parameter	Any reported security breach shall be logged into the SLA Management solution as a security breach

Breach in supply of Technical Manpower

Note: This SLA for supply of Technical Manpower is applicable over and above the SLAs mentioned in the above table

Definition	MSI is required to propose the details of the required technical manpower (as mentioned in Scope of work Section). It is vital that such manpower is available to Authority and performs to the expected levels. The current SLA breach shall specify penalty amount for non-availability of these manpower
Service Level Requirement	Availability of the required manpower should be 100%
Measurement of Level Service Parameter	Following instances would be considered as SLA non-compliances: • Replacement of a profile by the MSI (only one replacement per profile would be permitted per year) • Non-deployment of the profile for more than 1 month. Authority reserves the right to ask Service Provider to replace the profile if the performance / commitment is not up to the mark Note: Replacement due to reasons not in control of MSI (like resignation of the resource, accident, etc.) would not be counted in the permissible one replacement.



Explanation Notes for SLA Matrix

A. Camera Availability

Definition	Camera Availability means availability of the camera feed to the command centres/Viewing centres
Measurement of Level Service Parameter	$[(\text{Total average Uptime of all the Cameras in a quarter}) / (\text{Total Time in a quarter})] * 100$

B. Application Availability

Definition	Application availability refers to the total time when the Application is available to the users for performing all activities and tasks
Measurement of Level Service Parameter	$[(\text{Total Uptime of the Application in a quarter}) / (\text{Total Time in a quarter})] * 100$

C. Quality of Feed

Definition	“Poor Quality video feed” means blurred, jiggered, dim or unclear video. Camera Feed Error Resolution time is the time taken to improve the feed to satisfactory levels after it has been detected & logged by the Surveillance System / administrative officials. Logging of such calls would be through helpdesk system
Service Level Requirement	The average availability of the quality of feed should be at 99.94%. This period is excluding the period of unavailability of camera. (i.e. the camera video quality would be judged for the period its available)
Measurement of Level Service Parameter	$[(\text{Total average Uptime of all the Cameras in a quarter} - \text{Total time logged for poor quality video feed}) / (\text{Total average Uptime of all the Cameras in a quarter})] * 100$

D. Issue Resolution

Explanation	Issue Resolution SLA shall monitor the time taken to resolve a complaint / query after it has been reported to the MSI
Service Level Requirement	Different Issues/Queries shall be classified as in following three categories as defined above. Critical: Issue that impacts more than one production services / is raised by higher management / is impacting high importance areas Medium: has a potential to impact or may get escalated to top management if not resolved quickly Low: impact on services

SLA Reporting System:

All the SLA reporting will be based on system generated reports through EMS/ NMS.

The selected MSI shall design, implement/customize the Enterprise Management System (EMS) and shall develop any additional tools required to monitor the performance indicators listed under SLA prescribed in this DPIP. The Acceptance Testing & Certification agency shall verify the accuracy and completeness of the information captured by the SLA monitoring system implemented by the MSI and shall certify the same. The EMS deployed for system, based on SLAs, shall be configured to calculate the monthly transaction-based payout by Delhi Police to MSI. The MSI has to provide an end to end Service Level Management System for the Data Center and other



components under its responsibility. The reports will be submitted to TSP (C-DAC) as the nodal acceptance testing and certifying authority. The MSI will:

- a. Provide end-to-end, comprehensive, modular and integrated management of IT infrastructure components to maximize the availability of IT services and SLA performance.
- b. The management system needs to aggregate events and performance information from the domain managers and tie them to service definitions. This capability is critical for the administrators to have a complete view of the performance and availability of various application services being managed.
- c. The proposed tools should automatically document problems and interruptions for various IT services offered and integrate with the service level management system for reporting on service level agreements (SLAs).
- d. The system must be capable of managing IT resources in terms of the business services they support, specify and monitor service obligations, and associate users/Departments/ Organizations with the services they rely on and related Service/Operational Level Agreements.
- e. Provide a detailed service dashboard view indicating the health of each of the departments / offices in the organization and the health of the services they rely on as well as the SLAs.
- f. Provide a high level view for executives and other users of the system using a real time business services Dashboard.
- g. Provide an outage summary that gives a high level health indication for each service as well as the details and root cause of any outage.
- h. Support for a User Definition Facility to define person(s) or organization(s) that uses the business Services or is a party to a service level agreement contract with a service provider or both. The facility must enable the association of Users with Services and SLAs.
- i. The Service Level Agreements (SLAs) definition facility must support defining a set of one or more service Guarantees that specify the Service obligations stipulated in an SLA contract for a particular time period (weekly, monthly, and so on). Guarantees supported must include one that monitors service availability (including Mean Time to Repair (MTTR), Mean Time between Failure (MTBF), and Maximum Outage Time thresholds) and the other that monitors service transaction response time.
- j. SLA violation alarms must be generated to notify whenever an agreement is violated or is in danger of being violated.
- k. Provide the capability to designate planned maintenance periods for services and take into consideration maintenance periods defined at the IT resources level. In addition, the capability to exempt any service outage from impacting an SLA must be available.

A historical reporting facility that will allow for the generation of on-demand and scheduled reports of Business Service-related metrics with capabilities for customization of the report presentation.



Service Level Change Control

a) General

It is acknowledged that this **Service levels may change as C-DAC's business needs evolve over the course of the contract period**. As such, this document also defines the following management procedures:

- a. A process for negotiating changes to the Service Levels
- b. An issue management process for documenting and resolving particularly difficult issues.
- c. C-DAC and MSI management escalation process to be used in the event that an issue is not being resolved in a timely manner by the lowest possible level of management.

Any changes to the levels of service provided during the term of this Agreement shall be requested, documented and negotiated in good faith by both parties. Either party can request a change.

b) Service Level Change Process:

The parties may amend Service Level by mutual agreement in accordance. Changes can be proposed by either party. Unresolved issues shall also be addressed. MSI's representative shall maintain and distribute current copies of the Service Level document as directed by C-DAC. Additional copies of the current Service Levels shall be available at all times to authorized parties.

c) Version Control / Release Management:

All negotiated changes shall require changing the version control number. As appropriate, minor changes may be accumulated for periodic release or for release when a critical threshold of change has occurred.

4.14 CHANGE Management- Training, Capacity Building

A critical success factor for the success of the project is to get the buy in of the employees and the management by ensuring that they are aware of the benefits that accrue to them out of the project implementation. The MSI will conduct all Change Management sessions for efficient and effective transition of the Department with the envisaged system in place.

As safe city project aims at creating a comprehensive and integrated system for enhancing the efficiency and effectiveness of the Video/CCTV surveillance system through adoption of IT-enabled-state-of-the-art tracking system around public and property safety, it is important the MSI communicate with the employees to ensure their support and eliminate any miscommunication. Further, pervasive use of Technology should be done which requires not only re-skilling the officers but also introducing them to different set of ethics and rules. This may also lead to the change in the organization structures of existing organizations. Thus, change management and capacity building are an imperative part for the success of safe city project which is a key responsibility of the appointed MSI.

Capacity Building for "Safe city project will aim to engender an environment which is apposite for its successful implementation. Capacity Building Framework would primarily include:

Planning for Capacity Building (Training)



- a. Identify Audience & Training Needs
- b. Arrange for Requisite Infrastructure
- c. Monitor & Evaluate Effectiveness
- d. Ensure Sustainability of the CB Programs

Change management

- a. It is crucial that change management and capacity building programmes by MSI form an integral part of the Women Centric safe city project. These initiatives will acquaint the stakeholders to the proposed system and its associated processes.
- b. Furthermore, it will motivate, train and empower the security agency officials to adopt revised/ automated methods of working and appreciate the resultant benefits through the ICCV and VMS systems.
- c. Change management methodology by MSI must keep every stakeholder informed about the changes in the process flow and information management systems. It will empower the officials with the necessary skills and attitude in order to facilitate them in performing their duties in a more effective manner.

Capacity building

It is prudent to build the capacities of the departmental officials who are involved in the operations and decision making, by disseminating the necessary knowledge and skills for smooth implementation of the envisaged processes. It is equally important to generate an attitude that is receptive to a technology based delivery of services. Merely developing, redefining processes and implementing technology will deliver the quality of services envisaged. Henceforth, The MSI will ensure that the concerned officials learn to operate the redesigned services, and efficiently deliver the desired outputs.

Based on the needs and the objectives of the project, training programs would be organized by the MSI with qualifying criterion under the following themes:

- a. Creating awareness about the benefits of Safe City Project and specialized application skills.
- b. Role-based training for people at different levels of monitoring and control.
- c. “Train the Trainer” programs, where members of the staff would be trained to enable them to conduct further training programs, thus helping build up scalability in the training program and also reducing the dependency on external vendors for training.
- d. System Administrator training: a few members of the staff with high aptitude shall be trained to act as system administrators and trouble-shooters for Delhi police.
- e. MSI shall train officers and other staff nominated by the Delhi Police in different aspects of equipment usage, operations, maintenance and repair at each location separately.
- f. The MSI shall at every stage of installation; testing and commissioning provide all facilities for adequate training of the TSP & Delhi Police’s personnel who may be deputed to work on the Projects.
- g. The System Administration and Maintenance Training Program will be structured so as to train Delhi Police Officers/ Personnel.
- h. The user operational training program will be structured so as to train Delhi Police’s supervisory and training personnel per site.
- i. MSI will provide complete details on the training programs to be offered including:



- a) Material to be covered,
 - b) Number of hours of training per operator or technician or supervisors for each specific course; along with all the supporting documents.
- j. MSI shall provide training to the staff of Delhi Police/TSP. The training part should cover the following aspects:
- The system architecture and networking different features of ACD, main switch and servers.
 - Description of call takers, dispatcher console, IP/ digital voice logger, storage, GIS /GPS map etc.
 - Vehicle sub system capabilities with GIS Operation & GPS capability, portable/mobile devices
 - Description of various links and their bandwidth etc.
 - Description of all functional assemblies of the system, including controls, indicators and monitoring system.
 - Tune up procedures for the system and adjustment of operating parameters and other Operation and maintenance procedures.
 - Practical replacement procedures/practices for major assemblies, to the experienced technicians of police in the complete trouble shooting and maintenance of the equipment, both at the board replacement and preferably at the board repair level
 - MIS reports for system health check-up & operation, dashboard features etc.
 - Inventory Management System.
 - All trainings to be completed before Go-live.

Training Audience

Based on the nature of their responsibilities and their requirements from safe city project, Personnel can be classified into the following categories for training purposes:

- a. Key senior officers: Additional Commissioner of Police and above
- b. Other senior level officers: Asst. Commissioner of Police to Deputy Commissioner of Police at the district level.
- c. Key officers (Inspector /Sub-Inspector / Assistant Sub-Inspector)
- d. Lower level officers (Head Constable and Constables), for monitoring at each police station, district and C4I level.

Training Topics

Training will be imparted on following topics:

- 1. Change management
- 2. Team work and Project management



3. Gender sensitizations
4. IT systems and computers
5. Data Center & Network administration
6. Hardware & its maintenance
7. Dashboards and their features along with SOP's
8. VMS
9. ANPR
10. Analytics
11. Cyber security
12. EMS

Other Capacity Building Initiatives

- a. Throughout the duration of the implementation of safe city project, Delhi Police shall try and leverage to the extent possible, existing training institutions including Police Training College, Recruitment training Center, IT training Center and other CCTNS training institutes to train the existing and new recruits in the Delhi Police in order to compensate the additional requirement of trained personnel with the expansion of the project year on year.
- b. Delhi Police will also explore possibilities of partnering with academic institutions for training programs where appropriate.
- c. In addition to the training of the Delhi Police Recruits it is suggested that people with IT education background be directly hired for Data Center & Network Administration and Hardware Installation and Maintenance aspects of the system.
- d. Delhi Police shall be laying increased focus on e-Learning, which makes learning process more engaging and effective. E-Learning systems typically enhance effectiveness by:
 - i. Imparting lessons through graphics, visuals, etc.
 - ii. Use of animation clips to describe a process using audio visual aids
 - iii. Inter Intelligent questioning and taking feedbacks
 - iv. Rolling back to any other previous topics to get a better understanding

Training Schedule

Sr. No.	Name of the Training Program	No. of Days	Batch Size
1	Change management Workshop – Orientation	1	25-30
2	Change management workshop -Automated Operation and Team Work Skills for ICC	1	25-30
3	Training on ICC Operations	2	25-30
4	Work Shop on Gender Sensitization & Police Distress Response Vehicle (Prakhar Van and the likes) Usability	1	40-50
5	Data Center & Network Administration Enterprise & Asset Management Cyber Security	2	15-20
6	Basic Knowledge -Hardware and Software	1	30-40



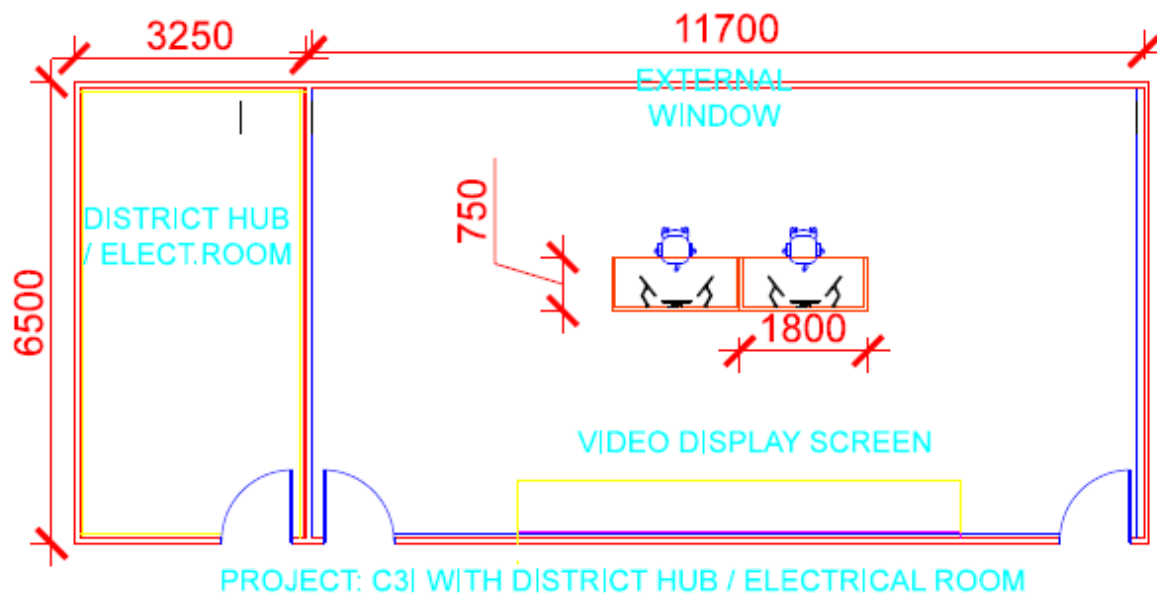
Sr. No.	Name of the Training Program	No. of Days	Batch Size
7	Management Information System (Higher Authorities)	1	15-20

4.15 DC & C4i drawings

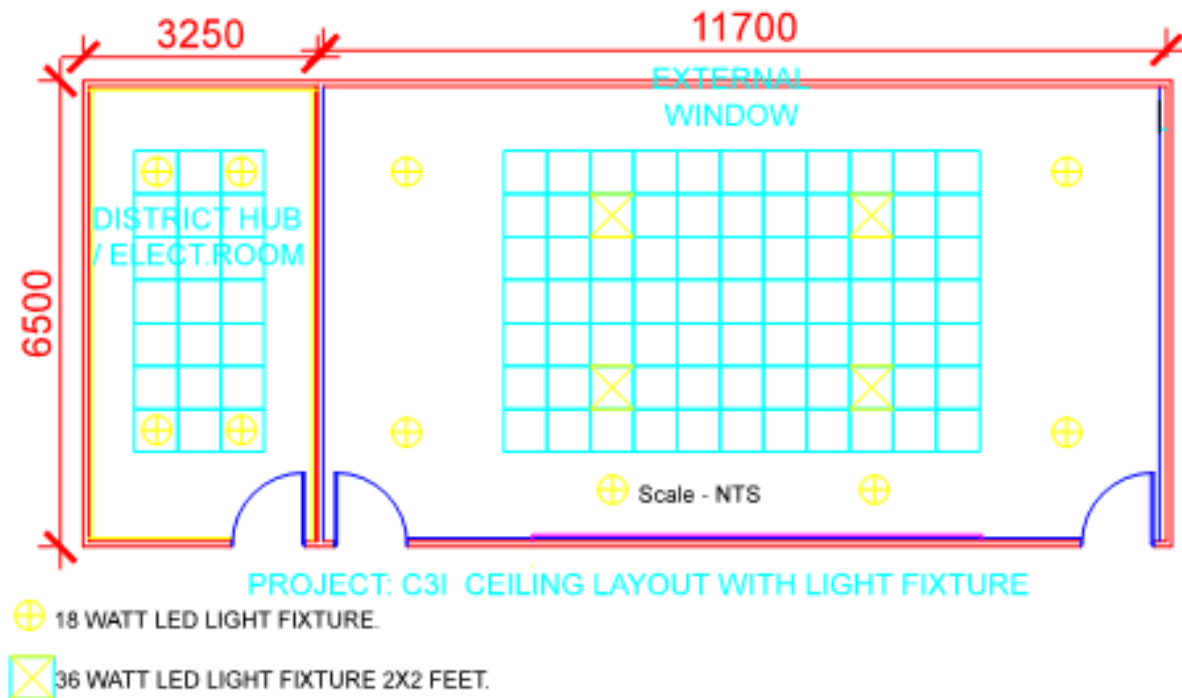
The details of the drawing and other details will be shared post the signing of the Non- Disclosure agreement with MSI.

4.16 Layout drawings of C3i

- a. Electrical Layout at C3i office locations at DHQ (indicative)



- b. Lighting Fixtures' Layout at C3i office locations at DHQ (indicative)



4.17 Certifications for Project components

- All the mandatory component-wise certifications by Competent Authorities (for safety security, IT and Non IT parameters) for ensuring adequate performance levels for the project have been **defined in the Technical Specifications** laid down in the RFP chapter 4.
- All the certifications will be **furnished by the OEM** as a part of the submitted bid which will be an **essential parameter for Technical Evaluation**.
- The OEM will be required to provide **Manufacturing Authorization Form/ Certificate** with the **Country of Origin details** for every Product being provided as a part of Project requirement. It will be the prerogative of the end customer to reject any particular country of origin for product lines offered for the project by the vendor.
- The OEM will submit **Factory Acceptance Certification** for all its products along with the aforementioned certifications.
- The above described certificates will not only benchmark the quality parameters however would also enable to conduct vendor selection without any dispute.
- The bidder will also be required to provide **compliance for all the specifications for the offered product with respect to each functionality** laid down in RFP.
- Also, the installation of every equipment will be considered commissioned and accepted upon successful **Final Testing and User Acceptance Certification**.
- Considering, the certification of the field equipment like poles for successful installation in terms of seismic strength, durability, etc. and the building floor strength a third party inspection can be conducted through Government/ PSU Authorized Institutions like IIT- Delhi, IIT-Powai, IIT-Kharagpur, PDIL, EIL, RITES.
- Further, the entire project will be subjected to STQC and a Third-Party Implementation Audit



by CERT-IN empaneled agency before Go-live operations, which will certify the project implementation as good to proceed with Operation and Maintenance phase in line with the RFP. Also, Third Party Security and Network Performance Audits will be performed every quarter of year by CERT-IN empaneled agency

The summary of all certifications enlisted for every component as below.

S No.	Key Components	Certifications
1	C4i Design and Standards	Green guard gold Certified (Modular Metal Ceiling, Flooring & Modular Metal wall paneling) Integrated Ceiling & Paneling: UL certified The Modular Metal Paneling, Modular Control Desks and Designer Metal Ceiling shall be RoHS certified Test certification for ASTM D2571 for the surface burning characteristics of Modular furniture Tiles Perforation – UL certified UL Certified design feature of Load bearing capacity of Paneling UL Certified design feature of Modular wall Paneling Illumination: - Control Room illumination shall be designed as per ISO 11064 norms. Table-top: ANSI/NEMA LD3 certified scratch-resistant Laminate The Console OEM should be an FSC Certified manufacturer Monitor Arm: - UL certified
2	VideWall Controller and software	All features and functionality should be certified by the OEM.
3	LED Monitor- 55” cubes in a 1 X 2 arrangement	UL/EN/CE/IEC/BIS certification for Safety and CE/FCC Certifications for EMC & Immunity.
4	Workstations'- PSU	80PLUS (Gold Certified) Energy Star Compliant
5	Monitor:	TCO Certified
6	Network Color Laser Printer	BEE or Energy Star certified
7	C4i software- Cyber Security Requirements	TLS encryption with digital certificates to secure the communication channel. Secured media stream requests shall be secured with strong certificate-based authentication leveraging RTSPS (aka RTSP over TLS). AES 128-bit encryption
8	Face Recognition Software for 370 FRS channels	The Vendor should have any performance benchmarking certificate. NIST certificate will be preferred.



9	Service Helpdesk - Incident Management	Pink VERIFY certification on at least 6 available ITIL processes
10	Layer 2 Network Switches - 24 Ports	Efficiency and safety: RoHS, EN 61000-4-5/EN 61000-3-2/ EN 61000-3-11
11	10KVA UPS (for C3i) & 3 KVA (for C2i) with 60 min & 30 min battery backup at 80% load	ISO 9001, ISO 14001, CE Certified
12	Server	Certified for OS: Windows Server 2016 or latest, VMWare vSphere & Viewing Center, Red Hat Enterprise Linux, SUSE Linux Enterprise Server
13	Storage	Security- Write Once Read Many (WORM) compliant to SEC17a-4. OS & other Software Support- It must be certified to support OS like Microsoft Windows Server, HP UX, Red Hat, VMware, Citrix XenServer, IBM AIX, Oracle Solaris, Oracle Linux, Novell NetWare, SLES, etc.
14	L2 Switch (100 Gbps) WAN	RoHS, IPv6 ready for host and router, Fresh Air Compliant
15	Layer 2 TOR Switches - 48 Ports 10G	RoHS, FCC CFR 47 Part 15, EN 61000-4-5: Surge, NDcPP/EAL2
16	Racks with Smart PDU	Rack shall have EIA, UL, RoHS, REACH certified The PDU should be CE certified.
17	Web Application Firewall	ICSA certified WAF functionality.
18	Key Manager for Encryption	Level 3 Certified HSM Card in Appliance or VM
19	Outdoor Fixed Camera - 4MP	CE, FCC, UL/cUL, BIS, NEMA 4X compliant
20	Outdoor PTZ Camera - 4MP, 30x Optical Zoom	CE, FCC, UL/cUL, BIS, NEMA 4X compliant
21	Outdoor Fixed ANPR Camera with IR Illuminator- 2MP	CE, FCC, UL/cUL, BIS, NEMA 4X compliant
22	Pole - for Cameras with 1 mtr ARMs for Fixed Bix & PTZ cameras and with cantilever for ANPR camera	Design and foundation Should be certified from government organization or government empaneled agency
23	Network Access Switches - 8 or more ports	IP 30 rating, DIN Rail Mountable, NEMA-TS2 certification.
24	Junction Box (Surface Mount / Pole Mount)	



		Certified from NABL Accredited Labs
25	UPS (1KVA / 2 KVA)	BIS, CE

Note: Equivalent Indian Standards for all items/equipment will be acceptable; wherever applicable.

4.18 Coordinates of all Police Stations (C2i locations)- district wise and the status of civil infrastructure

The details of the location and coordinates of the sites will be shared post the signing of the Non-Disclosure agreement with MSI.

4.19 Location details of 3351 field sites and the respective number of deployable cameras

The details of the location and coordinates of the sites will be shared post the signing of the Non-Disclosure agreement with MSI.

4.20 Details of the poles to be erected/ installed (5361 no.)

The details of the location and coordinates of the poles to be installed will be shared post the signing of the Non- Disclosure agreement with MSI.

4.21 Important Instructions for Application Software

- If Linux* is quoted as OS, support subscription for 3+2 years shall be included.
- If bidder is proposing any open source software it should be enterprise version with support subscription for 3+2 years.
- All the quoted software and appliances should support offline update mechanism towards patch, firmware, license for software updates
- All the quoted software license should be perpetual in nature.
- The SDK shall provide an extensive list of programming functions to view and/or configure core entities such as: users and user groups, alarms, custom events, and schedules, and more.
- The OEM shall have well documented SDK
- The OEM shall have a structured support program in place to support 3rd party developers using SDK. The program details must be shared along with the technical bid
- The OEM must have well defined support by the means of online portal , Chat and Toll free no to support the SDK developers on timely basis
- The documentations and development process must be published online by the respective OEM



- SDK shall be made available within 2 weeks of release of the new version
- There must be backward version compatibility with the SDK's for at least 3 major releases and all the release notes must be made available online for the development community.
- All type of API shall be developed by vendor within the quote cost.
- MSI will provision min 10 additional application integrations at no extra cost, during the terms of the contract after Go-Live
- MSI shall provide all software on common platform for integrations.

(End of Chapter – 4)

Chapter 5. : Price Bid Format

The bidders must submit the financial bid (.xls file) as per the format given below.

Name of the Bidder/ Bidding Firm / Company :

PRICE SCHEDULE

(This BoQ is for all the phases put together the order will be placed phasewise)

Sl. No.	Item Description	Quantity	Units	Unit Rate in Rs.	GST on Unit Rate in %	Extended Warranty 4th Year Rs. (Lump Sum)	Extended Warranty 5th Year Rs. (Lump Sum)	GST in % on Warranty	Comprehensive AMC 1st Year in Rs. (Lump Sum)	Comprehensive AMC 2nd Year in Rs. (Lump Sum)	Comprehensive AMC 3rd Year in Rs. (Lump Sum)	GST in % on Comprehensive AMC	Total Comprehensive AMC in Rs.	TOTAL AMOUNT in Rs.	TOTAL AMOUNT In Words
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	Integrated Command, Control, Communication and Compute Center at PHQ Delhi (C4i) A.Hardware Component														
1.01	Video Wall Solution- 70" cubes in a 4 X 4 arrangement 3 Video Walls	48	Nos										0.00	0.00	INR Zero Only
1.02	Video Wall Controller	4	Nos										0.00	0.00	INR Zero Only
1.03	LED Monitor- 55" cubes in a 1 X 2 arrangement	4	Nos										0.00	0.00	INR Zero Only
1.04	Workstation for LED Monitors	2	Nos										0.00	0.00	INR Zero Only
1.05	Workstations with 3 nos. 24" UHD Touch Monitors for C4i application at multiple rooms on 6th & 7th Floor (EoC) Mike + webcam +speaker along with operator workstation	16	Nos										0.00	0.00	INR Zero Only
1.06	Video Wall Software	1	Nos										0.00	0.00	INR Zero Only
1.07	Workstations with 3 nos. 24" UHD Touch Monitors for C4i application with Mike + webcam +speaker along with operator workstation	21	Nos										0.00	0.00	INR Zero Only
1.08	Network Colour Laser Printer	5	Nos										0.00	0.00	INR Zero Only



RFP- for selection of MSI for implementation and O&M of surveillance System
under Safe City Project of Delhi Police



1.09	IP Phones	39	Nos										0.00	0.00	INR Zero Only
1.11	Display port/ HDMI splitter (for C4i & C3i + C2i)	50	Nos										0.00	0.00	INR Zero Only
1.12	Racks 42U with Smart PDU	2	Nos										0.00	0.00	INR Zero Only
1.13	Workstation for Video wall without Monitor	16	Nos										0.00	0.00	INR Zero Only
1.14	Switch L2	14	Nos										0.00	0.00	INR Zero Only
1.15	Joystick for PTZ camera at Workstation	39	Nos										0.00	0.00	INR Zero Only
1.16	55" LED TV	4	Nos										0.00	0.00	INR Zero Only
1.17	Dual TV Stand with Power distribution	2	Nos										0.00	0.00	INR Zero Only
2	Integrated Command, Control, Communication and Compute Center at PHQ Delhi (C4i) B.Software Component														
2.01	C4i Software including following modules - Software Component 1. ICCC Base platform with GIS engine, reporting, real-time dashboard, User Interface and Alarm Management with unrestricted client connections 2. Threat Level Engine 3. Big data correlation Tool with crime insights 4. Incident Management, Rules Engine, Decision Management and collaboration tool 5. Active directory Integration or equivalent 6. Mobile App with unrestricted connections	1	Nos										0.00	0.00	INR Zero Only
2.02	Automatic Vehicle Location System (AVLS)	1	Nos										0.00	0.00	INR Zero Only
2.03	Computer Aided Dispatch Software (CAD)	1	Nos										0.00	0.00	INR Zero Only
2.04	GPS Location Based Services and GIS Software	1	Nos										0.00	0.00	INR Zero Only



RFP- for selection of MSI for implementation and O&M of surveillance System
under Safe City Project of Delhi Police



2.05	Video Management & Recording Software – 10,000 camera licenses + 1000 cameras floating licensing for existing camera integration	11000	Nos										0.00	0.00	INR Zero Only
2.06	Video Analytics Software for 2500 cameras (2 use cases on an average per camera)	5000	Nos										0.00	0.00	INR Zero Only
2.07	Face Recognition Software for 370 FRS channels	370	Nos										0.00	0.00	INR Zero Only
2.08	Automatic Number/ License Plate Recognition Software with licensing	1622	Nos										0.00	0.00	INR Zero Only
2.09	Video Summarization and Forensic Software	1	Nos										0.00	0.00	INR Zero Only
2.1	PIU (Picture Intelligence Unit) Software	1	Nos										0.00	0.00	INR Zero Only
2.11	Customized Interface software for integration with a. Community Surveillance b. CCTNS c. VAHAN d. Himmat plus App e. Dial 112 and other databases - Total 32 databases	1	Nos										0.00	0.00	INR Zero Only
2.12	LDAP Software to cater the offered solution	1	Nos										0.00	0.00	INR Zero Only
2.13	SQL Server 2019 Standard License for offered solution	2	Nos										0.00	0.00	INR Zero Only
2.14	Enterprise Management System including SLA Management, Network Management, Asset Management, Incident & Work Flow Management, Privilege & Identity Management.	1	Nos										0.00	0.00	INR Zero Only
2.15	Helpdesk Management	1	Nos										0.00	0.00	INR Zero Only
2.16	Internal Audit: Half yearly for network and applications and operations (refer para 2.2.7 of chapter 2 of RFP)	10	Nos										0.00	0.00	INR Zero Only
2.17	External Audit: Yearly for network and applications and operations (refer para 2.2.7 of chapter 2 of RFP)	5	Nos										0.00	0.00	INR Zero Only
2.18	Security Software Tools and commissioning support of all software- additional licenses, etc.	1	Nos										0.00	0.00	INR Zero Only



RFP- for selection of MSI for implementation and O&M of surveillance System
under Safe City Project of Delhi Police



3	District Command, Control & Communication Center at 16 District Headquarters (C3I)														
3.01	Workstations with 3 nos. 24" Monitors Mike + webcam +speaker along with operator workstation	57	Nos										0.00	0.00	INR Zero Only
3.02	LED Monitor- 55" monitor displays	48	Nos										0.00	0.00	INR Zero Only
3.03	Workstations for LED Display without Monitor	16	Nos										0.00	0.00	INR Zero Only
3.04	Network Colour Laser Printer	16	Nos										0.00	0.00	INR Zero Only
3.05	IP Phones	57	Nos										0.00	0.00	INR Zero Only
3.06	Secure Network Device - SD WAN Router	16	Nos										0.00	0.00	INR Zero Only
3.07	Layer 2 Network Switches - 24 Ports	16	Nos										0.00	0.00	INR Zero Only
3.08	Network Racks 16U	16	Nos										0.00	0.00	INR Zero Only
3.09	Networking Cost (Passive Components)	16	Nos										0.00	0.00	INR Zero Only
3.1	10KVA UPS with 30 min battery backup at 80% load	32	Nos										0.00	0.00	INR Zero Only
3.11	Comfort AC 1.5/ 2 Ton	32	Nos										0.00	0.00	INR Zero Only
3.13	Edge Gateway for Community Surveillance	50	Nos										0.00	0.00	INR Zero Only
3.14	Joystick for PTZ camera at Workstation	57	Nos										0.00	0.00	INR Zero Only
4	Local Monitoring Center at 182 Police Stations (C2i)														
4.01	Workstations with 3 nos. 24" Monitors for C4i application Mike + webcam +speaker along with operator workstation	240	Nos										0.00	0.00	INR Zero Only
4.02	LED Monitor- 55" monitor displays	81	Nos										0.00	0.00	INR Zero Only
4.03	Workstations for LED Display without Monitor	70	Nos										0.00	0.00	INR Zero Only



RFP- for selection of MSI for implementation and O&M of surveillance System
under Safe City Project of Delhi Police



4.04	IP Phones	240	Nos										0.00	0.00	INR Zero Only
4.05	Secure Network Device - SD WAN Router	182	Nos										0.00	0.00	INR Zero Only
4.06	Network laser printer	182	Nos										0.00	0.00	INR Zero Only
4.07	Layer 2 Network Switches - 24 Ports	182	Nos										0.00	0.00	INR Zero Only
4.08	Network Racks 16U	182	Nos										0.00	0.00	INR Zero Only
4.09	Networking Cost (Passive Components) for each C2i as per the solution offered	182	Nos										0.00	0.00	INR Zero Only
4.1	3KVA UPS with 30 min battery backup at 80% load	174	Nos										0.00	0.00	INR Zero Only
4.11	10KVA UPS with 30 min battery backup at 80% load	8	Nos										0.00	0.00	INR Zero Only
4.12	Comfort AC 1.5 Ton	182	Nos										0.00	0.00	INR Zero Only
4.14	Joystick for PTZ camera at Workstation	240	Nos										0.00	0.00	INR Zero Only
5	Mobile Command Control Vehicle (MCCV)- For 02 Vehicles														
5.01	Chassis: WB 4200mm (approx.) from reputed OEM like TATA, Eicher, Ashok Leyland etc.	2	Nos										0.0	0.00	INR Zero Only
5.02	Custom designed & Fabricated Mobile Command Control Vehicle	2	Nos										0.0	0.00	INR Zero Only
5.03	Split Air Conditioner (1Ton)	2	Nos										0.0	0.00	INR Zero Only
5.04	Interiors design (as per the requirement)- for 02 Vehicles	1	Lump-sum										0.0	0.00	INR Zero Only
5.05	Chairs / Seating Arrangement for two Operator and one ICS	6	Nos										0.0	0.00	INR Zero Only
5.06	Chairs / Seating Arrangement for Supervisor with mini seating area	2	Nos										0.0	0.00	INR Zero Only
5.07	Console with provision for display	4	Nos										0.0	0.00	INR Zero Only



RFP- for selection of MSI for implementation and O&M of surveillance System
under Safe City Project of Delhi Police



5.08	Inter- communication Service Console	2	Nos										0.0	0.00	INR Zero Only
5.09	19" Rack with shock & vibration isolators for electronic	2	Nos										0.0	0.00	INR Zero Only
5.1	Mast	2	Nos										0.0	0.00	INR Zero Only
5.11	Storage	2	Nos										0.0	0.00	INR Zero Only
5.12	PC for Operator	4	Nos										0.0	0.00	INR Zero Only
5.13	32" LED Full HD TV	4	Nos										0.0	0.00	INR Zero Only
5.14	5KVA UPS System with Batteries for 1 hour backup	2	Nos										0.0	0.00	INR Zero Only
5.15	7.5 KVA Silent Petrol Generator Set	2	Nos										0.0	0.00	INR Zero Only
5.16	Vehicle Mast mounted PTZ Camera with Keyboard and Joystick	2	Nos										0.0	0.00	INR Zero Only
5.17	Vehicle mounted full HD Bullet Cameras	4	Nos										0.0	0.00	INR Zero Only
5.18	Industrial PC based Network Video Recorder	2	Nos										0.0	0.00	INR Zero Only
5.19	Video Management System	2	Nos										0.0	0.00	INR Zero Only
5.2	Standalone Mobile Hand-held device	2	Nos										0.0	0.00	INR Zero Only
5.21	4 SIM based 4G Aggregator Device with Dongles	2	Nos										0.0	0.00	INR Zero Only
5.22	Network Hardware:- - 1 x 24Port GigE Switch	2	Nos										0.0	0.00	INR Zero Only
5.23	32" or better LED Full HD Video Display	2	Nos										0.0	0.00	INR Zero Only
5.24	Vehicle Mounted Water Dispenser	2	Nos										0.0	0.00	INR Zero Only



RFP- for selection of MSI for implementation and O&M of surveillance System
under Safe City Project of Delhi Police



5.25	LED Flood Lights with 120-degree coverage (Mast Mounted)	6	Nos										0.0	0.00	INR Zero Only
5.26	Top Bar Light with Siren	2	Nos										0.0	0.00	INR Zero Only
5.27	PA System with 4 Speakers	2	Nos										0.0	0.00	INR Zero Only
5.28	Fire Extinguisher	8	Nos										0.0	0.00	INR Zero Only
5.29	First-Aid Box	2	Nos										0.0	0.00	INR Zero Only
5.3	4G Based live TV Streaming Device	2	Nos										0.0	0.00	INR Zero Only
5.31	Integration, Testing, Installation, Commissioning & Training	2	Nos										0.0	0.00	INR Zero Only
5.32	Interoperable Communication System with Operator Display, Pedal PTT, Speakers, GSM Modem, PTT Desk Mic & Record-Replay features.	2	Nos										0.0	0.00	INR Zero Only
5.33	Provision of Integration of APCO-P25 Radio Communication channel at MCCV	2	Nos										0.0	0.00	INR Zero Only
5.34	4G Aggregator/ Bonding Receiver with Unlimited bonding License	1	Nos										0.0	0.00	INR Zero Only
5.35	SIM recurring charges for MCCV (16 SIM)- Annual	5	Nos										0.0	0.00	INR Zero Only
5.36	Price of MCCV Vehicle	2	Nos										0.0	0.00	INR Zero Only
6	Data Centre														
	a. Servers														
6.01	C4I Servers at ICCV (PHQ)	2	Nos										0.00	0.00	INR Zero Only
6.02	Integration Servers	3	Nos										0.00	0.00	INR Zero Only
6.03	Video Management Servers	2	Nos										0.00	0.00	INR Zero Only
6.04	Video Recording Servers	60	Nos										0.00	0.00	INR Zero Only



RFP- for selection of MSI for implementation and O&M of surveillance System
under Safe City Project of Delhi Police



6.05	Video Analytics Servers with 3x GPU in each server for 2500 cameras each having 2 use cases on an average	42	Nos										0.00	0.00	INR Zero Only
6.06	Face Recognition Servers with 3x GPU in each server for 370 FRS Channels	20	Nos										0.00	0.00	INR Zero Only
6.07	AI Training and Continuous Learning Server	2	Nos										0.00	0.00	INR Zero Only
6.08	ANPR Servers for 1622 Channels	44	Nos										0.00	0.00	INR Zero Only
6.09	PIU (Picture Intelligence Unit) Server	2	Nos										0.00	0.00	INR Zero Only
6.1	Video Summarization/ Synopsis and Forensics Server	4	Nos										0.00	0.00	INR Zero Only
6.11	Domain Controller, EMS server	2	Nos										0.00	0.00	INR Zero Only
6.12	Antivirus Server- AI based	1	Nos										0.00	0.00	INR Zero Only
6.13	LDAP Server	1	Nos										0.00	0.00	INR Zero Only
6.14	Viewing Center Management Server	4	Nos										0.00	0.00	INR Zero Only
6.15	DLP Server	1	Nos										0.00	0.00	INR Zero Only
6.16	MFA Server + PKI Server	1	Nos										0.00	0.00	INR Zero Only
6.17	b. Storage Scale out Storage for surveillance video data for 30 days - 20 PB	1	Nos										0.00	0.00	INR Zero Only
6.18	SAN storage for database, boot, Flagged Data and Backup for 90 days - 2 PB	1	Nos										0.00	0.00	INR Zero Only
6.19	SAN Switches	4	Nos										0.00	0.00	INR Zero Only
6.2	c. Networking L2 Switch (100 Gbps) WAN	2	Nos										0.00	0.00	INR Zero Only
6.21	Layer 3 Core Switches - 48 ports 100G	4	Nos										0.00	0.00	INR Zero Only



RFP- for selection of MSI for implementation and O&M of surveillance System
under Safe City Project of Delhi Police



6.22	Layer 2 TOR Switches - 48 Ports 10G	4	Nos										0.00	0.00	INR Zero Only
6.23	L2/ KVM Management Switches	15	Nos										0.00	0.00	INR Zero Only
6.24	Layer 2 TOR Switches - 48 Ports 10G	15	Nos										0.00	0.00	INR Zero Only
6.25	Racks with Smart PDU	30	Nos										0.00	0.00	INR Zero Only
6.26	d. Security Firewall- 100 gig streaming throughput	2	Nos										0.00	0.00	INR Zero Only
6.27	IPS & Ddos for 65 Gig throughput	2	Nos										0.00	0.00	INR Zero Only
6.28	VAPT for 170000IP bands (IP Schema)	1	Nos										0.00	0.00	INR Zero Only
6.29	WAF (1 gig internet data)	2	Nos										0.00	0.00	INR Zero Only
6.3	Secure Network Device - SD WAN Router	2	Nos										0.00	0.00	INR Zero Only
6.31	Anti-APT (sandboxing)	2	Nos										0.00	0.00	INR Zero Only
6.32	Anti-virus- AI Based software	450	Nos										0.00	0.00	INR Zero Only
6.33	Data Leakage Prevention (DLP)	450	Nos										0.00	0.00	INR Zero Only
6.34	SIEM Appliance	1	Nos										0.00	0.00	INR Zero Only
6.35	Backup Appliance & Solution	1	Nos										0.00	0.00	INR Zero Only
6.36	AAA Server (NAC)	1	Nos										0.00	0.00	INR Zero Only
6.37	Network Load Balancer	1	Nos										0.00	0.00	INR Zero Only
6.38	Multi-Factor Authentication (with Finger print biometric and hard token devices) at all workstations	450	Nos										0.00	0.00	INR Zero Only



RFP- for selection of MSI for implementation and O&M of surveillance System
under Safe City Project of Delhi Police



6.39	Virtualization license for 77 Physical Servers using 02 Sockets each server	154	Nos										0.00	0.00	INR Zero Only
6.4	18 server Virtualization license for 18 servers using 02 Sockets each server (Used for DMZ)	36	Nos										0.00	0.00	INR Zero Only
6.41	Windows/Linux* OS (for 73 Server) a. OS Licenses for VMS Servers (Widows Data Center addition/ Linux* with 3+2 years support subscription) - 2 b. OS Licenses for Recording Servers (Widows Data Center addition/ Linux* with 3+2 years support subscription) - 60 c. Widows Data Center addition licenses - 11	73	Nos										0.00	0.00	INR Zero Only
6.43	e. NOC Layer 2 Network Switch 24 Ports	2	Nos										0.00	0.00	INR Zero Only
6.44	Wall mount 9U Rack for Switches	1	Nos										0.00	0.00	INR Zero Only
6.45	Workstation with single Monitor 24" for Management	3	Nos										0.00	0.00	INR Zero Only
6.46	IP Phone	3	Nos										0.00	0.00	INR Zero Only
6.47	Operator Console Desk	3	Nos										0.00	0.00	INR Zero Only
6.48	SMS Gateway (for alarms & notifications)	1	Nos										0.00	0.00	INR Zero Only
6.49	Laptop	5	Nos										0.00	0.00	INR Zero Only
6.5	IPPBX / Recording server + software	1	Nos										0.00	0.00	INR Zero Only
6.51	Installation, Configuration etc. and overall management	1	Nos										0.00	0.00	INR Zero Only
6.52	f. Non IT Component UPS (15 minutes backup) - 400 KVA	2	Nos										0.00	0.00	INR Zero Only
6.53	DG Set - 1000 KVA	1	Nos										0.00	0.00	INR Zero Only
6.54	g. Operation and Maintenance Operation and maintenance cost for	4	Years										0.00	0.00	INR Zero Only



RFP- for selection of MSI for implementation and O&M of surveillance System
under Safe City Project of Delhi Police



	4 years for Data Centre Non-IT Equipment only														
7	Near Disaster Recovery Center Hardware														
7.01	C4i Servers,Video management Servers,Server (Recording),ANPR Servers,Domain Controller,Antivirus Server,LDAP Server	11	Nos										0.00	0.00	INR Zero Only
7.02	Viewing Centre Management Server	1	Nos										0.00	0.00	INR Zero Only
7.03	Video Analytics Servers with 3x GPU in each server	4	Nos										0.00	0.00	INR Zero Only
7.04	Face Recognition Servers with 3x GPU in each server	3	Nos										0.00	0.00	INR Zero Only
7.05	Storage of application and tagged data (2 PB storage)- SAN/ Unified	1	Nos										0.00	0.00	INR Zero Only
7.06	L3 Switch 24 Port 10/25 GB	2	Nos										0.00	0.00	INR Zero Only
7.07	L2 Switch 24 Port 1GB	2	Nos										0.00	0.00	INR Zero Only
7.08	SAN Switch 12 port	2	Nos										0.00	0.00	INR Zero Only
7.09	RACK	4	Nos										0.00	0.00	INR Zero Only
7.1	Firewall- 3 Gig, IPS, DDoS, Anti-APT, VAPT, server security- 3 GB throughput	2	Nos										0.00	0.00	INR Zero Only
7.11	Network Load Balancer (NLB)	1	Nos										0.00	0.00	INR Zero Only
7.12	a) Virtualization Physical Servers	12	Nos										0.00	0.00	INR Zero Only
7.13	b) Server Virtualization Security	12	Nos										0.00	0.00	INR Zero Only
7.14	c) Windows OS Server	11	Nos										0.00	0.00	INR Zero Only
7.15	d) Civil, electrical wherever required	1	Lots										0.00	0.00	INR Zero Only
8	Field Devices														



RFP- for selection of MSI for implementation and O&M of surveillance System
under Safe City Project of Delhi Police



8.01	Outdoor Fixed Camera - 4MP	6121	Nos										0.00	0.00	INR Zero Only
8.02	Outdoor PTZ Camera - 4MP, 30x Optical Zoom and joystick control operations	2246	Nos										0.00	0.00	INR Zero Only
8.03	Outdoor Fixed ANPR Camera with IR Illuminator- 2 MP	1622	Nos										0.00	0.00	INR Zero Only
8.04	Poles - for Cameras with 1 mtr ARMS for fixed and PTZ	3802	Nos										0.00	0.00	INR Zero Only
8.05	Poles - Cantilever Poles for ANPR Cameras	1559	Nos										0.00	0.00	INR Zero Only
8.06	Network Access Switches - 8 or more ports	4633	Nos										0.00	0.00	INR Zero Only
8.07	Gun Shot solution	200	Nos										0.00	0.00	INR Zero Only
8.08	Public Address System + loudspeaker at 182(C2i) +16(C3i) +2(C4i) + 100(field) = 300 identified spots (locations) centrally regulated at C4i	300	Nos										0.00	0.00	INR Zero Only
8.09	Junction Box - Floor mounted (including last mile passive networking, earthing, etc.)	1201	Nos										0.00	0.00	INR Zero Only
8.1	Junction Box - Pole mounted (including last mile passive networking, earthing, etc.)	3432	Nos										0.00	0.00	INR Zero Only
8.11	Cat6A/ E Cable (UTP)	5500 00	Mtr.										0.00	0.00	INR Zero Only
8.12	Power Cable - Armoured 2 core 1.5 square MM	5000 00	Mtr.										0.00	0.00	INR Zero Only
8.13	Power-cable - Unarmoured 1.5 Square MM for Equipment Power with 3 PIN Top	5176 0	Mtr.										0.00	0.00	INR Zero Only
8.14	12 port loaded LIU with LC port for OFC Termination at Junction Poles	4633	Nos.										0.00	0.00	INR Zero Only
8.15	8 Port loaded Jack Panel for CAT-6 Cables	4633	Nos.										0.00	0.00	INR Zero Only
8.16	SN Duplex LC-LC Duplex Patch Cord	9266	Nos.										0.00	0.00	INR Zero Only
8.17	Surge Protector - single port internet RJ-45 Plug-in Surge	1000 0	Nos.										0.00	0.00	INR Zero Only



RFP- for selection of MSI for implementation and O&M of surveillance System
under Safe City Project of Delhi Police



	Protector for PoE and PoE+ for All field cameras and L2 Switches													
8.18	1 mtr. Patch Cord from jack panel to surge Protector & Vice-Versa	21064	Nos.									0.00	0.00	INR Zero Only
8.19	Field Terminal Connector	9989	Nos.									0.00	0.00	INR Zero Only
8.2	16 AMP DP-MCB for Mains INPUT at Junction Box	4633	Nos.									0.00	0.00	INR Zero Only
8.21	06-16 combine switch socket Box for UPS input	4633	Nos.									0.00	0.00	INR Zero Only
8.22	24 VAC 5 AMP Power supply for ANPR IR	1622	Nos.									0.00	0.00	INR Zero Only
8.23	Birds care for camera	9989	Nos.									0.00	0.00	INR Zero Only
8.24	Digging, Piping & Re-filling (Trenching and Restoration)	782480	Mtr.									0.00	0.00	INR Zero Only
8.25	Earthing - 2 Mtrs GI with 25x3 GI strip connectivity to junction boxes	1201	Nos									0.00	0.00	INR Zero Only
8.26	Earthing - 1 Mtrs with 8mm GI wire for connectivity to Boxes	5361	Nos									0.00	0.00	INR Zero Only
8.27	1KVA, 2KVA UPS (60 minutes backup) - for camera	4633	Nos									0.00	0.00	INR Zero Only
8.28	Mobile hand held devices for Police Officials	220	Nos									0.00	0.00	INR Zero Only
8.29	Any Additional Components including certification required for the field devices such as: - Transit insurance - Temporary storage Warehouse & watchmen cost - Field device insurance like camera etc. after deployment - Fencing of poles if required - Vehicles need to hire for engineer for supervising purpose at the time of installation period and for post installation purpose as well - Electrical tape, OFC Marker, feruling & node points numbering, OTDR machine, Tie, cable manager, GI heavy grade conduit, - Toolkit (spanner set, multimeter, digital analyser, screwdriver set,	1	Lot									0.00	0.00	INR Zero Only



RFP- for selection of MSI for implementation and O&M of surveillance System
under Safe City Project of Delhi Police



	torch etc) at every police station - Pest control & sanitization at C4i, C3i, C2i - 2 times in a year - First aid kit at every control room														
9	Operations & Management - Indicative Technical Manpower -MSI can give price of manpower in each head as per the requirement in Phase-I, Phase-II, Phase-III, Phase -IV and TO MEET THE SLA														
9.01	Manager - DC, C4i, C3i and C2i: 1 manager for Contract Period	3	Per person Per year										0.00	0.00	INR Zero Only
9.02	C4i Expert: 2 for Contract Period	6	Per person Per year										0.00	0.00	INR Zero Only
9.03	System Administrator: 6 for Contract Period	18	Per person Per year										0.00	0.00	INR Zero Only
9.04	Network and Security Manager along with Field Network Technician: 10 for Contract Period	30	Per person Per year										0.00	0.00	INR Zero Only
9.05	Storage Administrator: 4 for Contract Period	12	Per person Per year										0.00	0.00	INR Zero Only
9.06	Enterprise & Asset Manager : 2 for Contract Period	6	Per person Per year										0.00	0.00	INR Zero Only
9.07	Database Administrator: 1 for Contract Period	3	Per person Per year										0.00	0.00	INR Zero Only
10	Operation power charges														
10.01	Power Meter Charges (Installation & Others)(minus of pilot district)	3788	Nos										0.00	0.00	INR Zero Only
10.02	Power cabling from meter to site and miscellaneous	1	Lump-sum										0.00	0.00	INR Zero Only
10.03	Power meter & charges for Pilot (2 Districts) (unit rate till go-live of 1st phase)	845	Nos										0.00	0.00	INR Zero Only
11	Training and Change management														
11.01	Training schedule for trainees ((5080 trainees)	1	Nos										0.00	0.00	INR Zero Only
12	Manpower Deployment														
12.01	Operator at C2i: 240 operators for 03 years	720	Unit Rate Per Annum										0.00	0.00	INR Zero Only
12.02	Operator at C3i: 57 operators per shift * 3 shifts for 03 years	513	Unit Rate Per Annum										0.00	0.00	INR Zero Only
12.03	Operator at C4i: 21 operators per shift * 3 shifts for 03 years	189	Unit Rate Per Annum										0.00	0.00	INR Zero Only



RFP- for selection of MSI for implementation and O&M of surveillance System
under Safe City Project of Delhi Police



12.04	Supervisor/Manager at C4i: 3 for 03 years	9	Unit Rate Per Annum										0.00	0.00	INR Zero Only
12.05	Operator- Manpower at C2i for 2 Pilot Districts (approx. 27 Police Station) (till Go live of Phase 1)	41	Unit Rate Per Annum										0.00	0.00	INR Zero Only
12.06	Operator- Manpower at C3i for 2 Pilot Districts (till Go live of Phase 1)	27	Unit Rate Per Annum										0.00	0.00	INR Zero Only
12.07	Operator- Manpower at C4i for 2 Pilot Districts (till Go live of Phase 1)	15	Unit Rate Per Annum										0.00	0.00	INR Zero Only
13	Media campaigning and citizen awareness														
13.01	Media campaigning and citizen awareness	1	Lump-sum										0.00	0.00	INR Zero Only
14	Miscellaneous														
14.01	Pentascanning & Certification	1	Lump-sum										0.00	0.00	INR Zero Only
14.02	Insurance	1	Lump-sum										0.00	0.00	INR Zero Only
14.03	Travel Allowance	1	Lump-sum										0.00	0.00	INR Zero Only
14.04	Watchmen	1	Lump-sum										0.00	0.00	INR Zero Only
14.05	Warehouse on Rent to store field material	1	Lump-sum										0.00	0.00	INR Zero Only
14.06	Network Dressing	1	Lump-sum										0.00	0.00	INR Zero Only
14.07	Risk - Power Charges, ROW, RI Charges, Taxation	1	Lump-sum										0.00	0.00	INR Zero Only
14.08	2% Inventory spares to maintain SLA	1	Lump-sum										0.00	0.00	INR Zero Only
14.09	Additional Requirement in C4i for Interior	1	Lump-sum										0.00	0.00	INR Zero Only
14.1	Additional Furniture, Chairs, Tables	1	Lump-sum										0.00	0.00	INR Zero Only
14.11	Diesel for C4i till Go-live	1	Lump-sum										0.00	0.00	INR Zero Only



RFP- for selection of MSI for implementation and O&M of surveillance System
under Safe City Project of Delhi Police



14.12	Insurance to Manpower working in the field	1	Lump-sum										0.00	0.00	INR Zero Only
14.13	Freight Insurance	1	Lump-sum										0.00	0.00	INR Zero Only
14.14	Light Bar for vehicles & poles	1	Lump-sum										0.00	0.00	INR Zero Only
14.15	Logo Embossing on every equipment	1	Lump-sum										0.00	0.00	INR Zero Only
14.16	Battery Replacement, Theft in the field, etc.	1	Lump-sum										0.00	0.00	INR Zero Only
14.17	External DVD writers	5	Lump-sum										0.00	0.00	INR Zero Only
14.18	Others	1	Lump-sum										0.00	0.00	INR Zero Only
15	C4I Non-IT (Details of Non-IT components are given in the RFP and Reference is given in the items below, cumulative price should be mentioned against items)														
15.01	Demolition and Cartage Of Rubbish (Chapter-3>3.1>3.1.2>Refer Civil Works and interiors of C4i)	1	Lump-sum										0.00	0.00	INR Zero Only
15.02	Civil Works(Chapter-3>3.1>3.1.2>Refer Civil Works and interiors of C4i)	1	Lump-sum										0.00	0.00	INR Zero Only
15.03	Joinery (Chapter-3>3.1>3.1.2>Refer Civil Works and interiors of C4i)	1	Lump-sum										0.00	0.00	INR Zero Only
15.04	Doors (Chapter-3>3.1>3.1.2>Refer Civil Works and interiors of C4i)	1	Lump-sum										0.00	0.00	INR Zero Only
15.05	Ceiling (Chapter-3>3.1>3.1.2>Refer Civil Works and interiors of C4i)	1	Lump-sum										0.00	0.00	INR Zero Only
15.06	Finishes (Chapter-3>3.1>3.1.2>Refer Civil Works and interiors of C4i)	1	Lump-sum										0.00	0.00	INR Zero Only
15.07	Built in storages (Chapter-3>3.1>3.1.2>Refer Civil Works and interiors of C4i)	1	Lump-sum										0.00	0.00	INR Zero Only
15.08	Flooring (Chapter-3>3.1>3.1.2>Refer Civil Works and interiors of C4i)	1	Lump-sum										0.00	0.00	INR Zero Only



RFP- for selection of MSI for implementation and O&M of surveillance System
under Safe City Project of Delhi Police



15.09	Signage (Chapter-3>3.1>3.1.2>Refer Civil Works and interiors of C4i)	1	Lump-sum										0.00	0.00	INR Zero Only
15.1	Loose Furniture (Chapter-3>3.1>3.1.2>Refer Civil Works and interiors of C4i)	1	Lump-sum										0.00	0.00	INR Zero Only
15.11	Misc. Items (Chapter-3>3.1>3.1.2>Refer Civil Works and interiors of C4i)	1	Lump-sum										0.00	0.00	INR Zero Only
15.12	Electrical (Chapter-3>3.1>3.1.2>Refer Civil Works and interiors of C4i)	1	Lump-sum										0.00	0.00	INR Zero Only
15.13	CONDUITS AND MS PAINTED CHANNELS FOR STRUCTURED CABLING (Chapter-3>3.1>3.1.2>Refer Civi+B26I Works and interiors of C4i)	1	Lump-sum										0.00	0.00	INR Zero Only
15.14	INSTALLATION OF PANELS; SUPPLY AND INSTALLATION OF DB, CABLES AND EARTHING (Chapter-3>3.1>3.1.2>Refer Civil Works and interiors of C4i)	1	Lump-sum										0.00	0.00	INR Zero Only
15.15	SUPPLY OF LIGHTING FIXTURES (Chapter-3>3.1>3.1.2>Refer Civil Works and interiors of C4i)	1	Lump-sum										0.00	0.00	INR Zero Only
15.16	FIXING OF LIGHTING FIXTURES (Chapter-3>3.1>3.1.2>Refer Civil Works and interiors of C4i)	1	Lump-sum										0.00	0.00	INR Zero Only
15.17	CONSTRUCTION POWER AND LIGHTING (Chapter-3>3.1>3.1.2>Refer Civil Works and interiors of C4i)	1	Lump-sum										0.00	0.00	INR Zero Only
15.18	Networking (Chapter-3>3.1>3.1.2>Refer Civil Works and interiors of C4i)	1	Lump-sum										0.00	0.00	INR Zero Only
15.19	ACS, FDS, RRS (Chapter-3>3.1>3.1.2>Refer Civil Works and interiors of C4i)	1	Lump-sum										0.00	0.00	INR Zero Only
15.2	UPS System (Chapter-3>3.1>3.1.2>Refer Civil Works and interiors of C4i)	1	Lump-sum										0.00	0.00	INR Zero Only
15.21	Carpet (Chapter-3>3.1>3.1.2>Refer Civil Works and interiors of C4i)	1	Lump-sum										0.00	0.00	INR Zero Only
15.22	Modular Furniture (with Chairs) Sub-Total (Chapter-3>3.1>3.1.2>Refer Civil Works and interiors of C4i)	1	Lump-sum										0.00	0.00	INR Zero Only
15.23	HVAC Sub-Total (Chapter-3>3.1>3.1.2>Refer Civil Works and interiors of C4i)	1	Lump-sum										0.00	0.00	INR Zero Only
16	C3I Non-IT														



RFP- for selection of MSI for implementation and O&M of surveillance System
under Safe City Project of Delhi Police



16.01	Interior Works & Furnishings (Chapter-3>3.1>3.1.3>Refer Civil Works and interiors of C3i)	16	Lump-sum										0.00	0.00	INR Zero Only
16.02	Electrical Works (Chapter-3>3.1>3.1.3>Refer Civil Works and interiors of C3i)	16	Lump-sum										0.00	0.00	INR Zero Only
16.03	INSTALLATION OF PANELS; SUPPLY AND INSTALLATION OF DB, CABLES AND EARTHING (Chapter-3>3.1>3.1.3>Refer Civil Works and interiors of C3i)	16	Lump-sum										0.00	0.00	INR Zero Only
16.04	FIXING OF LIGHTING FIXTURES (Chapter-3>3.1>3.1.3>Refer Civil Works and interiors of C3i)	16	Lump-sum										0.00	0.00	INR Zero Only
16.05	SUPPLY OF LIGHTING FIXTURES (Chapter-3>3.1>3.1.3>Refer Civil Works and interiors of C3i)	16	Lump-sum										0.00	0.00	INR Zero Only
16.06	CONSTRUCTION POWER AND LIGHTING (Chapter-3>3.1>3.1.3>Refer Civil Works and interiors of C3i)	16	Lump-sum										0.00	0.00	INR Zero Only
16.07	MODULAR FURNITURE FOR WORKSTATIONS (Chapter-3>3.1>3.1.3>Refer Civil Works and interiors of C3i)	57	Lump-sum										0.00	0.00	INR Zero Only
17	C2i Non-IT														
17.01	INTERIOR WORKS & FURNISHINGS (Chapter-3>3.1>3.1.4>Refer Civil Works and interiors of C2i)	182	Lump-sum										0.00	0.00	INR Zero Only
17.02	Electrical Works (Chapter-3>3.1>3.1.4>Refer Civil Works and interiors of C2i)	182	Lump-sum										0.00	0.00	INR Zero Only
17.03	INSTALLATION OF PANELS; SUPPLY AND INSTALLATION OF DB, CABLES AND EARTHING (Chapter-3>3.1>3.1.4>Refer Civil Works and interiors of C2i)	182	Lump-sum										0.00	0.00	INR Zero Only
17.04	SUPPLY & FIXING OF LIGHTING FIXTURES (Chapter-3>3.1>3.1.4>Refer Civil Works and interiors of C2i)	182	Lump-sum										0.00	0.00	INR Zero Only
17.05	MODULAR FURNITURE FOR WORKSTATIONS (Chapter-3>3.1>3.1.4>Refer Civil Works and interiors of C2i)	240	Lump-sum										0.00	0.00	INR Zero Only
18	DC Non-IT														
18.01	Civil Works (Chapter-3>3.1>3.1.5>Refer Civil Works and interiors of Data Centre)	1	Lump-sum										0.00	0.00	INR Zero Only
18.02	JOINERY (Chapter-3>3.1>3.1.5>Refer Civil Works and interiors of Data Centre)	1	Lump-sum										0.00	0.00	INR Zero Only



RFP- for selection of MSI for implementation and O&M of surveillance System
under Safe City Project of Delhi Police



18.03	DOORS (Chapter-3>3.1>3.1.5>Refer Civil Works and interiors of Data Centre)	1	Lump-sum										0.00	0.00	INR Zero Only
18.04	CEILING (Chapter-3>3.1>3.1.5>Refer Civil Works and interiors of Data Centre)	1	Lump-sum										0.00	0.00	INR Zero Only
18.05	FINISHES (Chapter-3>3.1>3.1.5>Refer Civil Works and interiors of Data Centre)	1	Lump-sum										0.00	0.00	INR Zero Only
18.06	STORAGE (Chapter-3>3.1>3.1.5>Refer Civil Works and interiors of Data Centre)	1	Lump-sum										0.00	0.00	INR Zero Only
18.07	FLOORING (Chapter-3>3.1>3.1.5>Refer Civil Works and interiors of Data Centre)	1	Lump-sum										0.00	0.00	INR Zero Only
18.08	SIGNAGES (Chapter-3>3.1>3.1.5>Refer Civil Works and interiors of Data Centre)	1	Lump-sum										0.00	0.00	INR Zero Only
18.09	LOOSE FURNITURE (Chapter-3>3.1>3.1.5>Refer Civil Works and interiors of Data Centre)	1	Lump-sum										0.00	0.00	INR Zero Only
18.1	MISCELLANEOUS INTERIOR ITEMS (Chapter-3>3.1>3.1.5>Refer Civil Works and interiors of Data Centre)	1	Lump-sum										0.00	0.00	INR Zero Only
18.11	HVAC: AIR HANDLING UNIT, CHILLED WATER PIPING, AIR DISTRIBUTION, INSULATION (Chapter-3>3.1>3.1.5>Refer Civil Works and interiors of Data Centre)	1	Lump-sum										0.00	0.00	INR Zero Only
18.12	PAC (Chapter-3>3.1>3.1.5>Refer Civil Works and interiors of Data Centre)	1	Lump-sum										0.00	0.00	INR Zero Only
18.13	Electrical Works (Chapter-3>3.1>3.1.5>Refer Civil Works and interiors of Data Centre)	1	Lump-sum										0.00	0.00	INR Zero Only
18.14	CONDUITS AND MS PAINTED CHANNELS FOR STRUCTURED CABLING (Chapter-3>3.1>3.1.5>Refer Civil Works and interiors of Data Centre)	1	Lump-sum										0.00	0.00	INR Zero Only
18.15	FIXING OF LIGHTING FIXTURES. (Chapter-3>3.1>3.1.5>Refer Civil Works and interiors of Data Centre)	1	Lump-sum										0.00	0.00	INR Zero Only
18.16	SUPPLY OF LIGHTING FIXTURES (Chapter-3>3.1>3.1.5>Refer Civil Works and interiors of Data Centre)	1	Lump-sum										0.00	0.00	INR Zero Only
18.17	CONSTRUCTION POWER AND LIGHTING (Chapter-3>3.1>3.1.5>Refer Civil Works and interiors of Data Centre)	1	Lump-sum										0.00	0.00	INR Zero Only
18.18	Networking (Chapter-3>3.1>3.1.5>Refer Civil Works and interiors of Data Centre)	1	Lump-sum										0.00	0.00	INR Zero Only



RFP- for selection of MSI for implementation and O&M of surveillance System
under Safe City Project of Delhi Police



18.19	ACS, FDS, WLDS, VESDA, RRS, BMS, PAS, NOVEC (Chapter-3>3.1>3.1.5>Refer Civil Works and interiors of Data Centre)	1	Lump-sum										0.00	0.00	INR Zero Only
18.2	Floor strengthening (Chapter-3>3.1>3.1.5>Refer Civil Works and interiors of Data Centre)	1	Lump-sum										0.00	0.00	INR Zero Only
19	Any Additional item, equipment or services not covered above and required to complete the project														
19.01	Details of the item, equipment or services	1	per Year										0.00	0.00	INR Zero Only
20	AMC charges for two years starting from approx. March 2023, for following items of 88 nos of Prakhar Vans already supplied to Delhi Police.														
20.01	MDT (Mobile Data Terminal) - 88 Nos.	2	per Year										0.00	0.00	INR Zero Only
20.02	Finger Print Scanner Compatible with MDT - 88 Nos.	2	per Year										0.00	0.00	INR Zero Only
20.03	Communication Device - 88 Nos.	2	per Year										0.00	0.00	INR Zero Only
20.04	Body Worn Camera - 88 Nos.	2	per Year										0.00	0.00	INR Zero Only
20.05	Battery - 88 Nos.	2	per Year										0.00	0.00	INR Zero Only
20.06	Vehicle Mounted Camera - 352 Nos.	2	per Year										0.00	0.00	INR Zero Only
20.07	Mobile Network Video Recorder (MnVR) - 88 Nos.	2	per Year										0.00	0.00	INR Zero Only
20.08	GPS, Software	2	per Year										0.00	0.00	INR Zero Only
Total in Figures														0.00	INR Zero Only
Quoted Rate in Words		INR Zero Only													



(End of Chapter – 5)

Chapter 6. Contract Form (Draft)

This is a draft agreement and contract terms and conditions will be finalized after mutual discussion with selected MSI and Stakeholder. However, by and large, the terms and conditions of the Contract shall be in-line with those stipulated in this RFP document.

This Agreement is made and executed at ____ on this ____

BY AND BETWEEN

Centre for Development of Advanced Computing, an autonomous Society of the Ministry of Electronics and Information Technology (MeitY), Government of India, registered under the Societies Registration Act, 1860 and the Bombay Public Trusts Act, 1950 having its registered office at _____ (hereinafter referred to as “C-DAC”) which expression shall, unless it be repugnant to the context or meaning thereof, be deemed to mean and include its successors and assigns,

AND

_____, an Indian Company, incorporated under the Companies Act, 2013 and having its office at _____, through its authorized signatory, _____, (hereinafter referred to as “_____”) which expression shall, unless it be repugnant to the context or meaning thereof, be deemed to mean and include its subsidiaries and Affiliates and their respective representatives, successors and assigns,

C-DAC and ____ hereinafter individually referred to as a “Party” or together the “Parties”

Whereas C-DAC had published a Request for Proposal No. CDACP/Safe City/2020/313 dated xx December, 2020 for appointment of Main System Integrator (hereafter referred as MSI) for supply, installation and commissioning of CCTV City Surveillance System as a part of Safe City project of Delhi Police.

Whereas, M/s (MSI) being interested in execution of said work, participated in the tendering process and submitted their techno-commercial offer.

And Whereas, M/s (Name of MSI) having visited and carefully and completely inspected and fully familiarized the scope and responsibilities, represented to C-DAC that they have the required professional skills, personnel and technical and financial capability and resources, have agreed to execute the work as per the scope of work stipulated in this Contract (along with Annexures), the same be treated and read as part and parcel of this Contract.

And Whereas, M/s (MSI) hereby agrees to execute the said work and subject to the conditions set forth herein, for Rs. (amount), excluding the applicable GST, (all of which are collectively hereinafter referred to as the “said Conditions” and forming a part and parcel of this Contract).



And whereas, based on representation made by M/s (MSI), C-DAC agreed to avail the services of M/s (MSI) for completion of aforesaid work, and hence the parties agreed to enter into the present contract.

Now hereby it is agreed by and between the parties hereto as under:

1. Definitions: (As per para 1.6 of chapter 1.)
2. Scope of Contract:

M/s (MSI) shall upon and subject to the conditions of the Contract, execute and complete the work shown upon and described in the schedule of requirements (As given in **Annexure xx** attached) and as per said specifications, at agreed rates.

C-DAC shall pay M/s (MSI) as per this contract for the work completely done to the satisfaction of C-DAC that may become payable at times and in manner hereinafter specified in the said conditions
3. Order of precedence of documents:
 - a. Contract Agreement
 - b. Letter of Intent
 - c. C-DAC's RFP No _____ dated ____ read with the corrigenda published
 - d. The techno-commercial bid submitted by M/s (MSI) subject to acceptance by C-DAC
4. Locations for Delivery and Project Implementation mentioned in para 2.1.13 of chapter 2
5. Performance Security mentioned in para 2.1.15 of chapter 2
6. Timelines linked with Payment Schedule mentioned in para 2.1.16 of chapter 2
7. Warranty mentioned in para 2.1.17 of chapter 2
8. Operations and Maintenance mentioned in para 2.1.18 of chapter 2
9. Liquidated Damages mentioned in para 2.1.19 of chapter 2
10. Penalties for Non/Under Performance mentioned in para 2.1.20 of chapter 2
11. Termination mentioned in para 2.1.21 of chapter 2
12. Consequence of Termination mentioned in para 2.1.22 of chapter 2
13. Limitation of Liability mentioned in para 2.1.23 of chapter 2
14. Indemnity mentioned in para 2.1.24 of chapter 2
15. Security and Safety mentioned in para 2.1.25 of chapter 2
16. Confidentiality mentioned in para 2.1.26 of chapter 2
17. Events of Default by MSI mentioned in para 2.1.27 of chapter 2
18. Severability and renegotiation mentioned in para 2.1.28 of chapter 2
19. Non-Waiver mentioned in para 2.1.29 of chapter 2
20. Fall Clause mentioned in para 2.1.30 of chapter 2



21. Jurisdiction mentioned in para 2.1.31 of chapter 2

22. Other paras stipulated in RFP

NOW, THEREFORE, for valuable consideration, the adequacy of which is hereby acknowledged, the Parties covenant and agree as follows:

6.1. Scope of work

- a. Scope of the work is defined in RFP Chapter 4 of the Bid.
- b. MSI is required to provide such goods, services and support as C-DAC may deem fit proper and necessary, during the term of this Contract and includes all such processes and activities which are consistent with the proposals set forth in the Bid, the RFP and this Contract and are deemed necessary by C-DAC, in order to meet its business requirements (hereinafter 'Scope of Work').

6.2. Key Performance Measurements

- a. Unless specified by C-DAC to the contrary, MSI shall deliver the goods, perform the services and carry out the Scope of Work in accordance with the terms of this Contract, Scope of Work and the Service Specifications as laid down under Service Level Agreement in (4.13 of Chapter 4) of this Contract.
- b. C-DAC in consultation with Delhi Police may amend any of the terms and conditions in relation to the Contract / Service Specifications and may issue any such directions which are not necessarily stipulated therein if it deems necessary for the fulfilment of the Schedule of Requirements.

6.3. Commencement and Progress

- a. MSI shall subject to the fulfillment of the conditions precedent above, commence the performance of its obligations within 7 days from the date of execution of this Contract, in a manner as per the Scope of Work (Chapter 4).
- b. MSI shall proceed to carry out the activities / services with diligence and expedite in accordance with any stipulation as to the time, manner, mode, and method of execution contained in this Contract.
- c. MSI shall be responsible for and shall ensure that all activities/services are performed in accordance with the Contract, Scope of Work and Service Specifications and that MSI's Team complies with such Specifications and all other standards, terms and other stipulations/conditions set out hereunder.

6.4. Standards of performance

MSI shall perform the Services and carry out its obligations under the Contract with due diligence, efficiency and economy, in accordance with generally accepted techniques and best practices used in the industry and with IT standards recognized by international professional bodies and shall observe sound management, engineering and security practices. It shall employ appropriate advanced technology and engineering practices and safe and effective equipment, machinery, material and methods. MSI shall always act,



in respect of any matter relating to the Contract, as faithful advisors to C-DAC and shall, at all times, support and safeguard C-DAC's legitimate interests in any dealings with Third Parties.

6.5. Approvals and Required Consents

- a. C-DAC shall extend necessary support to MSI to obtain, maintain and observe all relevant and customary regulatory and governmental licenses, clearances and applicable approvals (hereinafter the "Approvals") necessary for MSI to provide the Services. The costs of such Approvals shall be borne by MSI. Both Parties shall give each other all co-operation and information reasonably required.
- b. C-DAC shall also provide necessary support to the MSI in obtaining the Approvals. In the event that any Approval is not obtained, MSI and C-DAC shall co-operate with each other in achieving a reasonable alternative arrangement as soon as reasonably practicable for MSI, to continue to process its work with as minimal interruption to its business operations as is commercially reasonable until such Approval is obtained, provided that MSI shall not be relieved of its obligations to provide the Services and to achieve the Service Levels until the Approvals are obtained if and to the extent that MSI's obligations are dependent upon such Approvals.

6.6. MSI's Obligations

- a. MSI's obligations shall include all the activities as specified by C-DAC in the Scope of Work and other sections and Annexures of the RFP and Contract and changes thereof to enable C-DAC to meet the objectives and operational requirements. It shall be MSI's responsibility to ensure the proper and successful implementation, performance and continued operation of the proposed solution in accordance with and in strict adherence to the terms of his Bid, the RFP and this Contract.
- b. In addition to the aforementioned, MSI shall provide services to manage and maintain the said system and infrastructure.
- c. MSI will prepare reports in accordance with SLAs signed with the respective ISPs of ISP network uptime and outage. These reports shall help the TSP to release the payments to the ISP based on the service availability
- d. Responsibility of MSI's operations team to raise the tickets towards any network issues with the respective ISP.
- e. MSI shall deploy all such Key Personnel whose resume was submitted to C-DAC as a part of its Bid and evaluated at the RFP stage. C-DAC reserves the right to interview the personnel proposed that shall be deployed as part of the Project team. If found unsuitable, C-DAC may reject the deployment of the personnel. But ultimate responsibility of the efficient Project implementation shall lie with MSI.
- f. C-DAC reserves the right to require changes in personnel which shall be communicated to MSI. MSI with the prior approval of C-DAC may make additions to the Project team immediately. MSI shall provide C-DAC with the resume of personnel and provide such other information as C-DAC may reasonably require. In case of change in its team members/ personnel including Key Personnel, for any reason whatsoever, MSI shall also ensure that the exiting members are replaced with at least equally qualified and professionally competent members/ personnel in comparison to the personnel whose



replacement is being sought. C-DAC may interview the resources suggested by MSI before their deployment on board the Project.

- g. MSI shall ensure that none of the Key Personnel and manpower exit from the Project during first 6 months of the beginning of the Project. In such cases of exit a penalty for such replacements shall be imposed on the MSI as per below table.

Manpower	Penalty (in INR)
Project Manager	2,00,000/-
DC/ DR- Cloud Expert	1,50,000/-
Command Center Design Expert	1,00,000/-
GIS Expert	80,000/-
Solution Architect	80,000/-
ITMS Expert	80,000/-
Software Management Expert	80,000/-
IT/ ICT Infrastructure Expert	80,000/-
Database Architect	80,000/-
IT/ Cyber Security Expert	80,000/-

- h. In case of change in its personnel/ team members, MSI shall ensure a reasonable amount of time overlap in activities to ensure proper knowledge transfer and handover / takeover of documents and other relevant materials between the outgoing and the new member.
- i. MSI shall ensure that MSI's Team is competent, professional and possesses the requisite qualifications and experience appropriate to the task they are required to perform under this Contract. MSI shall ensure that the Services are performed through the efforts of MSI's Team, in accordance with the terms hereof and to the satisfaction of C-DAC. Nothing in this Contract relieves MSI from its liabilities or obligations under this Contract to provide the Services in accordance with C-DAC's directions and requirements and as stated in this Contract and the Bid to the extent accepted by C-DAC and MSI shall be liable for any non-performance, non-compliance, breach or other loss and damage resulting either directly or indirectly by or on account of its Team.
- j. Typical Scaled site Plan and Equipment layout Plan for the System to be deployed at each location shall be prepared by the MSI. The layout shall show interconnecting cable routings between various equipment of the System.
- k. The MSI shall ensure that MCCV, C2i, C3i, C4i designs has to be approved by C-DAC before actual implementation.
- l. The MSI shall ensure that all necessary approvals/permissions required for installation of equipment at the locations (except C2i, C3i, C4i, Data Centre & near DR) identified under the project and laying of cables, etc., are obtained from the concerned civic agencies within the timelines fixed. The C-DAC shall, to the extent of writing letters to the concerned agencies, provide all necessary assistance in obtaining the required approvals/permissions from civic agencies, for installation of equipment/items at the locations identified. However, MSI will be responsible to apply for approvals from civic agencies, pursue and completing all formalities with the civic agencies.
- m. MSI shall ensure that earthing arrangements for all the equipment shall be completed as per standard practice



- n. Before the equipment(s)/system(s) are taken over by the C-DAC, MSI shall supply installation, operation, repair and maintenance manuals of the equipment/system. This shall include the following: -
- System interface Drawings,
 - System interconnection and Block Diagrams,
 - User Operation Manuals
 - Equipment Maintenance manuals.
 - As Build-up Drawings
- o. MSI shall be fully responsible for deployment / installation / development/ procurement of network fiber and integration of all the software and hardware components and resolve any problems / issues that may arise due to integration of components.
- p. MSI shall ensure that the OEMs supply equipment/ components including associated accessories and software required and shall support MSI in the installation, commissioning, integration and maintenance of these components during the entire period of contract. MSI shall ensure that the COTS OEMs supply the software applications and shall support MSI in the installation / deployment, integration, roll-out and maintenance of these applications during the entire period of contract. It must clearly be understood by MSI that warranty and O&M of the system, products and services incorporated as part of system would commence from the day of Go-Live of system as a complete Safe city solutions including all the solutions proposed. MSI would be required to explicitly display that it shall have a back to back arrangement for provisioning of warranty/ O&M support till the end of contract period with the relevant OEMs. The Annual Maintenance support shall include patches and updates the software, hardware components and other devices.
- q. Deployment and patch management software has to be included which should support both windows* and Linux* environments.
- r. MSI should setup an Acceptance lab, which will be used to induct any IT hardware, software, Network and associated components. The following activities will be carried out in the Acceptance lab:
- Physical inspection
 - Confirming the COO, COA, COM
 - Sanitization of software including firmware of appliances for various vulnerabilities
 - Patching of the systems and software
 - Behavioral analysis of various systems and software on the network
 - Compatibility with respect to the existing infrastructure deployed under Safe City Project
- s. Bidder need to specify the software, hardware and network components factored under the Acceptance lab
- t. NMS software & license supply shall include all the features mentioned under NMS shall also include Policy deployment, Firmware deployment on all or selected network switches
- u. All the software licenses that MSI proposes should be perpetual software licenses. The software licenses shall not be restricted based on location and C-DAC should have the flexibility to use the software licenses for other requirements if required.



- v. All the OEMs that have been proposed by MSI should have Dealer/Manufacturer possession licenses and the OEM shall confirm and provide the Authorization certificates in the name of the Dealer.
- w. C-DAC reserves the right to review the terms of the Warranty and Annual Maintenance agreements entered into between MSI and OEMs and no such agreement/contract shall be executed, amended, modified and/or terminated without the prior written consent of C-DAC. An executed copy of each of such agreements/contracts shall, immediately upon execution be submitted by MSI to C-DAC.
- x. MSI shall ensure that none of the components and sub-components are declared end-of-sale or end-of-support by the respective OEM till 18 months from the date of commissioning. If the OEM declares any of the products/ solutions end-of-sale subsequently, the MSI shall ensure that the same is supported by the respective OEM for contract period.
- y. The quoted make & model of component should be available on the global website.
- z. If a product is de-supported by the OEM for any reason whatsoever, from the date of Acceptance of the System till the end of contract, MSI should replace the products/ solutions with an alternate that is acceptable to C-DAC at no additional cost to C-DAC and without causing any performance degradation.
- aa. Obtaining necessary Licenses shall be the responsibility of the MSI. However, all the Licenses shall be in the name of Delhi Police.
- bb. MSI shall ensure that the OEMs provide the support and assistance to MSI in case of any problems / issues arising due to integration of components supplied by him with any other component(s)/ product(s) under the purview of the overall solution. If the same is not resolved for any reason whatsoever, MSI shall replace the required component(s) with an equivalent or better substitute that is acceptable to C-DAC without any additional cost to C-DAC and without impacting the performance of the solution in any manner whatsoever.
- cc. MSI shall ensure that the OEMs for firmware and software install all type of updates, patches, fixes and/or bug fixes for the firmware or software from time to time at no additional cost to C-DAC.
- dd. MSI shall ensure that the OEMs for hardware servers/ equipment or MSI's trained engineers conduct the preventive maintenance on a Quarterly basis and break-fix maintenance in accordance with the best practices followed in the industry. MSI shall ensure that the documentation and training services associated with the components shall be provided by the OEM partner or OEM's certified training partner without any additional cost to C-DAC.
- ee. The training shall be conducted using official OEM course curriculum mapped with the hardware/ software Product's to be implemented in the project.
- ff. MSI and their personnel/representative shall not alter/ change/ replace any hardware component and/or under warranty or O&M of third party without prior consent of C-DAC.
- gg. MSI shall provision the required critical spares/ components at the designated Datacenter Sites/ office locations of C-DAC for meeting the uptime commitment of the components supplied by him.
- hh. MSI's representative(s) shall have all the powers requisite for the execution of Scope of Work and performance of Services under this contract. MSI's representative(s) shall liaise with C-DAC's representative for the proper coordination and timely completion of the works and on any other matters pertaining to the works. MSI shall extend full co-



- operation to C-DAC's representative in the manner required by them for supervision/ inspection/ observation of the equipment/ goods/ material, procedures, performance, progress, reports and records pertaining to the works. He shall also have complete charge of MSI's personnel engaged in the performance of the works and to ensure compliance of rules, regulations and safety practice. He shall also cooperate with the other service providers/vendors of C-DAC working at C-DAC's office locations & field locations and DC & DR sites. Such MSI's representative(s) shall be available to C-DAC's Representative at respective Datacenter during the execution of works.
- ii. MSI shall be responsible on an ongoing basis for coordination with other vendors and agencies of Delhi Police in order to resolve issues and oversee implementation of the same. MSI shall also be responsible for resolving conflicts between vendors in case of borderline integration issues.
- jj. MSI is expected to set up a project office in Delhi. The technical manpower deployed on the Project should work from the same office. However, some resources may be required to work from the client office/sites of Delhi Police during the contract period.
- kk. Bandwidth and connectivity taken exclusively for the facility by MSI shall be the sole property of Delhi Police and as per TRAI guidelines, any move by MSI for resale of bandwidth connectivity is not allowed.
- ll. MSI shall develop the plan and design documents and the same shall be submitted by MSI for approval by C-DAC. MSI shall commence the installation after obtaining the approval from C-DAC.
- Sites would include Server Room, Command and Control Center at various sites in Delhi. The list of locations and the facility to be developed will be shared after signing the NDA document.
 - C-DAC's representative upon receipt of request from MSI intimating commencement of activities at various locations shall give to MSI access to as much of the Sites as may be necessary to enable MSI to commence and proceed with the installation of the works in accordance with the program of work. Any reasonable proposal of MSI for access to Site to proceed with the installation of work in accordance with the program of work shall be considered for approval and shall not be unreasonably withheld by C-DAC. Such requests shall be made to C-DAC's representative in writing at least 7 days prior to start of the work.
 - At the site locations, C-DAC's representative shall give to MSI access to as much as may be necessary to enable MSI to commence and proceed with the installation of the works in accordance with the program of work.
- mm. MSI hereby declares that the systems sold to the C-DAC/ Delhi Police under this contract shall be of the best quality and workmanship and shall be strictly in accordance with the specifications and particulars contained/ mentioned in the contract and agreed upon.

nn. Start of Installation

MSI shall co-ordinate with C-DAC and stakeholders for the complete setup of sites before commencement of installation of other areas. MSI shall also co-ordinate regarding Network / Bandwidth connectivity in order to prepare the installation plan and detailed design / architectural design documents.

oo. Reporting Progress



- MSI shall be responsible for the execution of the Contract, shall monitor the progress of all the activities and shall submit to the C-DAC, progress reports during the implementation phase.
- Formats and frequency for all above mentioned reports and their dissemination mechanism shall be discussed and finalized along with project plan. C-DAC may change the formats, periodicity and dissemination mechanism for such reports.
- During the implementation phase, meetings shall be held between the representatives of C-DAC and MSI once in every 15 days to discuss the progress of implementation. After the implementation phase is over, the meeting shall be held as desired by C-DAC, to discuss the performance of the Contract.
- MSI shall ensure that the respective solution teams involved in the execution of work are part of such meetings.
- Several review committees involving representative of C-DAC and representative officials of MSI shall be formed for the purpose of this project. These committees shall meet at intervals, as decided by C-DAC later, to oversee the progress of the implementation.
- All the goods, services and manpower to be provided/deployed by MSI under the Contract and the manner and speed of execution and maintenance of the work and services are to be conducted in a manner to the satisfaction of C-DAC's representative in accordance with the Contract.
- C-DAC reserves the right to inspect and monitor/ assess the progress/ performance of the work / services at any time during the course of the Contract. C-DAC may demand and upon such demand being made, MSI shall provide documents, data, material or any other information which C-DAC may require, to enable it to assess the progress/ performance of the work / service.
- At any time during the course of the Contract, C-DAC shall also have the right to conduct, either itself or through another agency as it may deem fit without any notice to MSI, an audit to monitor the performance by MSI of its obligations/ functions in accordance with the standards committed to or required by C-DAC and MSI undertakes to cooperate with and provide to C-DAC/ any other agency appointed by C-DAC, all Documents and other details as may be required by them for this purpose.
- Should the rate of progress of the works or any part of them at any time fall behind the stipulated time for completion or is found to be too slow to ensure completion of the works by the stipulated time, or is in deviation to Bid requirements/ standards, C-DAC's representative shall so notify MSI in writing.
- MSI shall reply to the written notice giving details of the measures he proposes to take to expedite the progress so as to complete the works by the prescribed time or to ensure compliance to RFP requirements. MSI shall not be entitled to any additional payment for taking such steps. If at any time it should appear to C-DAC or C-DAC's representative that the actual progress of work does not conform to the approved plan, MSI shall, at the request of C-DAC's representative, prepare a revised plan showing the modification to the approved plan necessary to ensure completion of the works within the time for completion or steps initiated to ensure compliance to the stipulated requirements
- The submission seeking approval by C-DAC or C-DAC's representative of such plan shall not relieve MSI of any of his duties or responsibilities under the Contract.
- In case during execution of works, the progress falls behind schedule or does not meet the RFP requirements, MSI shall deploy extra manpower/ resources to make up the



progress or to meet the RFP requirements. Plan for deployment of extra man power/ resources shall be submitted to C-DAC for its review and approval. All time and cost effect in this respect shall be borne, by MSI within the Contract Value.

- MSI representative shall prepare and distribute Service Level Performance reports in a mutually agreed format by the 5th working day of subsequent month. The reports shall include “actual versus target” Service Level Performance, a variance analysis and discussion of appropriate issues or significant events. Performance reports shall be distributed to C-DAC management personnel as directed by C-DAC.
- Also, MSI may be required to get the Service Level Performance reports audited by independent Auditor with necessary approval of C-DAC. All related costs will be borne by the MSI.

pp. Knowledge of Server Room, Command and Control Center

- MSI shall be granted access to the Server Room, Command and Control Center, for inspection by C-DAC and its representatives before commencement of installation. The plan shall be drawn mutually at a later stage.
- MSI shall be deemed to have knowledge of the Server Room, Command and Control Center,, and its surroundings and information available in connection therewith and to have satisfied itself the form and nature thereof including, the data and information contained in the Bidding Documents and the RFP, the physical and climatic conditions, the quantities and nature of the works and materials necessary for the completion of the works, the means of access, etc. and in general to have obtained itself all necessary information of all risks, contingencies and circumstances affecting his obligations and responsibilities therewith under the Contract and his ability to perform it. However, if during pre-installation survey / during delivery or installation, MSI and/or C-DAC detects physical conditions and/or obstructions affecting the work, MSI shall take all measures to overcome them.

qq. Project Plan

- MSI should have submitted along with the Bid proposal the Project Plan meeting with the Project completion time as specified in the Bidding document. Modified Project Plan shall be submitted by the MSI, within 15 calendar days Issuance of LoI, for C-DAC’s approval. MSI shall submit the detailed Project Plan with details of the project showing the sequence, procedure and method in which he proposes to carry out the works for its approval. The Plan so submitted by MSI shall conform to the requirements and timelines specified in the Contract. C-DAC and MSI shall discuss and agree upon the work procedures to be followed for effective execution of the works, which MSI intends to deploy and shall be clearly specified. The Project Plan shall include but not limited to project organization, communication structure, proposed staffing, roles and responsibilities, processes and tool sets to be used for quality assurance, security and confidentiality practices in accordance with industry best practices, project plan and delivery schedule in accordance with the Contract. Approval by C-DAC’s Representative of the Project Plan shall not relieve MSI of any of his duties or responsibilities under the Contract.
- If MSI’s work plans necessitate a disruption/ shutdown in C-DAC’s operation, the plan shall be mutually discussed and developed so as to keep such disruption/shutdown



to the barest unavoidable minimum. Any time and cost arising due to failure of MSI to develop/adhere such a work plan shall be to his account.

rr. Adherence to safety procedures, rules regulations and restriction

- a. MSI's Team shall comply with the provision of all laws including labor laws, rules, regulations and notifications issued thereunder from time to time. All safety and labor laws enforced by statutory agencies and by C-DAC shall be applicable in the performance of this Contract and MSI's Team shall abide by these laws including PF, ESI and Medical Insurance etc.
- b. Access to the Server Room, Command and Control Center shall be strictly restricted. No access to any person except the essential members of MSI's Team who are authorized by C-DAC and are genuinely required for execution of work or for carrying out management/ maintenance shall be allowed entry. MSI and Team shall be having the access restricted to the equipment supplied under this Contract or any of the Equipment's as provided by C-DAC. MSI shall maintain a log of all activities carried out by each of its team personnel.
- c. No access should be given to any staff of MSI, except the essential staff who has genuine work-related need. All such access should be logged in a loss free manner for permanent record with unique biometric identification of the staff to avoid misrepresentations or mistakes.
- d. MSI shall take all measures necessary or proper to protect the personnel, work and facilities and shall observe all reasonable safety rules and instructions. MSI's Team shall adhere to all security requirement/ regulations of C-DAC during the execution of the work. C-DAC's employee also shall comply with safety procedures/ policy.
- e. MSI shall report as soon as possible any evidence, which may indicate or is likely to lead to an abnormal or dangerous situation and shall take all necessary emergency control steps to avoid such abnormal situations.

ss. Statutory Requirements

During the tenure of this Contract MSI or his team including JV members, its successors and assigns, shall follow all the security, safety and statutory requirements as per the applicable law, act and/ or rules/regulations, or any amendment thereof governing inter-alia customs, stowaways, foreign exchange etc. and shall keep C-DAC indemnified in this regard.

6.7. C-DAC's Obligations

- a. C-DAC or its nominated representative shall act as the nodal point for implementation of the contract and for issuing necessary instructions, approvals, commissioning, acceptance certificates, payments etc. to MSI.
- b. C-DAC shall ensure that timely approval is provided to MSI as and when required, which may include approval of project plans, implementation methodology, design documents, specifications, or any other documents necessary in fulfillment of this Contract provided that MSI is in compliance with the requirements under various policies and as per the terms of the Contract.
- c. C-DAC's representative shall interface with MSI, to provide the required information, clarifications, and to resolve any issues as may arise during the execution of the Contract. C-DAC shall provide adequate cooperation in providing details, coordinating and obtaining of approvals from various governmental agencies, in cases, where the intervention of C-DAC is proper and necessary.



- d. C-DAC may provide on MSI's request, particulars/ information or documentation that may be required by MSI for proper planning and execution of work and for providing services covered under this Contract and for which MSI may have to coordinate with respective vendors.
- e. C-DAC shall provide to MSI only sitting space and basic infrastructure not including, stationery and other consumables at Delhi Police's office locations.
- f. C-DAC reserves the right to procure the hardware including devices on quarterly basis in first year based on actual deployment and O&M shall be applicable whenever the devices are procured and deployed till end of the contract.
- g. **Site Not Ready:** C-DAC hereby agrees to make the project site ready as per the agreed dimensions and specifications, within the agreed timelines. C-DAC agrees that MSI shall not be in any manner liable for any delay arising out of C-DAC's failure to make the site ready within the stipulated period.

6.8. Payment Terms

- a. The MSI should raise the tax invoice for supply and installation of material actually supplied and installed while claiming payments at each stage, based on the unit prices quoted, along with the acceptance report issued by C-DAC/Delhi Police.
- b. C-DAC will take judicious decision on invoices submitted (along with inspection report) by MSI regarding acceptance or rejection of material delivered and/or services provided under this Project within 30 days and payment will be released to the MSI of the accepted amount after proportionate adjustment of the advance.
- c. C-DAC shall make payments to MSI at the times and in the manner set out in the Payment schedule as specified in the Payment Schedule mentioned in para 2.1.25 of Chapter 2 subject to the penalties as mentioned under para 2.1.29 of Chapter 2.
- d. All payments agreed to be made by C-DAC to MSI in accordance with the Price Bid shall be inclusive of all statutory levies, duties, taxes and other charges whenever levied/applicable, if any, and C-DAC shall not be liable to pay any such levies/ other charges under or in relation to this Contract and/or the Services.
- e. Payment during the period of Extended Warranty i.e. 4th year and 5th year from the date of Acceptance of the System/completion of Warranty Period, will be payable on quarterly basis, after completion of that period.
- f. The applicable TDS/TCS will be deducted from the payable amount.
- g. No invoice for extra work/change order on account of change order shall be submitted by MSI unless the said extra work /change order has been authorized/approved by C-DAC in writing in accordance with Change Control Note.
- h. In the event of C-DAC noticing at any time that any amount has been disbursed wrongly to MSI or any other amount is due from MSI to C-DAC, C-DAC may without any prior notice and without prejudice to its rights to recover such amounts by other means after notifying MSI or deduct such amount from any payment falling due to MSI. The details of such recovery, if any, shall be intimated to MSI. MSI shall receive the payment of undisputed amount under subsequent invoice for any amount that has been omitted in previous invoice by mistake on the part of C-DAC or MSI.
- i. All payments to MSI shall be subject to the deductions of tax at source under Income Tax Act, and other taxes and deductions as provided for under any law, rule or regulation of the land. All costs, damages or expenses which C-DAC may have paid or incurred, for which under the provisions of the Contract, MSI is liable, the same shall be deducted by



C-DAC from any dues to MSI. All payments to MSI shall be made after making necessary deductions as per terms of the Contract and recoveries towards facilities, if any, provided by C-DAC to MSI on chargeable basis.



6.9. Ownership and Retention of Documents

- a. C-DAC shall own the Documents, prepared by or for MSI arising out of or in connection with this Contract and its execution thereof.
- b. Forthwith upon expiry or earlier termination of this Contract and at any other time on demand by C-DAC, MSI shall deliver to C-DAC all documents provided by or originating from C-DAC and all documents produced by or for MSI in the course of performing the Services, unless otherwise directed in writing by C-DAC at no additional cost. MSI shall not, without the prior written consent of C-DAC store, copy, distribute or retain any such documents.

Ownership of Work Product. The parties hereby acknowledge that the Work Product, and all documentation, information, systems, and other results developed in connection with the Work Product, will, to the extent permitted by Law, be a "work made for hire" within the definition of Section 101 of the Copyright Act (17 U.S.C. 101) and will remain Delhi Police's exclusive property.

Assignment of Work Product. If and to the extent that any Work Product is not deemed to be a work made for hire within the definition of the Copyright Act, at the completion and acceptance of the Safe City Project, MSI shall promptly assign to C-DAC all its right, title, and interest in and to the Work Product, including any Intellectual Property rights.

Cooperation. During and after the Term, on C-DAC's reasonable request, MSI shall provide all assistance necessary and desirable for C-DAC to establish, preserve, and enforce its rights, title, and interest in and to the Work Product.

6.10. Information Security

- a. MSI shall not carry any written/printed document, layout diagrams, CD, hard disk, storage tapes, other storage devices or any other goods /material proprietary to C-DAC/Delhi Police into / out of any location of Service without written permission from C-DAC.
- b. MSI shall not destroy any unwanted documents; defective tapes/media present at any location on their own. All such documents, tapes/media shall be handed over to C-DAC.
- c. All documentation and media at any location shall be properly identified, labeled and numbered by MSI. MSI shall keep track of all such items and provide a summary report of these items to C-DAC whenever asked for.
- d. Access to C-DAC's data and systems, Internet facility by MSI at any location shall be in accordance with the written permission of C-DAC. C-DAC shall allow MSI to use facility in a limited manner subject to availability. It is the responsibility of MSI to prepare and equip himself in order to meet the requirements.
- e. MSI must acknowledge that C-DAC/Delhi Police's business data and other C-DAC/Delhi Police proprietary information or materials, whether developed by C-DAC/Delhi Police or being used by C-DAC/Delhi Police pursuant to a license agreement with a third party (the foregoing collectively referred to herein as "proprietary information") are confidential and proprietary to C-DAC/Delhi Police; and MSI along with its team agrees to use reasonable care to safeguard the proprietary information and to prevent the unauthorized use or disclosure thereof, which care shall not be less than that used by MSI



to protect its own proprietary information. MSI recognizes that the goodwill of C-DAC depends, among other things, upon MSI keeping such proprietary information confidential and that unauthorized disclosure of the same by MSI or its team could damage the goodwill of C-DAC, and that by reason of MSI's duties hereunder. MSI may come into possession of such proprietary information, even though MSI does not take any direct part in or furnish the services performed for the creation of said proprietary information and shall limit access thereto to employees with a need to such access to perform the services required by this Contract. MSI shall use such information only for the purpose of performing the said services.

- f. MSI shall, upon termination of this Contract for any reason, or upon demand by C-DAC, whichever is earliest, return any and all information provided to MSI by C-DAC, including any copies or reproductions, both hardcopy and electronic.
- g. By virtue of this Contract, MSI team may have access to personal information of C-DAC/Delhi Police and/or a third party. C-DAC/Delhi Police has the sole ownership of and the right to use, all such data in perpetuity including any data or other information pertaining to the citizens that may be in the possession of MSI team in the course of performing the Services under the Contract

6.11. Records of contract documents

- a. MSI shall at all-time make and keep sufficient copies of the process manuals, operating procedures, specifications, Contract documents and any other documentation required for him to fulfil his duties under the Contract.
- b. MSI shall keep on the Site at least three copies of each and every specification and Contract Document, in excess of his own requirement and those copies shall be available at all times for use by C-DAC's Representative and by any other person authorized by C-DAC's Representative.

(End of Chapter – 6)



Chapter 7. : Standard Formats

7.1. Annexure – 1: Covering Letter

Date: dd/mm/yyyy

To,

Executive Director

Centre for Development of Advanced Computing(C-DAC)

Innovation Park, Panchavati,

Pashan Road, Pune – 411008

Subject: Request for Proposal for selection of Master System Integrator for Implementation of Delhi Safe City Project

Ref: RFP No _____

Dear Sir,

We, <<name of the undersigned Bidder>, having read and examined in detail all the bidding documents in respect of “**Request for Proposal No. _____** **for Selection of Master System Integrator for Implementation of Delhi Safe City Project**” do hereby submit our techno-commercial bid comprising of e-packets 1 and 2.

We hereby declare that all the information and statements made in this bid are true and we accept that any misinterpretation contained in it, may lead to our disqualification.

We agree to abide by all the terms and conditions of the RFP document. We would hold the terms of our proposal valid for 120 days as stipulated in the RFP document.

We also undertake that we/any of the member of the JV are not blacklisted or debarred from bidding process, by any Department/Office of the GoI or of any State Government, PSU, Autonomous Organization of GoI, as on date of submission of the bids and that there have been no regulatory actions initiated / pending against us as on the date of release of RFP.

We also undertake that we/any of the member of the JV do not have any conflict of interest or hostile interest in principle against C-DAC and/or Delhi Police and we accept that any misinterpretation, misleading, false statements with respect to may lead to our disqualification and debarment. We also confirm that we shall not attract conflict of interest in principle in future too.

It is hereby confirmed that I/We are entitled to act on behalf of our company/corporation/firm/organization and empowered to sign this document as well as such other documents, which may be required in this connection.



It is hereby declared and confirmed that I/we are authorized to act on behalf of other members of the JV and empowered to sign this document as well as such other documents, which may be required in this connection.

We declare that all the services shall be performed strictly in accordance with the RFP documents.

We confirm that the information contained in this response or any part thereof, including its exhibits, and other documents and instruments delivered or to be delivered to C-DAC is true, accurate, verifiable and complete. This response includes all information necessary to ensure that the statements therein do not in whole or in part mislead C-DAC in its evaluation process.

We hereby declare that in case the contract is awarded to us, we shall submit the contract Performance Bank Guarantee in the form prescribed in this RFP.

We hereby declare that , while preparation and submission of this bid, we have not acted in concert or in collusion with any other Bidder or other person(s) and also not done any act, deed or thing, which is or could be regarded as anti-competitive. We further confirm that we have not offered nor will offer any illegal gratification in cash or kind to any person or organization in connection with the instant bid.

We understand that our Bid is binding on us and that you are not bound to accept a Bid you receive.

Thanking you,

Yours sincerely,
(Signature of the Sole Bidder/ JV Bidder Members)
Printed Name
Designation

Seal

Date:
Place:
Business Address:



7.2. Annexure – 2: Format for Power of Attorney to Authorized Signatory

[To be executed on non-judicial stamp paper of the appropriate value in accordance with relevant Stamp Act. The stamp paper to be in the name of the company who is issuing the power of attorney.]

We, M/s.____ (name of the bidding firm or company with address of the registered office) hereby constitute, appoint and authorize Mr. or Ms.____ (Name, Designation and residential address) ----- (please mention the name of his organization/company), in his official and personal capacity, who's whose signature is appended below, as our Attorney to do in our name and our behalf all or any of the acts, deeds or things necessary or incidental to your RFP No. _____ for the **Safe City Project of Delhi Police**, including signing and submission of the RFP response, participating in the meetings, responding to queries, submission of information or documents and generally to represent us in all the dealings with C-DAC or any other Government Agency or any person, in connection with the works until culmination of the process of bidding till the Project Agreement is entered into with successful bidder/proposed MSI and thereafter till the expiry of the Project Agreement.

We hereby agree to ratify all acts, deeds and things lawfully done by our said Attorney pursuant to this power of attorney for conducting and completion of the Project and that all acts, deeds and things done by our aforesaid Attorney shall and shall always be deemed to have been done by us and legally binding on us.

Specimen signature of the Person holding Power of Attorney:

For (Name of Bidder)

Authorised Signatory
Name, Designation, mobile #
(Add in the case of a JV:

The bid is being submitted for and on behalf of Joint Venture comprising of _____, _____ and _____.)

We declare that we are authorized to sign this Power of Attorney.

Dated this the ____ day of ____ 2020

(Signature and Name/s of authorized signatory/ Signatories of Sole Bidder/ JV Members- as applicable)

Seal of firm Company

Witness 1:

Witness 2:

Notes:



7.3. Annexure – 3: Undertaking towards EMD

Subject: Undertaking as per GFR – 2017, Rule 170(iii)

To:

Executive Director

Centre for Development of Advanced Computing(C-DAC)

Innovation Park, Panchavati,

Pashan Road, Pune – 411008

Dear Sir,

We, the undersigned, offer to implement the CCTV surveillance project, in response to your RFP No _____.

We are hereby submitting our proposal for same, which includes Technical bid and the Financial Bid through www.eprocure.gov.in. As a part of eligibility requirement stipulated in said tender document, we hereby submit a declaration in lieu of Earnest Money Deposit (EMD), as given below:

1. Our bid shall remain valid for 120 days from the date of submission and that we will not withdraw or modify our bid during the validity period,
2. In case, we are declared as successful bidder and an order is placed on us, we will submit the acceptance in writing within 7 days of placement of order on us.
3. In case, we are declared as successful bidder and an order is placed on us, we undertake, to submit a Performance Bank Guarantee, as per terms stipulated in the RFP.
4. In case of failure on our part to comply with any of the above said requirements, we are aware that we shall be declared as un-eligible for said tender and /or debarred from any future bidding process of Ministry of Electronics and Information Technology, MHA or any other Government entity for a period of minimum one year.
5. The undersigned is authorized to sign this undertaking.

Yours sincerely,

Authorized Signatory:

Name and Title of Signatory:

E-mail:

Mobile No:



7.4. Annexure – 4: Documents Check-List

Sr. No.	Checklist Item	Compliance (Yes/No)	Page No. and Section No. in the Bid
1.	Technical Bid Covering Letter		
2.	Technical Bid Check-List		
3.	Bid Security/Earnest Money Deposit (EMD) receipt		
4.	Bid Security/Earnest Money Deposit (EMD) receipt or Declaration		
5.	RFP Document Fee Receipt		
6.	GST registration certificate/s		
7.	Copy of PAN		
8.	Certificate of Incorporation / Registration under applicable Indian Laws. In case of JV, the certificates of all members are required.		
9.	Registration certificate or a declaration in compliance with the provisions stipulated in office memorandum F/No/6/18/2019-PPD dated 23 July 2020 issued by public procurement Division, Dept. of Expenditure, Ministry of Finance, GoI		
10.	A written undertaking from each of the JV members, in case of a JV, duly signed by the authorized signatory, holding a written power of attorney for this bid on a stamp paper, authorizing the JV to incur liabilities and receive instructions for and on behalf of any and all JV members, and the entire execution of the Contract, including but not limited to the payments		
11.	MoA among the JV Partners showing the area of business (If applicable) and their internal arrangement per se.		
12.	Copies of audited balance sheets for the financial years 2019-20, 2018-19 and 2017-18 pertaining to sole bidder/ members of JV (In case of JV)		
13.	Certificate from the Statutory Auditor/CA on net worth and Profitability for financial years 2019-20, 2018-19 and 2017-18 pertaining to sole bidder / each member of JV (In case of JV)		
14.	Certificate from the Statutory Auditor/CA certifying the annual turnover of sole bidder/lead partner (In case of JV) in the areas of Supply, Implementation and Integration of City Surveillance System and/or, Data Centre		



	infrastructure in years 2019-20, 2018-19 and 2017-18.		
15.	Certificate from the Statutory Auditor/CA on net worth and Profitability for financial years 2019-20, 2018-19 and 2017-18 pertaining to OEM of cameras, ICCC and VMS.		
16.	Certificate from the Statutory Auditor/CA certifying the annual turnover of OEM of cameras, ICCC and VMS for the FY 2019-20, 2018-19 and 2017-18.		
17.	Anti-Collusion Certificate		
18.	List and address of bidder's office in Delhi or, undertaking from authorized signatory of bidder to open office with GST registration in Delhi within 60 days from Contract signing.		
19.	The details of TAC centre/s in India with toll free number pertaining to OEMs of camera, ICCC and VMS		
20.	Copies of the valid ISO /CMMi certificates in the name of the sole bidder/JV members		
21.	Non-blacklisting certificate for Bidder (In case of JV, this needs to be provided by each of the JV member).		
22.	The non-blacklisting certificate pertaining to OEMs of Cameras, Servers, VMS, ICCC, storage and networking components		
23.	supply orders, contracts, and agreements on completion / installation certificates in the name of bidder/s issued by end user in support of eligibility criteria/ pre-qualification criteria		
24.	The copies of supply orders, contracts, and agreements on completion / installation certificates in the name/s of respective OEMs of components/subsystems, issued by end user in support of eligibility criteria/ pre-qualification criteria		
25.	Non-Malicious Code undertaking from OEMs of Camera and Video Analytic software		
26.	Certificate from Chartered Accountant or Cost Accountant to the effect that for the purpose of this RFP, the bidding firm complies with the Order No P-45021/2/2017-PP (BE-II). Dated 4th June, 2020 issued by Public Procurement Division, Department of Investment and Internal Trade, Ministry of Commerce, GoI.		
27.	Certificates of origin and certificate of country of manufacture pertaining to Cameras, Servers, VMS, ICCC, UPS, IP Phones, and Hand held		



	devices, Video walls, Laptops/workstations, Television, Printers, Joystick, Storage and networking components.		
28.	Certificate from OEM of cameras in their letterhead confirming that any component/ hardware / parts / assembly / software including firmware used in the offered solution (hardware / software) DO NOT COMPLY to - GB28181, GB/T 28181-2011; GB/T28181-2011; GBT 28181-2011; GBT28181-2011 standards.		
29.	Address and other details of RMA set up OEM of camera in India		
30.	Certificate from OEM of Cameras that OEM is not banned or suspended by ONVIF		
31.	Certification from OEM of ICCV towards compliance of eligibility /Pre-qualification		
32.	Certification from OEM of VMS towards compliance of eligibility /Pre-qualification criteria		
33.	Details of service centre/Lab in India pertaining to OEM's of Cameras, servers, Storage, Display Monitors, Video Wall.		
34.	Documents related to understanding of the scope of work and all aspects of this project.		
35.	Documents related to project implementation approach, Phase wise scope and overlapping of activities		
36.	Documents related to availability and utilization of funds, contingency plan		
37.	Documents related to vendor management and plans for procurement of material in time		
38.	Documents related to risk Mitigation Plan/ Strategy/ SLA		
39.	Technical specifications of major components of the solution		
40.	Detailed technical compliance sheet		
41.	Documents related to Scalability, Safety, Reliability and Security features of the offered solutions		
42.	Manpower deployment details as per RFP		
43.	Bill of quantities		
44.	Product Certifications pertaining to components, Sub-systems offered as a part of solution.		
45.	Manufacturers'/Producers' Authorization Form (MAF)		
46.	Total responsibility undertaking		
47.	Pre-Qualification Criteria Document Index List		



7.5. Annexure – 5: Undertaking for Non-Malicious Code

(To be issued by OEMs of Cameras, VMS, Server, Storage, Network Equipment and ICCV)

Date: dd/mm/yyyy

To,

Executive Director

Centre for Development of Advanced Computing(C-DAC)

Innovation Park, Panchavati,

Pashan Road, Pune – 411008.

Subject: Request for Proposal for selection of Master System Integrator for Implementation of Delhi Safe City Project

Dear Sir,

This refers to the bid submitted by M/s (Name of Bidder) in response to your RFP No. _____ **for Selection of Master System Integrator for Implementation of Delhi Safe City Project.**

We, (Name of OEM) as the OEM of (Name of the Product) offered for said requirement, hereby certify that (Name of the Product) to be supplied through M/s (Name of Bidder) for Safe City project of Delhi Police, shall not contain any embedded malicious code which may cause any breach of confidentiality, infringement of Intellectual Property rights, loss, damages of whatsoever nature and detrimental to the interest of C-DAC and/or Delhi Police.

We are aware that we shall be liable under information Technology Act, 2000 and Indian Penal Code 1860 in case any such malicious code is found in our offered products.

The undersigned is authorized to sign this undertaking.

Yours sincerely,

Authorized Signatory:

Name and Title of Signatory:

E-mail:

Mobile No:



7.6. Annexure – 6: Manpower Plan

7.6.1. Till Go-Live (Implementation)

Manpower distribution								
S. No.	Name	Role	Month wise time to be spent by each personnel (in days) Total					
			Month 1	Month 2	Month 3	...	...	Month 12
1		Project Manager						
2		DC/ DR- Cloud Expert						
3		Command Center Design Expert						
4		GIS Expert						
5		Solution Architect						
6		ITMS Expert						
7		Software Management Expert						
8		IT/ ICT Infrastructure Expert						
9		Database Architect						
10		IT/ Cyber Security Expert						

Note: Proposed Resources/Key personnel should be deployed onsite and penalty shall be applicable as per RFP.

7.6.2. After Go-Live (Operation & Maintenance)

S. No.	Manpower/ Role	Years			
		Year 1	Year 2	Year 3	



7.6.3. Details of Resources proposed

S. No.	Name of the Resource	Proposed Role	Highest degree	Basic Qualification (E.g. B.Sc. or B.E. or MCA or Diploma)	Certifications (ex. PMI or ITIL or TOGAF or CCNP etc.)	Total Experience (in years)
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						



7.6.4. Curriculum Vitae (CV) of Team Members

Name:					
1.	Proposed position or role	(only one candidate shall be nominated for each position)			
2.	Date of Birth		Nationality		
3.	Education	Qualification	Name of School or College or University	Degree Obtained	Year of Passing
4.	Years of Experience				
5.	Areas of Expertise and no. of years of experience in this area	(as required for the Profile)			
6.	Certifications and Training attended				
7.	Employment Record	Employer	Position	From	To
		[Starting with present position and last 2 firms, list in reverse order, giving for each employment: dates of employment, name of employing organization, positions held.]			
8.	Detailed Tasks Assigned	(List all tasks to be performed under this project)			



7.6.5. Relevant Work Undertaken that best illustrates the experience as required for the Role

Project 1	
Name of assignment	
Year	
Location	
Employer	
Main project features	
Position held	
Activities performed	
Project 2	
Name of assignment	
Year	
Location	
Employer	
Main project features	
Position held	
Activities performed	
Project 3	
Name of assignment	
Year	
Location	
Employer	
Main project features	
Position held	
Activities performed	
Project 4	
Name of assignment	
Year	
Location	
Employer	
Main project features	
Position held	
Activities performed	



7.7. Annexure – 7 : Manufacturers' Authorization Form

(This form has to be provided by the OEMs of the Cameras, Servers, Storage, Networking & Security components, Junction Box, VMS, ICCV, FRS, VA, ANPR, GIS, Video Summarization, EMS, NAC, Help Desk Management, DG set, UPS and HVAC system. This letter to C-DAC should be on the letterhead of the manufacturer and should be signed by a person competent and having the power of attorney to bind the manufacturer.)

Date:

To:

**Executive Director
Centre for Development of Advanced Computing(C-DAC)
Innovation Park, Panchavati,
Pashan Road, Pune – 411008.**

Subject: Manufacturer's Authorization Form

Ref: RFP No _____

Dear Sir,

We _____ (Name of the OEM) who are established and reputable manufacturers of _____ (List of Goods) having factories or product development centers at the locations _____ or as per list attached, do hereby authorize M/s _____ (Name and address of the Bidder) to bid, negotiate and conclude the contract with you against RFP No _____
_____ for the above goods manufactured or developed by us.

We hereby extend, our warranty for the hardware goods supplied by the Bidder and/ or maintenance or support services for software products against this invitation for bid by _____ (Name of the Bidder) as per requirements and for the duration of contract as specified in this RFP.

We also confirm that our offered product will not be end of life for minimum of 18 months from the date of commissioning and the support for such offered product/s will be available for minimum of 5 years from the date of bidding.

For OEM of Camera: The well documented SDK shall provide an extensive list of programming functions to view and/or configure core entities such as: users and user groups, alarms, custom events, and schedules, and more.

1. We have a structured support program in place to support 3rd party developers using SDK. The program details are shared along with the technical bid
2. We will provide well defined support by the means of online portal, Chat and Toll-free no to support the SDK developers on timely basis
 - i. SDK shall be made available within 2 weeks of release of the new version

Country of Origin of OEM: _____



Country of Manufacture of Item:

For OEM of ICCC:

1. We have India / Global development program for 3rd party developers using our SDK.
2. We will provide well documented SDK for further developments and integration with 3rd party systems along with online support portal outlining all the 3rd party integrations and 24/7 support on SDK package
3. We confirm that ICCC has native frameworks for public safety technologies like FRS, Analytics, VMS, PA, Traffic congestion, ANPR, Big Data Co Relation and Community surveillance

Country of Origin of OEM: _____

Country of Manufacture of Item:

The undersigned is authorized to sign this undertaking.

Thanking you,

Yours faithfully,

(Signature)

For and on behalf of: _____ (Name of the OEM)

Authorised Signatory

Name:

Designation:

Place:

Date:



7.8. Annexure – 8: Total Responsibility Certificate

To,

**Executive Director
Centre for Development of Advanced Computing(C-DAC)
Innovation Park, Panchavati,
Pashan Road, Pune – 411008**

Dear Sir,

This is to certify that we undertake the total responsibility for the defect free operation of the proposed solutions as per the requirement of the RFP for the duration mentioned in all the chapters of the RFP.

(Authorised Signatory)

7.9. Annexure - 9: Unconditional and Irrevocable Performance Bank Guarantee Format

Ref: _____

Date _____

Bank Guarantee No. _____

<Name>

<Designation>

<Address>

<Phone Nos.>

<Fax Nos.>

<Email id>

Whereas, <<name of the Successful Bidder and address>> (hereinafter called “the Successful Bidder” or “Master System Integrator”) has undertaken, in pursuance of LOI no. <Insert LOI No.> dated <Date> to provide Implementation services for <<name of the assignment>> to C-DAC (hereinafter called “C-DAC”)

And whereas it has been stipulated by in the said LOI that the Successful Bidder shall furnish you with a bank guarantee by a recognized bank for the sum specified therein as security for compliance with its obligations in accordance with the contract;



And whereas we, <Name of Bank> a banking company incorporated and having its head/registered office at <Address of Registered Office> and having one of its office at <Address of Local Office> have agreed to give the Successful Bidder such a bank guarantee.

Now, therefore, we hereby affirm that we are guarantors and responsible to you, on behalf of the Successful Bidder, up to a total of Rs.<Insert Value> (Rupees <Insert Value in Words> only) and we undertake to pay you, upon your first written demand declaring the Successful Bidder to be in default under the contract and without cavil or argument, any sum or sums within the limits of INR <Insert Value> (Rupees <Insert Value in Words> only) as aforesaid, without your needing to prove or to show grounds or reasons for your demand or the sum specified therein.

We hereby waive the necessity of your demanding the said debt from the Successful Bidder before presenting us with the demand.

We further agree that no change or addition to or other modification of the terms of the Contract to be performed there under or of any of the contract documents which may be made between you and the Successful Bidder/ Master System Integrator shall in any way release us from any liability under this guarantee and we hereby waive notice of any such change, addition or modification.

This Guarantee shall be valid until <<Insert Date>>)

Notwithstanding anything contained herein:

I. Our liability under this bank guarantee shall not exceed INR <Insert Value> (Rupees <Insert Value in Words> only).

II. This bank guarantee shall be valid up to <Insert Expiry Date>)

III. It is condition of our liability for payment of the guaranteed amount or any part thereof arising under this bank guarantee that we receive a valid written claim or demand for payment under this bank guarantee on or before <Insert Expiry Date>) failing which our liability under the guarantee will automatically cease.

Date _____
Place _____ Signature _____
Witness _____ Printed name _____

(Bank's common seal)

Seal: Date:



7.10. Annexure – 10: Non-Blacklisting Declaration by JV Members

(To be provided on the Company letter head)

{Place}

{Date}

To,

Executive Director

Centre for Development of Advanced Computing(C-DAC)

Innovation Park, Panchavati,

Pashan Road, Pune – 411008

**Subject: Self Declaration of not been blacklisted in response to the Request for Proposal
for selection of Master System Integrator for Implementation of _____ for**

Ref: RFP No. _____

Dear Sir,

We confirm that our {company or firm}, M/s _____, is currently and during the period of last 05 years, not blacklisted in any manner whatsoever by any of the State or UT and or Central Government in India on any ground including but not limited to indulgence in corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice.

(Signature of the JV Member)

Printed Name

Designation

Seal Date:

Place: Business Address:



7.11. Annexure – 11: Brief company profile (required for both bidder and JV member)

S No.	Particulars	Description
1.	Name of Bidder	
	Whether bidding as a Sole Bidder or as a JV	
	If Bidding as a JV, names of JV members	
a.		
b.		
c.		
2.	Legal status of Bidder (Company etc.)	
3.	Whether the Sole Bidder (or Lead bidder and/or any member/s of JV – in case of JV) are from any country which share land border with India. If yes, please give details.	
4.	Main business of the Bidder	
5.	Registered office address	
6.	Delhi office Address	
7.	Incorporation date and number	
8.	GST Number	
9.	PAN details	
10.	Primary Contact Person (Name, Designation, address, mobile number, fax, email)	
11.	Secondary Contact Person (Name, Designation, address, mobile number, fax, email)	
12.	EMD details	
13.	Role in JV (if applicable)	Brief scope of work in the JV



7.12. Annexure - 12: Change Control Note

Change Control Note	CCN Number:
Part A: Initiation	
Title:	
Originator:	
Sponsor:	
Date of Initiation:	
Details of Proposed Change	
(To include reason for change and appropriate details/specifications. Identify any attachments as A1, A2, and A3 etc.)	
Authorized by C-DAC	Date:
Name:	
Signature:	
Received by the MSI	Date:
Name:	
Signature:	

Change Control Note	CCN Number:
Part B: Evaluation	
(Identify any attachments as B1, B2, and B3 etc.)	
Changes to Services, payment terms, payment profile, documentation, training, service levels and component working arrangements and any other contractual issue.	
Brief Description of Solution:	
Impact:	
Deliverables:	
Timetable:	
Charges for Implementation: (including a schedule of payments)	
Other Relevant Information: (including value-added and acceptance criteria)	
Authorized by the MSI	Date:
Name:	
Signature:	

Change Control Note	CCN Number :
Part C: C-DAC to Proceed	
Implementation of this CCN as submitted in Part A, in accordance with Part B is: (tick as appropriate)	



Approved Rejected Requires Further Information (as follows, or as Attachment 1 etc.)	
For C-DAC and its nominated Agencies	For MSI
Signature	Signature
Name	Name
Title	Title
Date	Date



7.13. Annexure – 13: JV Agreement

DRAFT MEMORANDUM OF UNDERSTANDING EXECUTED BY MEMBERS OF THE JV

[On Non-judicial stamp paper of INR 100 duly attested by notary public]

This Memorandum of Understanding (MoU) entered into this day of [Date] [Month] [Year] at [Place] amongst

M/s _____, having our principal place of business or registered office at _____, acting through _____ (hereinafter referred to as the “Sole Bidder/ JV Bidder” which expression shall, unless repugnant to the context include its successors and permitted assigns)

1. M/s _____, having our principal place of business or registered office at _____, acting through _____ (hereinafter referred to as the “JV Member 1” which expression shall, unless repugnant to the context include its successors and permitted assigns)

AND

2. M/s _____, having our principal place of business or registered office at _____, acting through _____ (hereinafter referred to as the “JV Member 2” which expression shall, unless repugnant to the context include its successors and permitted assigns)

The parties are individually referred to as Party and collectively as Parties.

WHEREAS C-DAC, Pune, India has issued a Request for Proposal No _____ (RFP) inviting Bids/proposals from interested Bidder for Selection of Master System Integrator for Delhi Safe City Project:

AND WHEREAS the Parties have had discussions for formation of a JV for bidding for the said Project and have reached an understanding on the following points with respect to the Parties' rights and obligations towards each other and their working relationship.

As MUTUAL UNDERSTANDING OF THE PARTIES, IT IS HEREBY AGREED AND DECLARED AS FOLLOWS:

- i. The purpose of this Agreement is to define the principles of collaboration among the Parties to:
 - a. Submit a response jointly to Bid for the “**Request for Proposal for surveillance system under Delhi Safe City Project**” as a JV.
 - b. Sign Contract in case of award.
 - c. Provide and perform the supplies and services which would be ordered by C-DAC pursuant to the execution Contract.



ii. This MoU shall not be construed as establishing or giving effect to any legal entity such as, but not limited to, a company, a partnership, etc. It shall relate solely towards C-DAC for “**Request for Proposal for surveillance system under Delhi Safe City Project**” and related execution works to be performed pursuant to the Contract and shall not extend to any other activities.

iii. The Sole Bidder/ Principal JV Bidder shall be solely and severally responsible and bound towards C-DAC for the performance of the works in accordance with the terms and conditions of the RFP document, and Contract. The other JV Members shall support the Sole Bidder/Principal JV Bidder in successful implementation of the objectives.

iv. The Principal Partner shall be liable for all acts and omissions. The Principal Partner shall be responsible for the successful completion of the Contract / Agreement and C-DAC shall be communicating with the Principal Partner for all necessary actions. The Principal Partner shall be held liable and responsible for any breach of any of the terms and conditions of the Contract / Agreement.

v. ----- (Name of Party) shall act as the Sole Bidder/ Principal JV Bidder. As such, it shall act as the coordinator of the Party’s combined activities and shall carry out the following functions:

- a. To ensure the Technical, Financial and administrative co-ordination of the Project work and the services to be rendered in relation thereto
- b. To lead the contract negotiations of the Project work with C-DAC.
- c. The Principal JV Bidder member is authorized to receive instructions and incur liabilities for and on behalf of all other JV Members.
- d. In case of an award, act as channel of communication between C-DAC and the Parties to execute the Contract

vi. That the Parties shall carry out all responsibilities jointly and severally as Master System Integrator in terms of the Contract.

vii. That the broad roles and the responsibilities of each Party at each stage of the Bidding shall be as below:

Party A: _____

Party B: _____

Party C: _____

vii. That the Parties affirm that they shall implement the Project in good faith and shall take all necessary steps to see the Project through expeditiously.

viii. That this MoU shall be governed in accordance with the laws of India and courts in Delhi shall have exclusive jurisdiction to adjudicate disputes arising from the terms herein.

In witness thereof the Parties affirm that the information provided is accurate and true and have caused this MoU duly executed on the date and year above mentioned.

(Party of the first part) (Party of the second part) (Party of the third part)

Witness:



7.14. Annexure – 14: Pre-Qualification Criteria Document Index List

References of all the documents pertaining to Pre-Qualification/Eligibility Criteria must be indexed as per the format given below.

Sl. No.	Pre-Qualification Criteria	Page No. and Section No. in the Bid
1.		
2.		
3.		
4.		



7.15. Annexure – 15: Integrity Pact

(Format of Integrity Pact)

(TO BE ATTACHED WITH TECHNICAL BID DULY FILLED, STAMPED AND SIGNED ON EACH PAGE OF THE PACT)

PRE CONTRACT INTEGRITY PACT

Between

Centre for Development of Advanced Computing (C-DAC), a Scientific Society of Ministry of Electronics and Information Technology (MeitY), Govt of India, registered under the Societies Registration Act of 1860 and the Bombay Public Trusts Act of 1950, having its registered office at C-DAC Innovation Park, Panchavati, Pashan, Pune 411008, hereinafter referred to as “C-DAC” which expression shall mean and include, unless the context otherwise requires, his successors in office and assigns of the **First Part**.

And

M/s _____, a company/ firm/ individual (status of the company) constituted in accordance with the relevant law in the matter and having its registered office at _____ represented by Shri _____, hereinafter referred to as “The Bidder/Contractor” which expression shall mean and include, unless the context otherwise requires, his successors and permitted assigns of the Second Part.

WHEREAS C-DAC proposes to procure under laid down organizational procedures, contract/s for ----- (Name of the work/ goods/ services) and the Bidder/Contractor is willing to offer against NIT No. _____

NOW, THEREFORE,

To avoid all forms of corruption by following a system that is fair, transparent and free from any influence/prejudiced dealings prior to, during and subsequent to the currency of the contract to be entered into with a view to: -

Enabling C-DAC to obtain the desired said (work/ goods/ services) at a competitive price in conformity with the defined specifications by avoiding the high cost and the distortionary impact of corruption on public procurement, and

Enabling the Bidder(s)/Contractor(s) to abstain from bribing or indulging in any corrupt practice in order to secure the contract by providing assurance to them that their competitors will also abstain from bribing and other corrupt practices and C-DAC will commit to prevent corruption, in any form, by its officials by following transparent procedures.

1.0 Commitments of C-DAC

1.1 C-DAC undertakes that no official of C-DAC, connected directly or indirectly with the contract, will demand, take a promise for or accept, directly or through intermediaries, any bribe,



consideration, gift, reward, favour or any material or immaterial benefit or any other advantage from the Bidder/Contractor, either for themselves or for any person, organization or third party related to the contract in exchange for an advantage in the bidding process, bid evaluation, contracting or implementation process related to the contract.

- 1.2 C-DAC will, during the pre-contract stage, treat all the Bidders/Contractors alike, and will provide to all the Bidders/Contractors the same information and will not provide any such information to any particular Bidder/Contractor which could afford an advantage to that particular Bidder/Contractor in comparison to other Bidders/Contractors.
- 1.3 All the officials of C-DAC will report to the appropriate Authority any attempted or completed breaches of the above commitments as well as any substantial suspicion of such a breach.
- 1.4 In case any such preceding misconduct on the part of such official(s) is reported by the Bidder to C-DAC with full and verifiable facts and the same is prima facie found to be correct by C-DAC, necessary disciplinary proceedings, or any other action as deemed fit, including criminal proceedings may be initiated by C-DAC or Independent External Monitor and such a person shall be debarred from further dealings related to the contract process. In such a case while an enquiry is being conducted by C-DAC the proceedings under the contract would not be stalled.

2.0 Commitments of the Bidder(s)/Contractor(s)

The Bidder(s)/Contractor(s) commits itself to take all measures necessary to prevent corrupt practices, unfair means and illegal activities during any stage of its bid or during any pre-contract or post-contract stage in order to secure the contract or in furtherance to secure it and in particular commit itself to the following :-

- 2.1 The Bidder(s)/Contractor(s) will not offer, directly or through intermediaries, any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of C-DAC, connected directly or indirectly with the bidding process, or to any person, organization or third party related to the contract in exchange for any advantage in the bidding, evaluation, contracting and implementation of the contract.
- 2.2 The Bidder/Contractor further undertakes that it has not given, offered or promised to give, directly or indirectly any bribe, gift consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of C-DAC or otherwise in procuring the Contract or forbearing to do or having done any act in relation to the obtaining or execution of the contract or any other contract with Employer for showing or forbearing to show favour or disfavour to any person in relation to the contract or any other contract with C-DAC.
- 2.3 The Bidder(s)/Contractor(s) shall disclose the name and address of agents and representatives and Indian Bidder(s)/Contractor(s) shall disclose their foreign principals or associates.
- 2.4 The Bidder(s)/Contractor(s) shall disclose the payments to be made by them to agents/brokers or any other intermediary, in connection with this bid/contract.



- 2.5 The Bidder, either while presenting the bid or during pre-contract negotiations or before signing the contract, shall disclose any payments he has made, is committed to or intends to make to officials of C-DAC or their family members, agents, brokers or any other intermediaries in connection with the contract and the details of services agreed upon for such payments.
- 2.6 The Bidder/Contractor will not collude with other parties interested in the contract to impair the transparency, fairness and progress of the bidding process, bid evaluation, contracting and implementation of the contract.
- 2.7 The Bidder/Contractor will not accept any advantage in exchange for any corrupt practice, unfair means and illegal activities.
- 2.8 The Bidder/Contractor shall not use improperly, for purposes of competition or personal gain, or pass on to others, any information provided by C-DAC as part of the business relationship, regarding plans, technical proposals and business details, including information contained in electronic data carrier. The Bidder/Contractor also undertakes to exercise due and adequate care lest any such information is divulged.
- 2.9 The Bidder(s)/Contractor(s) commits to refrain from giving any complaint directly or through any other manner without supporting it with full and verifiable facts.
- 2.10 The Bidder(s)/Contractor(s) shall not instigate or cause to instigate any third person to commit any of the actions mentioned above.
- 2.11 If the Bidder/Contractor or any employee of the Bidder/Contractor or any person acting on behalf of the Bidder/Contractor, either directly or indirectly, is a relative of any of the officers of C-DAC, or alternatively, if any relative of an officer of C-DAC has financial interest/stake in the Bidder(s)/Contractor(s) firm(excluding Public Ltd. Company listed on Stock Exchange), the same shall be disclosed by the Bidder/Contractor at the time of filling of tender.
- The term 'relative' for this purpose would be as defined in Section 2(77) of the Companies Act 2013.
- 2.12 The Bidder(s)/Contractor(s) shall not lend to or borrow any money from or enter into any monetary dealings or transactions, directly or indirectly, with any employee of C-DAC.
- 2.13 The Bidder/supplier shall follow all rules and regulations of India.

3.0 Previous Transgression

- 3.1 The Bidder(s)/Contractor(s) declares that no previous transgression occurred in the last three years immediately before signing of this Integrity Pact, with any other company in any country in respect on any corrupt practices envisaged hereunder or with any Public Sector Enterprise / Government Department in India.



- 3.2 The Bidder agrees that if it makes incorrect statement on this subject, Bidder can be disqualified from the tender process or the contract, if already awarded, can be terminated for such reason.

4.0 Earnest Money (Security Deposit)

The provision regarding Earnest Money/Security Deposit as detailed in the Notice Inviting Tender (NIT) and Instruction to Bidders (ITB) section of the Bid Document is to be referred.

5.0 Sanctions for Violations

- 5.1. Any breach of the aforesaid provisions by the Bidder/Contractor or any one employed by it or acting on its behalf shall entitle C-DAC to take action as per the procedure mentioned in the “Guidelines on Banning of Business Dealings” and initiate all or any one of the following actions, wherever required:-
- (i) To immediately call off the pre contract negotiations without assigning any reason or giving any compensation to the Bidder/Contractor. However, the proceedings with the other Bidder(s)/Contractor(s) would continue.
 - (ii) The Earnest Money Deposit (in pre-contract stage) and/or Security Deposit/Performance Bond (after the contract is Signed) shall stand forfeited either fully or partially, as decided by C-DAC and C-DAC shall not be required to assign any reason thereof.
 - (iii) To immediately cancel the contract, if already signed, without giving any compensation to the Contractor. The Bidder/Contractor shall be liable to pay compensation for any loss or damage to C-DAC resulting from such cancellation/rescission and C-DAC shall be entitled to deduct the amount so payable from the money(s) due to the Bidder/Contractor.
 - (iv) To encash the Bank guarantee, in order to recover the dues if any by C-DAC, along with interest as per the provision of contract.
 - (v) To debar the Bidder/Contractor from participating in future bidding processes of C-DAC, as per provisions of “Guidelines on Banning of Business Dealings” which may be further extended at the discretion of C-DAC.
 - (vi) To recover all sums paid in violation of this Pact by Bidder(s)/Contractor(s) to any middleman or agent or broker with a view to securing the contract.
 - (vii) In cases where irrevocable Letters of Credit have been received in respect of any contract signed by C-DAC with the Bidder/ Contractor, the same shall not be opened/operated.
 - (viii) Forfeiture of Performance Security in case of a decision by C-DAC to forfeit the same without assigning any reason for imposing sanction for violation of this Pact.
- 5.2. C-DAC will be entitled to take all or any of the actions mentioned at para 6.1 to 6.8 of this Pact also on the Commission by the Bidder/Contractor or any one employed by it or acting on its behalf (whether with or without the knowledge of the Bidder/Contractor), of an offence as defined in Chapter IX of the Indian Penal Code, 1860 or Prevention of Corruption Act, 1988 or any other statute enacted for prevention of corruption in Employer’s country.
- 5.3. The decision of C-DAC to the effect that a breach of the provisions of this Pact has been committed by the Bidder / Contractor shall be final and conclusive on the Bidder / Contractor. However, the Bidder/Contractor can approach the Independent External Monitor(s) appointed for the purposes of this Pact.



6.0 Independent External Monitor(s)

- 6.1. C-DAC may appoint Independent External Monitor(s) (hereinafter referred to as Monitors) for this Pact.
- 6.2. The task of the Monitors shall be to review independently and objectively, whether and to what extent the parties comply with the obligations under this Pact.
- 6.3. The Monitors shall not be subject to instructions by the representatives of the parties and perform their functions neutrally and independently.
- 6.4. Both the parties accept that the Monitors have the right to access all the documents relating to the project/procurement, including minutes of meetings. The right to access records should only be limited to the extent absolutely necessary to investigate the issue related to the subject tender/contract.
- 6.5. As soon as the Monitor notices, or has reason to believe, a violation of this Pact, he will so inform ED/DG of C-DAC and request C-DAC to discontinue or take corrective action, or to take other relevant action. The Monitor can in this regard submit non-binding recommendations. Beyond this the Monitor has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action.
- 6.6. The Bidder(s)/Contractor(s) accepts that the Monitor has the right to access without restriction, to all Project documentation of C-DAC including that provided by the Bidder/Contractor. The Bidder/Contractor will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to Subcontractor(s). The Monitor shall be under contractual obligation to treat the information and documents of the Bidder/Contractor/Subcontractor(s) with confidentiality.
- 6.7. C-DAC will provide to the Monitor sufficient information about all meetings among the parties related to the project provided such meetings could have an impact on the contractual relations between the parties. The parties will offer to the Monitor the option to participate in such meetings as and when required.
- 6.8. The Monitor will submit a written report to the ED/DG of C-DAC within 10 days from the date of reference or intimation to him by C-DAC/Bidder and should the occasion arise, submit proposals for correcting problematic situations.
- 6.9. The word 'Monitor' would include both singular and plural.

7.0 Facilitation of Investigation

In case of any allegation of violation of any provisions of this Pact or payment of commission, C-DAC or its agencies shall be entitled to examine all the documents including the Books of Accounts of the Bidder/Contractor and the Bidder/Contractor shall provide necessary information and documents in English and shall extend all possible help for the purpose of such examination.

8.0 Law and Place of Jurisdiction

This Pact is subject to Indian Law. The place of performance and jurisdiction is the Registered Office of C-DAC. The arbitration clause provided in the tender document/contract shall not be applicable for any issue/dispute arising under Integrity Pact. The decision of C-DAC regarding breach of this Pact shall be final and binding on Bidder/Contractor.

9.0 Other Legal Actions



9.1. The actions stipulated in this Integrity Pact are without prejudice to any other legal action that may follow in accordance with the provisions of the extant law in force relating to any civil or criminal proceedings.

9.2. Changes and supplements as well as termination notice need to be made in writing.

9.3. If the Contractor is a partnership or a consortium or a joint venture, this pact must be signed by all partners of the consortium/joint venture.

10.0 Validity

10.1 The validity of this Integrity Pact shall be from date of its signing and extend upto 5 years or the complete execution/completion of the contract to the satisfaction of both C-DAC and the Bidder/Contractor/Seller, including warranty period, whichever is later. In case BIDDER is unsuccessful, this Integrity Pact shall expire after six months from the date of the signing of the contract or six months from the date of opening of price bids, whichever is earlier.

10.2 Should one or several provisions of this Pact turn out to be invalid, the remainder of this Pact shall remain valid. In this case, the parties will strive to come to an agreement to their original intention.

The Parties hereby sign this Integrity Pact at _____ on _____.

Employer	Bidder (Authorised Person)
Name of the Officer	(Name of the Person)
Designation	Designation
Place-----	Place-----
Date-----	Date-----
Witness1._____	Witness1._____
(Name and address)	(Name and address)

(End of Chapter & and End of Document)