

SECTION: 6
Service Level Agreement (SLA's)
&
Penalties

Section 6: SLA & Penalties

1.1 SLA defines the terms of the successful bidder's responsibility in ensuring the performance of the network based on the agreed performance indicators as detailed in the agreement. successful bidder has to co-ordinate with ISP and get the complaint closed and also has to produce documentary evidence regarding failure of Bandwidth by ISP & not by Network equipment's.

1.2 The table below summarizes the performance indicators for the services to be offered by the bidder-

S/N	SLA Terms	Description
1	Uptime	'Uptime' refers to network backbone availability across various segments of City wide area network i.e. between City Junction/locations and the CCC and Data center "%Uptime" means ratio of 'up time' (in minutes) in a month to Total time (in minutes) in the month multiplied by 100.
2	Planned Network Outage	'Planned Network Outage' refers to unavailability of network services due to infrastructure maintenance activities such as configuration changes, up gradation or changes to any supporting infrastructure. Details related to such planned outage shall be approved by the TENDERER or authorized authority and shall be notified to all the concerned stakeholder in advance (at least seven working days). It is desirable that such outage shall be taken on Sundays or other Government holidays to the extent possible.
3	Unplanned Network Outage	'Unplanned Network Outage' refers to an instance in which no traffic can pass in or out through which users are connects to the network Backbone
4	Not keeping man-power	If successful bidder does not deploy the required specified quantity & quality of manpower as per RFP or a person deployed is not reporting to the duty, there would be a penalty per person per day as defined in below table and will be deducted from the quarterly payment
5	Accuracy of ANPR/RLVD/Face Recognition System	RMC AND RAJKOT CITY POLICE or its nominated agency shall once in a month visit the CCC to check the accuracy of the said systems on random basis and mark out the difference if found lower than the accuracy level as per the SoW. Each such instance of accuracy lower than the defined limit shall be counted as an "instance" for penalty calculation
6	Incidence Resolution (Network)	The network outage, security or performance related issues impacting the network availability/performance and leading to unavailability of the services. Resolution of incidence as per below priority Levels: <ul style="list-style-type: none"> • L1 Level Severity: Impacting Command & Control Center. • L2 Level Severity: impacting one or more Zones. • L3 Level Severity: Impacting one or Junctions/ Endpoints/ Offices • L4 Level Severity: Impacting one or more end devices/utilities

S/N	SLA Terms	Description			
		#	Severity	Initial Response Time	Issue Resolution Time
		1	Level 1	15 Mins	1 Hour
		2	Level 2	30 Mins	2 Hours
		3	Level 3	60 Mins	6 Hours
		4.	Level 4	240 Mins	24 Hours
7	Incidence Resolution (CCC)	<ul style="list-style-type: none"> • Priority Level 1 Incident - Within 1 hr • Priority Level 2 Incident - Within 12 hr • Priority Level 3 Incident - Within 24 hr • Note: Incidents will be logged in the Helpdesk and the successful bidder will have to resolve the incident and provide necessary updates through the Help Desk Portal and co-ordinate with the stakeholders. Root Cause should be identified for all incidents; if root cause is not identified then additional penalties will be levied. 			
8	Security Breach	<ul style="list-style-type: none"> • Detection of security Breach - within 30 minutes • Mitigation of Security Breach - within 1 hr from the time of Breach • Note: The security breach will include but not limited to successful penetration of any Virus, trojan, malwares, zero-day attacks, intrusion, Denial of Service Attacks, etc. up to the server level. In case of any compromise of data due to the Security Breach then double penalty will be levied (this will not be counted within the maximum penalty cap limit). 			
9	Request Resolution (CCC)	<ul style="list-style-type: none"> • Priority Level 1 Incident - Within 2 hr • Priority Level 2 Incident - Within 24 hr • Priority Level 3 Incident - Within 36 hr • Note: Requests (like password reset, firewall port opening, hardening, etc.) will be logged in the Helpdesk and the successful bidder will have to resolve the request and provide necessary updates through the Help Desk Portal and co-ordinate with the stakeholders. 			

1.3 Successful Bidder shall be paid Quarterly Payment (QP) as per the services provided to the TENDERER. The overall penalty would be capped at 15% of QP amount. If the cap of overall penalty is reached in two consecutive quarters, the penalty cap for the third quarter onwards, for each quarter will increase by 5% over the penalty cap for the preceding quarter till it reaches 25% of the QP. In addition to the applicable penalty and the provisions pertaining to closure/termination of contract, the TENDERER shall be within its rights to undertake termination of contract if or anytime the penalty reaches to 20 % of the QP. Once the penalty cap has increased beyond 25%, if the bidder through better performance delivery for any quarter, brings the leviable penalty below 15% then the computation of the 1st of the 2 consecutive quarters as referred above will reset and will begin afresh. Availability will be calculated on a quarterly basis.

1.4 Appropriate Penalties will be recovered from the quarterly payment if successful bidder is not able to achieve required Service levels as mentioned below:

S/N	SLA	Target	Penalties
1	Delay in Delivery of Hardware	As per Implementation Time Lines	<ul style="list-style-type: none"> 1% of Contract value of undelivered/delayed hardware (as per Schedule-A & C of Price BID) per week or part thereof for delay in delivery
2	Delay in Implementation: Installation and Commissioning and FAT of hardware/software at Central and Site Location	As per Implementation Time Lines	<ul style="list-style-type: none"> 0.75% of Contract value (as per Schedule - A & B of Price BID) per week or part thereof for delay in implementation subject to maximum of 10% of the contract value. Once the maximum penalty reached, the TENDERER may terminate the contract and Forfeit the PBG.
3	Availability/Uptime of End Points like CCTV camera/ Wi-Fi APs/ LED Display panel/ IOT sensors etc.	99.00%	<ul style="list-style-type: none"> 99.00% or Better= NIL 98.50% to 98.99%=0.50% of QP 98.00 to 99.49% = 1.00% of QP 95.00 to 98% = 1.50% of QP Less than 95% = 5% of QP
4	Not keeping required Manpower	As per SLA	<ul style="list-style-type: none"> Management level staffs like PM/ Manager: 5000/- per day per person for un-sanctioned/ non-reporting All other staffs: 1000/- per day per person for un-sanctioned/ non-reporting Above charges are in addition to deduction of actual wages for the period of absence based on the rate schedule
5	Accuracy of ANPR/RLVD/Face Recognition System	As per SLA	Rs. 1000/- per instance
6	Delay in resolution of support/incidents for the devices installed by the bidder	As per SLA	<ul style="list-style-type: none"> Level 1: 0.25% of QP for every 2 Hours Delay in resolution. Level 2: 0.25% of QP for every 3 Hours delay in resolution; Level 3: 0.25% of QP for every 6 Hours delay in resolution Level 4: 0.25% of QP for every 8 Hours delay in resolution

7	Time Line for Retrieval from the Storage	Maximum 1 Hours for per request is allowed	<ul style="list-style-type: none"> • 0.50 % of the QP for every instance of delay beyond 1- hours • Note: Data Retrieval Request Through a Request Log Mechanism
8	Uptime of all IT components & services under scope	99.741% (at each individual component level)	<ul style="list-style-type: none"> • For each component 99.241-99.741 - 1.0% of QP; 98.741-99.241 - 2.0% of QP And so on If the uptime goes below 96.741, additional penalty of 1% will be charged on QP for each slab 1% downtime.
9	Uptime of all non-IT Components & services under scope	99.741% (at each individual component level)	<ul style="list-style-type: none"> • 99.249-99.749 - 0.5% of QP; 98.749-99.249 - 1.0% of QP And so on If the uptime goes below 96.749%, additional penalty of 0.5% will be charged on QP for a slab of 1%.
10	Security Breach	As per SLA	<ul style="list-style-type: none"> • 3% Of QP for every 30 Minutes delay in detection and additional 1% for every 1 hr. delay in the mitigation of security breach
11	Request Resolution (DC)	As per SLA	<ul style="list-style-type: none"> • level 1 Incident 0.25% of QP for every 2 hr. delay in resolution; Level 2 Incident 0.25% of QP for every 12 Hr delay in resolution; Level 3 Incident 0.25% of QP for every 18 hrs. delay in resolution
12	Incident Resolution (DC)	As per SLA	<ul style="list-style-type: none"> • level 1 Incident 0.25% of QP for every 2 hr delay in resolution; Level 2 Incident 0.25% of QP for every 6 Hr delay in resolution; Level 3 Incident 0.25% of QP for every 12 hrs delay in resolution

Note: The above clause for penalties due to delay in FAT shall only be applicable for the delay attributed solely to the successful bidder as per his roles and responsibilities.

SECTION: 7

FORMATS & ANNEXURES



Format 1 – Pre-Qualification Bid Letter

To,
XXXXXX
Sir/ Madam,

Sub: **“RFP for Selection of Implementation Agenc**

y for Supply, Installation, Commissioning, Operation & Maintenance of City-wide Surveillance and Wi-Fi Infrastructure at Rajkot City, Gujarat”

Reference: RFP No: <Bid REFERENCE NUMBER> Dated <DD/MM/YYYY>

We, the undersigned Bidder, having read and examined in detail the entire Bid documents do hereby propose to provide the services as specified in the above referred Bid document number along with the following:

1. **Earnest Money Deposit (EMD):** We have enclosed an EMD in the form of a Demand Draft/ Bank Guarantee no. _____ dated xx/xx/xxxx for Rs. 20,00,000 (Rupees Twenty Lakh only) drawn on_____. This EMD is liable to be forfeited in accordance with the provisions of this RFP.
2. **Contract Performance Bank Guarantee:** We hereby declare that in case the contract is awarded to us, we shall submit the contract performance bank guarantee as per compliance to the General terms Conditions mentioned in this RFP and Contract document.
3. We hereby declare that our bid is made in good faith, without collusion or fraud and the information contained in the bid is true and correct to the best of our knowledge and belief.
4. We understand that our bid is binding on us and that you are not bound to accept a bid you receive.

Thanking you,

Yours faithfully,

(Signature of the Bidder)

Seal :

Date:

Name & Designation:

BusinessAddress:

Format 2 – General Information about the Bidder

Details of the Bidder			
1	Name of the Bidder & Address of the Bidder		
2	Status of the Company (Public Ltd/ Pvt. Ltd)		
3	Details of Incorporation of the Company		Date:
			Ref. #
4	Details of Commencement of Business		Date:
			Ref. #
5	Company Identification Number (CIN)		
6	Registered Office of the Company:		
7	Composition of the Board of Directors of the Company. Please furnish Name, Designation and their DIN.		
8	Name of Company Secretary of the Company and his/her Membership No.		
9	Name and address of the Statutory Auditors of Company for the Financial years 2013-14, 2014-15 and 2015-16.		
10	Valid Value Added Tax Registration No. & Date		
11	Valid Service Tax Registration No. & Date		
12	Permanent Account Number (PAN)		
13	Name & Designation of the contact person to whom all references shall be made regarding this tender		
14	Telephone No. (with STD Code)		
15	E-Mail of the contact person:		
16	Fax No. (with STD Code)		
17	Website		
	Financial Details (as per audited Balance Sheets) (in Crore)		
18	Year	2013-2014	2014-2015
	Net Worth		
	Total Turnover		
	PAT		

Format 3 – Compliance & Eligibility Criteria Check list

S/N	Specific Requirements	Documents Required	Compliance Yes/No	Supporting Documents Attached or Not									
1	Bidder should be registered under the Companies Act 1956 and should be in operation in India for a period of at least 5 years as on tender floating date.	Certificates of incorporation											
2	Bidder should be an established IT / Telecom System Integrator and should have been engaged in setting-up and Operations & Maintenance Services of Network (Active or Passive)/CCTV projects/Command Control Centre / Data Centres/Public Wi-Fi during last five years as on tender floating date.	Work Orders / Client Certificates /Work completion certificate confirming year and area of activity should be enclosed as per format 7 of the tender document.											
3	<p>The bidder must have annual turnover of at least Rs. 150 Crores for each of the last three financial years as on 31st March, 2016.</p> <p><i>Average Annual Turnover of the bidder generated solely from IT/ITES services which includes, but not limited to supply/service for (active and passive) Networking (setting up or O&M) and Data Centre, CCTV surveillance project , Command Control Centre during last three financial years, should be at least Rs. 100 crores.</i></p> <p>NOTE: In case of the consortium, following criteria should be fulfilled by the each of the consortium members:</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th></th> <th style="text-align: center;">Lead Bidder</th> <th style="text-align: center;">Consortium Member</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">Annual turnover for each of the last three financial years as on 31st March, 2016.</td> <td style="text-align: center;">Min Rs. 75.0 Crores each year</td> <td style="text-align: center;">Min Rs. 75.0 Crores each year</td> </tr> <tr> <td style="text-align: center;">Average Annual Turnover during last three financial years generated solely from IT/ITES</td> <td style="text-align: center;">Min Rs. 50.0 Crores</td> <td style="text-align: center;">Min Rs. 50.0 Crores</td> </tr> </tbody> </table>		Lead Bidder	Consortium Member	Annual turnover for each of the last three financial years as on 31 st March, 2016.	Min Rs. 75.0 Crores each year	Min Rs. 75.0 Crores each year	Average Annual Turnover during last three financial years generated solely from IT/ITES	Min Rs. 50.0 Crores	Min Rs. 50.0 Crores	<p>Audited and Certified Balance Sheet and Profit/Loss Account of last 3 Financial Years i.e FY 13-14, FY 14-15, FY 15-16 should be enclosed.</p> <p>CA certificate mentioning turnover of the bidder should be enclosed as per format 6 of the tender document.</p>		
	Lead Bidder	Consortium Member											
Annual turnover for each of the last three financial years as on 31 st March, 2016.	Min Rs. 75.0 Crores each year	Min Rs. 75.0 Crores each year											
Average Annual Turnover during last three financial years generated solely from IT/ITES	Min Rs. 50.0 Crores	Min Rs. 50.0 Crores											

	<i>services as above mentioned</i>				
4	The bidder must have positive net worth and should be Profit making in each of the last three financial years as on 31 st March, 2016.	Audited and Certified Balance Sheet and Profit/Loss Account of last 3 Financial Years i.e FY 13-14, FY 14-15, FY 15-16 should be enclosed.	CA certificate mentioning Net worth & profit making of the bidder should be enclosed as per format 6 of the tender document.		
5	The bidder should have demonstrable expertise and experience in executing at least ONE project of <i>CCTV surveillance with</i> Command Control Centre during last five years reckoned from tender floating date, having a minimum value of Rs. 25 crores or TWO projects having a minimum value of Rs. 15 crores each. In case of ongoing project, bidder to demonstrate that the work completed as on tender floating date should meet the executed value criteria mentioned above.	Details of such projects undertaken along with Work Order copy and clients' completion/progress certificate should be enclosed as per format 7 of the tender document.			
6	Bidder along with OEMs of Major items (like CCTV Camera of all types, VMS, Video Analytics, Servers, Storages, Load balancer, Wifi with accessories, LED Display boards, Video wall etc.) should not be blacklisted by any Ministry under Government of India or by Government of any other State in India or by Government of Gujarat or any of the Government PSUs as on tender floating date.	Certificate / affidavit mentioning that the Bidder is not blacklisted by any Ministry of Government of India or by Government of any State in India or by Government of Gujarat or any of the Government PSUs. Self-Declaration Form must be submitted as per format 4 of the tender document			
7	OEMs of proposed equipment/components should have their own registered office in India as per the prevalent/ applicable laws of India and be in operation in India for last five years as on 31 st Mar	Undertaking from OEM confirming the compliance along with Gartner magic quadrant			

	<p>2016. Registered offices by way of Joint ventures, Franchise, agency, distribution partners will not be considered.</p> <p>a) OEMs for networking devices at aggregation layer and data center layer should be one of the leaders OR Challengers from the latest GARTNER list of companies for data center networking.</p> <p>b) OEM for other networking equipment's should be in the top Five positions in terms of market share in India as per latest available IDC report/ latest Gartner magic Quadrant.</p> <p>c) OEM for storage and servers should be one of the leaders OR Challengers from the latest GARTNER list of companies for storage.</p>	report copy .		
8	<p>The proposed camera OEM should have following:</p> <p>I. Direct presence in India more than 5 years as on bid submission date (not as joint venture, partnership firms or through any other association)</p> <p>II. Own RMA set up in India</p>	<p>Camera OEM should submit a declaration letter confirming the same along with</p> <p>(i) OEM's TIN no to be given as address proof.</p> <p>(II) OEM's Service tax no to be given as proof.</p>		
9	<p>The bidder should have Office in Gujarat OR</p> <p>The bidder should give undertaking for setting up Gujarat office in 45 days from the award of Work Order.</p>	<p>Copies of any two of the followings:</p> <p>Property Tax / Electricity / VAT/ CST / Telephone Bill / Registration / Lease agreement.</p> <p>OR</p> <p>Undertaking to open Office in Gujarat</p>		
10	<p>A letter of authority from the OEM / principals to provide support and product warranty services for offered products for following items must be enclosed.</p> <ol style="list-style-type: none"> 1. Camera (Individual 360° camera / 180° camera / PTZ / Surveillance / ANPR / RLVD) 2. VMS (Hardware & Software) 3. Video Analytics 4. Active Networking 5. IOT Sensors 6. Wi-Fi access point 7. Display units 8. Servers 	<p>The Letter of Authority (Manufacturer Authorization Form-MAF) from the respective principals / OEMs authorizing System Integrator to supply, installation, testing, commissioning & maintenance support must be enclosed along with the technical bid & without which the bid</p>		

	<p>9. Storage 10. UTM 11. SAN Switch 12. NMS Command control centre equipments</p>	<p>shall not be considered. OEM must ensure & confirm for minimum 5 years product support from the date of completion of the project and handing over to user for operation. Please refer MAF form format as per Annexure E in the RFP Undertaking of OEM for ONVIF support of VMS.</p>		
11	<p>In the event of a consortium - maximum two consortium members (including lead bidder) are allowed.</p> <p>All the members have to define their distinct roles and responsibilities as per format given in the Section 17 of RFP.</p> <p>Note: Both the Members of the Consortium are jointly and severally responsible and liable for successful completion of the Project.</p>	<p>Original Power of Attorney should be submitted in order to support their authorization to sign the document. The original power of attorney should be submitted on a stamp paper of Rs. 100/- (Rupees Hundred Only).</p>		



Format 4 – Declaration Letter regarding Black listing

To,
XXXXX

Sir/Madam,

I have carefully gone through the Terms & Conditions contained in the RFP Document [No _____] regarding **“RFP for Selection of Implementation Agency for Supply, Installation, Commissioning, Operation & Maintenance of City-wide Surveillance and Wi-Fi Infrastructure at Rajkot City, Gujarat”** for a period of five years. I hereby declare that we shall not be blacklisted / banned / disqualified / declared ineligible / declared having dissatisfactory performance by any government / quasi-government authority in India for supply of materials / carrying out operations and maintenance work.

I further certify that I am the Director/Company Secretary and am therefore, competent in my Company to make this declaration.

Yours faithfully,

(Signature of the Bidder)

Name & Designation
Seal
DIN/Membership No.
Date:
Business Address:

-----XXX-----



Format 5 – Unconditional Acceptance of RFP terms and conditions

To,
XXXXX

Sir/ Madam,

I have carefully gone through the Terms & Conditions contained in the RFP Document [No_____] regarding **“RFP for Selection of Implementation Agency for Supply, Installation, Commissioning, Operation & Maintenance of City-wide Surveillance and Wi-Fi Infrastructure at Rajkot City, Gujarat”**. I declare that all the terms and conditions and provisions of this RFP Document including Scope of Work and SLAs are acceptable to my company.

I further certify that I am the Director/Company Secretary and am therefore, competent in my Company to make this declaration.

Yours faithfully,

(Signature of the Bidder)

Name & Designation:

Seal DIN/Membership No.:

Date:

Business Address:

-----XXX-----

Format 6 – Annual Sales Turnover Statement

(On CA's letterhead)

Date: __/__/____

This is to certify that we M/s _____ are the statutory Auditors of M/s _____ and that the below mentioned calculations are true as per the Audited Financial Statements of M/s _____ for the below mentioned years.

S/N	Turnover	2013-2014	2014-2015	2015-2016
1	Annual Turnover as per Profit and Loss Account			
2	Net worth as per Audited Balance Sheet			
3	Average Annual Turnover of the bidder generated solely from IT/ITES services which includes, but not limited to supply/service for (active and passive) Networking (setting up or O&M), Data Centre, CCTV surveillance project, Command Control Centre.			
4	Net Profit as per Profit & Loss Account			

Note: Please upload the Copy of the audited Annual Accounts of the company for the last three years including Balance sheet, Profit & Loss A/c, Directors' Report and Statuary Auditor's Report.

-----XXX-----

Format 7 – Statement of Projects completed of Prescribed Nature & Size

Please fill one separate form for each project according to pre-qualification criteria/eligibility criteria: -

S/N	Criteria	Project
1	Implementer Company	
2	Customer's Name	
3	Scope of the Project	Please provide scope of the project, highlight Key Result Areas expected and
4	Value of Project	
5	Did the project involve supply/service for (active and passive) Networking (setting up or O&M) and Data Centre (setting up or O&M) / CCTV surveillance project and Command Control Centre	Yes/No
6	Total No. of nodes	
7	Total No. of Cameras	
8	Completion certificate	Yes/No
9	Customer Contact Person's detail	
A	Name	
B	Designation	
C	Email	
D	Phone	
E	Fax	
F	Mailing address	

Note:

1. The Copies of work order and the client certificates for satisfactory completion of the project and showing the order value and cost.
2. Completion certificate of prescribed nature and size as mentioned to be uploaded

-----XXX-----



Format 8 – Technical Bid Letter

(Shall be submitted on Bidder's letterhead duly signed by Authorized signatory)

Date: __/__/__

To,
XXXXX

Sir/ Madam,

Sub: "RFP for Selection of Implementation Agency for Supply, Installation, Commissioning, Operation & Maintenance of City-wide Surveillance and Wi-Fi Infrastructure at Rajkot City, Gujarat"

Reference: RFP No: <Bid REFERENCE NUMBER> Dated <DD/MM/YYYY>

We, the undersigned Bidder, having read and examined in detail the entire Bid documents do hereby propose to provide the services as specified in the above referred Bid document number along with the following:

1. We declare that all the services shall be performed strictly in accordance with the bid documents. Further we agree that additional conditions or assumptions, if any, found in the RFP documents shall not be given effect to.
2. We agree to abide by this bid for a period of 180 days from the date of bid submission or for any further period for which bid validity is extended and it shall remain binding upon us and Bid may be accepted at any time before the expiration of that period.
3. We hereby declare that our bid is made in good faith, without collusion or fraud and the information contained in the bid is true and correct to the best of our knowledge and belief.
4. We understand that our bid is binding on us and that you are not bound to accept a bid you receive.

Thanking you,

Yours faithfully,

(Signature of the Bidder)

Seal :

Date:

Name & Designation:

Business Address:

Format 9 – Technical Compliance Sheet

S/N	Name of Item	Make	Model	Supporting Documents (uploaded or Not) Pg. No. in physical bid
1				
2				
3				
4				

-----XXX-----

Format 10 – Relationship with OEM

Bidder needs to enclose the authorization on OEM's letterhead for direct OEM support for all IT equipment's major critical equipment's like routers, switch network device, etc. During the contract period, if OEM declares any equipment as end of support for any reasons, bidder has to replace that equipment with better or equivalent products without any cost to the TENDERER. OEM has to also submit on their letter head, complete details on the support available for the equipment, their end of support dates and replacement model if any. Format enclosed:

"Format for Certificate of Support from OEM"

Dated: __/__/__

To,
XXXX

Sir/ Madam,

Subject: Support for "Name of OEM" Inventory installed and in use for" _____"

Reference: RFP No: <Bid Ref. NUMBER> Dated <DD/MM/YYYY>

Certified that the hardware / software proposed by M/s _____, for which our company, "Name of OEM" is the OEM, has been quoted for support in the bid.

Subject to existence of valid pre-purchased support contract with "Name of OEM" we undertake to provide the following:

1. TAC Support for operation, maintenance and upgrade of the quoted product on 24 x 7 basis up to _____.
2. RMA replacement when required identified and approved by "Name of OEM" Technical Team (with an equivalent or upgrade model)
3. Full support towards migration to IPV6 for the _____ network by studying, planning, designing and recommending the migration path and methodology.



We also certify that the Bidder and "Name of OEM" have agreed to execute agreement in the above respect subject to the Bidder being selected for the Project and Bidder loading support order on "Name of OEM", a copy of same shall be shared with you, with in 1 month of ordering of support by Bidder.

For Partner
OEM

For

Authorized signatory of Bidder

Authorized signatory of OEM

<<BILL OF MATERIAL>>

-----**XXX**-----

Format 11 – Proposed Technical Solution

1. The Bidder is required to describe the proposed Technical Solution in this section. Following should be captured in the explanation:
 - ⇒ Clear articulation and description of the design and technical solution and various components (including diagrams and calculations wherever applicable)
 - ⇒ Extent of compliance to technical requirements specified in the scope of work
 - ⇒ Technical Design and clear articulation of benefits to Govt. of various components of the solution vis-à-vis other options available.
 - ⇒ Strength of the Bidder to provide services including examples or case-studies of similar solutions deployed for other clients.
2. The Bidder should provide detailed design and sizing calculation for the following listing all assumptions that have been considered:
 - ⇒ Supply, Installation and commissioning of the said Infrastructure
 - ⇒ Operations & Maintenance
 - Help Desk Services
 - Escalation Plan
 - Training Content and Schedules
 - System Maintenance & Management
 - Network / Security Administration
 - Backup & Restoration
3. Approach & Methodology for O&M of ICT infrastructure and adherence to SLAs, setting up of new Junctions/Locations, Operation and Services of Complete Infrastructure,
4. Bidder shall provide a detailed project plan with timelines, handing over and taking over process, resource allocation, milestones etc. for setting up of required ICT infrastructure and its Operations & Maintenance.
5. Bidder has to give their proposed technical solution's presentation to TENDERER at the time of technical evaluation. If any deviation/any changes given by TENDERER bidder has to submit undertaking the same.

-----XXX-----

Format 12 – Project Management Plan

The Bidder shall give a detailed description of Project Management Plan it plans to implement as part of the Project “_____”.

Any Best practices that it would use could also be mentioned. Typical questions that would need to be answered include:

1. What kind of hierarchy for Project Management does the Bidder propose?
2. What issues generally arise with regard to Project management of WAN and Data Centre and CCC , Edge Utilities ?
3. How the Bidder plans to mitigate any risks with regard to project management?
4. How Bidder proposes to deploy manpower for Upgradation and O&M?

-----**XXX**-----



Format 13 – Core Project Team

Bidder shall provide a detailed description of the proposed Core Project Team to be deployed for the O&M of project “_____”. The description should include details about the Project Team hierarchy and a detailed explanation of the role to be played by each individual that would be part of the O&M team.

-----XXX-----

Format 14 – Financial Bid Letter

To,
XXXX

Sir/Madam,

Subject: **“RFP for Selection of Implementation Agency for Supply, Installation, Commissioning, Operation & Maintenance of City-wide Surveillance and Wi-Fi Infrastructure at Rajkot City, Gujarat”**

Reference: **RFP No: <Bid REFERENCE NUMBER> Dated <DD/MM/YYYY>**

We, the undersigned Bidder, having read and examined in detail all the Bid documents in respect of **“RFP for Implementation Agency for Supply, Installation, Commissioning, Operation & Maintenance for of City wide Surveillance and Wi-Fi Infrastructure for Rajkot City”** do hereby propose to provide services as specified in the Tender documents number **<Bid REFERENCE NUMBER> Dated <DD/MM/YYYY>**

1. PRICE & VALIDITY

- All the prices mentioned in our Bid are in accordance with the terms as specified in the Bid documents. All the prices and other terms and conditions of this Bid are valid for a period of 180 calendar days from the date of Bid submission.
- We hereby confirm that our Bid prices are exclusive all taxes. However, all the applicable taxes are quoted separately under relevant sections.
- We have studied the clause relating to Indian Income Tax and hereby declare that if any Income Tax, surcharge on Income Tax, Professional and any other corporate Tax is altered under the law, we shall pay the same.

2. UNITRATES

- We have indicated in the relevant schedules enclosed the unit rates for the purpose of on account of payment as well as for price adjustment in case of any increase to / decrease from the scope of work under the contract.

3. DEVIATIONS

- We declare that all the services shall be performed strictly in accordance with the Bid Documents Further we agree that additional conditions, if any, found in the bid documents, shall not be given effect to.

4. TENDERPRICING

- We further confirm that the prices stated in our bid are in accordance with your Instruction to Bidders included in RFP document.

5. QUALIFYINGDATA

- We confirm having submitted the information as required by you in your Instruction to Bidders. In case you require any other further information/documentary proof in this regard before evaluation of our bid, we agree to furnish the same in time to your satisfaction.

6. BID PRICE

- We declare that our Bid Price is for the entire scope of the work as specified in the Schedule of Requirements and RFP documents. These prices are indicated in Formats (Section 5) of this Section attached with our bid as part of the RFP.

7. CONTRACT PERFORMANCE GUARANTEE BOND

- We hereby declare that in case the contract is awarded to us, we shall submit the contract performance guarantee bond in the form prescribed in Format 16- Proforma and as per relevant clause(s) in the - General Terms and Conditions section.

8. We hereby declare that our Bid is made in good faith, without collusion or fraud and the information contained in the Tender is true and correct to the best of our knowledge and belief.

9. We understand that our Bid is binding on us and that you are not bound to accept a bid you receive.

10. We confirm that no Technical deviations are attached here with this Financial offer.

Thanking you,

Yours faithfully,

(Signature of the Bidder)

Name & Designation:

Seal :

Date:

Business Address:

Format 15

Format of Earnest Money Deposit in the form of Bank Guarantee

Ref:

Bank Guarantee No.

Date:

To,
XXXXXX

We, _____ bank, having our registered office at _____ (hereinafter called "the Bank" which expression shall unless repugnant to the context or meaning thereof, include its successors, administrators, executors and assigns) informed that (*Bidder's company Name*) _____ having its registered office at _____ (hereinafter called "the Bidder") has submitted to you its bid dated _____ (hereinafter called "the Bid") for E – tender (No: GIPL/RMC-SmartCity-ICT/16-17/__) issued for **"RFP for Selection of Implementation Agency for Supply, Installation, Commissioning, Operation & Maintenance of City-wide Surveillance and Wi-Fi Infrastructure at Rajkot City, Gujarat"**.

Furthermore, we understand that, according to your bid conditions, bid must be supported by a bank guarantee as EMD for the bid. We, the Bank, at the request of the bidder do hereby guarantee and undertake to pay the RMC during the currency of the guarantee on written demand any and all money payable by the bidder to the extent of **Rs. 90,00,000/- (Ninety Five Lacs only)** as aforesaid at any time up to **(9 months from the last date of bid submission)** (hereinafter called "the Expiry Date") without any demur, reservation, contest, recourse or protest and/or without any reference to the bidder. Any such demand made by the RMC on the Bank shall be conclusive and binding notwithstanding any difference between the RMC and the bidder or any dispute pending before any Court, Tribunal, Arbitrator or any other authority. The Bank undertakes not to revoke this guarantee during its currency without prior consent of the RMC and further agrees that the guarantee herein contained shall continue to be enforceable until RMC discharges this guarantee or until the Expiry Date, whichever is earlier.

The Bank also agrees that the bidder at its option shall be entitled to enforce this guarantee against the Bank as a principal debtor, in the first instance without proceeding against the bidder and notwithstanding any security or other guarantee that the RMC may have in relation to the bidder's liabilities.

At the request of the Bidder, we _____ (bank Name & Address) hereby irrevocably undertake to pay you any sum or sums not exceeding in total an amount of **Rs. 90,00,000/- (Ninety Lacs only)** upon receipt by us of your first demand in writing accompanied by a written statement stating that the Bidder is in breach of its obligation(s) under the bid conditions, because the Bidder:

THE CONDITIONS of this obligation are:

1. The E.M.D. may be forfeited:
 - a. if a Bidder withdraws its bid during the period of bid validity
 - b. Does not accept the correction of errors made in the tender document;
 - c. In case of a successful Bidder, if the Bidder fails:
 - i. To sign the Contract as mentioned above within the time limit stipulated by purchaser or
 - ii. To furnish performance bank guarantee as mentioned above or
 - iii. If the bidder is found to be involved in fraudulent practices.
 - iv. If the bidder fails to submit the copy of purchase order & acceptance thereof.

This guarantee will expire: (a) if the Bidder is the successful Bidder, upon our receipt of copies of the Performance Guarantee / Security Deposit by the successful bidder to RMC & upon the instruction of the RMC; and (b) if the Bidder is not the successful Bidder then upon our receipt of a copy of RMC's notification to the Bidder of the name of the successful Bidder; or (ii) End of the day of Expiry Date.

Consequently, any demand for payment under this guarantee must be received by us at the office on or before that date.

This guarantee is subject to the Uniform Rules for Demand Guarantees, ICC Publication No. 758.

Notwithstanding anything contained herein:

Our liability under this Bank Guarantee shall not exceed **Rs.90,00,000/- (Ninety Lacs only)**

This Bank Guarantee shall be valid up to the Expiry Date.

We are liable to pay the guaranteed amount or any part thereof under this Bank Guarantee only & only if we receive a written claim or demand on or before _____(Expiry date).

Dated this _____ day of _____ 2017.

(Name and designation of the officer)

(Name and designation of the officer)



Format 16: Performance Bank Guarantee

Ref. No. Bank Guarantee No.

Dated:

To,
Municipal Commissioner
Rajkot Municipal Corporation (hereinafter called as "RMC")
Dhebar Road
Rajkot-360001.

Dear Sirs,

In consideration of Rajkot Municipal Corporation (RMC) having its registered office at Dhebar Road, Rajkot – 360001, Gujarat (state) India, (hereinafter referred to as **RMC** which expression shall unless repugnant to the context or meaning thereof include all its successors, administrators, or meaning thereof include all its successors, administrators, executors and assignees) having issued **LOI No: Date of LOI/WO** for work of **"Selection of Implementation Agency for Supply, Installation, Commissioning, Operation & Maintenance of City-wide Surveillance and Wi-Fi Infrastructure at Rajkot City, Gujarat"** (herein after called the contract which express shall include all the amendments thereto) with **Name of successful bidder** having its registered Office at **Address** (hereinafter referred to as the **System Integrator or Contractor**) which expression shall unless repugnant to the context or meaning thereof mean and include all its successors, administrators, executors and assignees) and RMC having agreed that the contractor shall furnish to RMC a performance guarantee for Indian **Amount** for the faithfully performance of the entire contract / warranty for defects liability during the defects liability period.

1. We _____ (Name and full address of the bank) registered under the laws of _____ having head / registered office at _____ (hereinafter referred to as the 'Bank' which expression shall, unless repugnant to the context or meaning thereof, include all its successors, administrators, executors and permitted assigns) guarantee and undertake to pay immediately on first demand by RMC in writing, the monies to the extent of Indian **Amount** without any demur, reservation, contest or protest and / or without any reference to the contractor. Any such demand made by RMC on the Bank by serving a written notice shall be conclusive and binding, without any proof, on the Bank as regards the amount due and payable, notwithstanding any dispute(s) pending before any Court, tribunal, Arbitrator or any other authority and/or any other matter of thing whatsoever, as liability under these presents being absolute and unequivocal. We agree that the guarantee herein contained shall be irrevocable and shall continue to be enforceable until it is discharged by RMC in writing. This

guarantee shall not be determined, discharged or affected by the liquidation, winding up, dissolution or insolvency of the Contractor and shall remain valid, binding and operative against the bank.

2. The bank also agrees that RMC at its option shall be entitled to enforce this Guarantee against the bank as a principal debtor, in the first instance, without proceeding against the Contractor and notwithstanding any security or other guarantee that RMC may have in relation to the contractor's liabilities.
3. The bank further agrees that RMC shall have the fullest liberty without our consent and without affecting in any manner our obligations hereunder to vary any of the terms and conditions of the said contract or to extend time of performance by the said contractor from time to time or to postpone for any time or from time to time exercise of any of the powers vested in RMC against the said contractor and to forbear or enforce any of the terms and conditions relating to the said agreement and we shall not be relieved from our liability by reason of any such variation, or extension being granted to the said contract or for any forbearance, act or omission on the part of RMC or any indulgence by RMC to the said contractor or any such matter or thing whatsoever which under the law relating to sureties would, but for this provision, have effect of so relieving us.
4. The bank further agree that the Guarantee herein contained shall remain in full force during the period that is taken for the performance of the contract and all dues of RMC under or by virtue of this contract have been fully paid and its claim satisfied or discharged or till RMC discharges this guarantee in writing whichever is earlier.
5. This Guarantee shall not be discharged by any change in our constitution, in the constitution of RMC or that of the Contractor.
6. The Bank confirms that this Guarantee has been issued with observance of appropriate laws of the country of issue.
7. The Bank also agrees that this Guarantee shall be governed and construed in accordance with Indian Laws and subject to exclusive Indian Courts at Rajkot, Gujarat, India.
8. Notwithstanding anything contained herein above, our liability under this guarantee is limited to Indian **Amount** and our guarantee shall remain in force until **Months from the date of the submission**.

Any claim under this Guarantee must be received by us within 90 days from the expiry of this Bank Guarantee. If no such claim has been received by us by the said date, the rights of RMC under this guarantee will cease. However, if such a claim has been received by us by the said date, all the rights of RMC under this



guarantee shall be valid and shall not cease until we have satisfied that claim.

In witness whereof, the bank through its authorized officer has set its hand and stamp on this _____ day of _____ at _____.

(Signature)
Full name, designation and
official address (in legible letters) with Bank stamp

Attorney as per Power of Attorney No.
Date:

WITNESS NO. 1
(Signature)
Full name and official address
Address (in legible letters)

WITNESS NO. 2
(Signature)
Full name and official address
Address (in legible letters)

Format 17: Format for Consortium Agreement

(On Rs. 100/- Stamp paper)

Consortium Agreement

This Consortium Agreement (hereinafter the "Agreement") entered into this ___ day of _____ ("Date of Signing")

BETWEEN

1. _____ (First Party) through Authorized Signatory _____ having their principal place of business at _____ in India for and on behalf of _____ (hereinafter called "the Bidder" which expression shall include its legal successors and permitted assignees) of the

ONE PART;

2. _____ (Second Party) through Authorized Signatory _____ having their principal place of business at _____ in India for and on behalf of _____ (hereinafter called "the Consortium Partner" which expression shall include its legal successors and permitted assignees) of the

SECOND PART;

RECITALS

A. Guj Info Petro Limited (GIPL) on behalf of Rajkot Municipal Corporation, herewith called as RMC, has issued a E- TENDER NO: GIPL/RMC-SmartCity-ICT/16-17/32 (hereinafter the "Tender Document"), inviting bids for Selection of Implementation Agency for Supply, Installation, Commissioning, Operation & Maintenance of City-wide Surveillance and Wi-Fi Infrastructure at Rajkot City, Gujarat (RAJKOT EYE – WAY PROJECT);

B. As specified in clause No. 11 of the eligibility criteria of the Tender Document, the Bidder has formed a consortium and hereby enters into this Agreement and the Parties have agreed to the participate as members of the Consortium subject to said terms and conditions of this Agreement

The members of the Agreement shall each be referred to as the "Party" and together as the "Parties"

NOW THEREFORE, in consideration of the mutual covenants of the Parties, the sufficiency whereof is hereby acknowledged and other good valuable consideration, the Parties agree as follows:

1. Definitions and Interpretation

1.1. Definitions

Capitalized terms used in this Agreement shall have their respective defined meanings, and/or shall have the meaning specified in the Tender Document, unless the context expressly or by necessary implication otherwise requires.

1.2. Interpretation

- a. For the purpose of this Agreement, where the context so admits, (i) the singular shall be deemed to include the plural and vice-versa, and (ii) masculine gender shall be deemed to include the feminine gender and vice-versa.
- b. References to a "person" if any shall, where the context so admits, include references to natural persons, partnership firms, companies, bodies corporate and associations, whether incorporated or not or any other organization or entity including any governmental or political subdivision, ministry, department or agency thereof;
- c. The headings and sub-headings are inserted for convenience only and shall not affect the construction and interpretation of this Agreement.
- d. References to the word "include" and "including" shall be construed without limitation.
- e. Any reference to day shall mean a reference to a calendar day;

2. Purpose of Consortium Agreement

The purpose of this Agreement is to specify the roles and responsibilities of the Parties in implementation and matters connected with the ".....Tender floated by RMC and to set out further rights and obligations of the Parties supplementing but not conflicting with those present in the Tender Document. The Roles of each parties are specifically defined at each stage of the Project is as per Annexure-1 [Note: Bidder has to separately submit Annexure – 1 if any].

3. Duration

This Agreement shall come into force as of the date of signing and shall continue in full force and effect until the complete discharge of all obligations, concerning the carrying out of the Project, which have been taken on by the Parties under Tender Document and under this Agreement.

4. Coordinator

4.1 The Parties hereby understand and agree that there shall be a "Lead Partner" who shall be the point of contact for the purpose of the Project. It is hereby agreed by the Parties that for the purpose of the Agreement _____ has been appointed as "Lead Partner". The Lead Partner is hereby authorized by the Parties to make representations and declarations/ incur liabilities and receive instructions on their behalf and the parties shall not raise any dispute/ claim in this regard in future.

4.2 For the purpose of this Agreement, the Tender Document, the Lead Partner shall be the single point of contact for the RMC\GIPL, shall have the overall responsibility of the management of the Project and shall have single point responsibility for ensuring that all members of the consortium are complying with the terms and conditions set out in the Tender Document.

4.3 All instructions/communications from RMC\GIPL to the Lead Partner shall be deemed to have been duly provided to all the members of the consortium.

4.4 Notwithstanding anything to the contrary contained elsewhere in this agreement, all Parties of the consortium shall be jointly & severally responsible for the obligations under the Tender Document,

irrespective of the specific roles/responsibilities undertaken by them.

5. Rights and Obligations

5.1 For delivery of all services as per the agreement with RMC, Lead Partner shall be primarily accountable and responsible.

5.2 The Lead Partner shall be responsible for the transmission of any documents and information connected with the Project to the Parties concerned.

5.3 It is hereby clarified that representations and declarations made by the Lead Partner shall be legally binding on all the Parties of the Agreement.

5.4 Each Party shall use reasonable efforts to perform and fulfill, promptly, actively and on time, all of its obligations under the Tender Document and this Agreement.

5.5 All commercial activities with RMC will be conducted by the Lead Partner.

5.6 In case RMC suffers any loss or damages on account of any breach of the Contract, the Lead Partner as well as the other consortium members undertakes to promptly make good such loss or damage caused to VMC on demand without any demure. RMC shall have the right to proceed against anyone of the partners and it shall neither be necessary nor obligatory on the part of RMC to proceed against the Lead Partner before proceeding against the other consortium members.

6. Responsibilities towards each other

a) Each Party undertakes :-

- i. To promptly notify other Parties about any significant delay in fulfillment of milestones in relation to the Project;
- ii. To inform other Parties of relevant communications it receives from third parties in relation to the Project.

b) Each Party shall use reasonable efforts to ensure the accuracy of any information or materials it supplies hereunder and promptly to correct any error that came to its knowledge.

c) Each Party shall act in good faith. When a Party believes that for carrying out the Project or use of knowledge from the Project it might require access rights to another Party's pre-existing know-how or to another Party's knowledge and material which is not from the Project, it shall obtain written permission from the Party prior to the use of such material.

d) Each Party shall abide with the terms of confidentiality as described in Tender Document and shall also abide with all the clauses of the Tender Document.

e) Each Party shall share and disclose information including confidential information and documents as may be necessary for the Project. The Parties hereby understand and agree that the information shall be used solely for the purpose of the Project and not for its own use or for any third party benefit.

7. Assignment

No Party shall, without the prior written consent of the RMC and of the other Parties, assign or otherwise transfer partially or totally any of its rights and obligations under Agreement.

8. Representation and Warranties

8.1. The Parties hereby represents and warrants that: -

a) They are duly organized and validly existing under the laws of India and have full power and authority to enter into this Agreement and to perform its obligations under this Agreement. The execution and validity of this Agreement and the consummation of the transactions contemplated by this Agreement have been duly authorized by all necessary action on the part of the Parties;

b) This Agreement constitutes a valid and binding obligation of the Parties, enforceable against them in accordance with the terms hereof, and the execution, delivery and performance of this Agreement and all instruments or agreements required hereunder do not contravene, violate or constitute a default of or require any consent or notice under any provision of any agreement or other instrument to which the Bidder is a party or by which the Bidder are or may be bound.

c) Each of the representations and warranties shall be construed as a separate representation, warranty, covenant or undertaking, as the case may be, and shall not be limited by the terms of any other representation or warranty or by any other term of this Agreement.

d) The Parties have read, understood and agree with the terms of this Agreement and the Tender Document.

9. Irrevocable

Parties herein agrees that this Consortium Agreement shall be irrevocable and shall form an integral part of Contract and shall continue to be enforceable against the Parties herein by RMC till the terms of the Agreement for ERP Project are fulfilled.

10. Miscellaneous

a) Notices, demands or other communication required or permitted to be given or made under this Agreement shall be in writing in the English language and delivered personally or sent by prepaid post with recorded delivery addressed to the intended recipient at its address set forth below:

i. If to the Party of the First Part

ii. If to the Party of the Second Part

b) Any such notice, demand or communication shall, unless the contrary is proved, be deemed to have been duly served at the time of delivery in the case of service by delivery in person or by registered post.



- c) Each Party shall bear its own legal, accounting, professional and advisory fees, commissions and other costs and expenses incurred by it in connection with this Agreement and the transactions contemplated herein.
- d) This Agreement supersedes all prior discussions and agreements (whether oral or written, including all correspondence) if any, between the Parties with respect to the subject matter of this Agreement.
- e) Any provision of this Agreement, which is invalid or unenforceable, shall be ineffective to the extent of such invalidity or unenforceability, without affecting in any way the remaining provisions hereof.
- f) This Agreement shall be governed and interpreted by, and construed in accordance with the substantive laws of India, without giving effect to the principles of conflict of laws there under.
- g)
 - I. Any and all disputes or differences between the Parties arising out of or in connection with this Agreement or its performance shall, so far as it is possible, be settled amicably through consultation between the Parties.
 - II. If after 30 (thirty) days of consultation, the Parties have failed to reach an amicable settlement, on any or all disputes or differences arising out of or in connection with this Agreement or its performance, such disputes or differences shall be submitted to final and binding arbitration. The arbitration panel shall consist of three arbitrators: one nominated _____, one nominated by _____ and the third nominated jointly by both the arbitrators. The arbitration shall be governed by the Arbitration and Conciliation Act, 1996. The place of arbitration shall be Rajkot, India. The language to be used in the arbitration proceedings shall be English. The award of the arbitration proceedings will be final and binding on both Parties to the Agreement.
 - III. This Agreement shall be governed by the laws of India. Courts Rajkot shall have exclusive jurisdiction in all matters arising hereunder.

IN WITNESS WHEREOF, the Parties have entered into this Agreement the day and year first above written.

For _____

Authorized Signatory

Name:

Designation:

In the presence of:

Name:

Address:



For, _____

Authorized Signatory

Name:

Designation:

In presence of:

Witness 1: _____

Witness 2: _____

Annexure A
List of Locations for Camera System Deployment

Location Wise CCTV Camera Details - RAJKOT CITY

Sr. No.	Location Name	Type of Location	fixed cameras 2MP	PTZ Camera 2MP, 20x	360 Degree Camera	180 Degree Camera	Traffic Solution	
							2MP ANPR	5MP Context
1	Trikon Baug	Fully Covered Traffic Junction		3	1		8	4
2	Jubilee Chowk	Fully Covered Traffic Junction		4			8	4
3	KKV Chowk	Fully Covered Traffic Junction		4			8	4
4	Mavdi Chowkdi	Fully Covered Traffic Junction		3	1		8	4
5	Raiya Chowkdi	Fully Covered Traffic Junction		3	1		8	4
6	Hanuman Madhi	Fully Covered Traffic Junction		4			8	4
7	Indira Circle	Fully Covered Traffic Junction		4			8	4
8	Jamtower Chowk	Fully Covered Traffic Junction		4			8	4
9	Dhebar Chowk	Fully Covered Traffic Junction		4			8	4
10	Nagrik Bank Chowk	Fully Covered Traffic Junction		3	1		8	4
11	Makkam Chowk	Fully Covered Traffic Junction		3		1	8	4
12	Nanamava Circle	Fully Covered Traffic Junction		3	1		8	4
13	Astron Chowk	Fully Covered Traffic Junction		3	1		8	4
14	Ramdevpir Chowkdi	Fully Covered Traffic Junction		3	1		8	4
15	RMC Chowk	Traffic Junction (Only for Surveillance)	4	1				
16	Sanganva Chowk	Traffic Junction (Only for Surveillance)	4	1				
17	Kothariya Naka Police Chowkey	Traffic Junction (Only for Surveillance)	4	1				
18	Mandvi Chowk	Traffic Junction (Only for Surveillance)	4	1				

19	Hospital Chowk	Traffic Junction (Only for Surveillance)	4		1			
20	Court Chowk	Traffic Junction (Only for Surveillance)	4	1				
21	Ashapura Mandir	Traffic Junction (Only for Surveillance)	4	1				
22	Malaviya Chowk	Traffic Junction (Only for Surveillance)	4		1			
23	Yagnik Road - T Point	Traffic Junction (Only for Surveillance)	4			1		
24	Imperial Hotel	Traffic Junction (Only for Surveillance)	4	1				
25	Delux Chowk	Traffic Junction (Only for Surveillance)	4		1			
26	Parevadi Chowk	Traffic Junction (Only for Surveillance)	4	1				
27	Chunarwada Chowk	Traffic Junction (Only for Surveillance)	4	1				
28	Greenland Chowkdi	Traffic Junction (Only for Surveillance)	4		1			
29	Kuvadva Road Police Station	Traffic Junction (Only for Surveillance)	4	1				
30	Pedak Road Pani na Ghoda	Traffic Junction (Only for Surveillance)	4	1				
31	Marketing Yard Gate	Traffic Junction (Only for Surveillance)	4	1				
32	80 ft Road Chowkdi	Traffic Junction (Only for Surveillance)	4		1			
33	Haidari Chowkdi	Traffic Junction (Only for Surveillance)	4	1				
34	Ambedkar Colony Gate	Traffic Junction (Only for Surveillance)	4	1				
35	Kothariya Chowkdi (Hudco)	Traffic Junction (Only for Surveillance)	4		1			
36	Nanda Hall	Traffic Junction (Only for Surveillance)	4	1				
37	Trishul Chowk	Traffic Junction (Only for Surveillance)	4	1				
38	Hudco Police Chowkey	Traffic Junction (Only for Surveillance)	4	1				
39	Sorathiyawadi Circle	Traffic Junction (Only for Surveillance)	4	1				
40	Sorathiyawadi way bridge Chowk	Traffic Junction (Only for Surveillance)	4	1				
41	Bhaktinagar Circle	Traffic Junction (Only for Surveillance)	4	1				
42	Punitnagar Water Tank	Traffic Junction (Only for Surveillance)	4	1				

43	Govardhan Chowk 150 ft Road	Traffic Junction (Only for Surveillance)	4	1				
44	Umiya Chowk 150 ft Road	Traffic Junction (Only for Surveillance)	4	1				
45	Mahapuja Chowk 150 ft Road	Traffic Junction (Only for Surveillance)	4	1				
46	Nana Mava Chowk	Traffic Junction (Only for Surveillance)	4	1				
47	Big Bazaar 150 ft Road	Traffic Junction (Only for Surveillance)	4	1				
48	Anand Bungla Chowk	Traffic Junction (Only for Surveillance)	4	1				
49	Sawaminarayan Chowk	Traffic Junction (Only for Surveillance)	4	1				
50	Motamava Chowk	Traffic Junction (Only for Surveillance)	4		1			
51	Kotecha Chowk	Traffic Junction (Only for Surveillance)	4	1				
52	Rani Tower Kalavad Road	Traffic Junction (Only for Surveillance)	4	1				
53	Backbon Chowk	Traffic Junction (Only for Surveillance)	4	1				
54	Atithi Chowk	Traffic Junction (Only for Surveillance)	4	1				
55	Raiya Tele Exchange 150 Road	Traffic Junction (Only for Surveillance)	4	1				
56	Alap Green City	Traffic Junction (Only for Surveillance)	4		1			
57	Akashwani Chowki	Traffic Junction (Only for Surveillance)	4	1				
58	Bajarang Wadi Chowkdi	Traffic Junction (Only for Surveillance)	4	1				
59	Amrapali Fatak	Traffic Junction (Only for Surveillance)	4	1				
60	A G Chowk	Traffic Junction (Only for Surveillance)	4	1				
61	Bajarang wadi circle	Traffic Junction (Only for Surveillance)	4		1			
62	Salimar Building 150 ft Road Bridge	Traffic Junction (Only for Surveillance)	4	1				
63	Moti Tanki Chowk	Traffic Junction (Only for Surveillance)	4	1				
64	Railway Station Road	Traffic Junction (Only for Surveillance)	4	1				
65	Limda Chowk	Traffic Junction (Only for Surveillance)	4	1				

66	Bhilwas Chowk	Traffic Junction (Only for Surveillance)	4	1				
67	Junction Plot 5	Traffic Junction (Only for Surveillance)	4	1				
68	Kishanpara Chowk	Traffic Junction (Only for Surveillance)	4		1			
69	Police HQ Gate	Traffic Junction (Only for Surveillance)	4	1				
70	Sandhiya Pool Jamnagar Road	Traffic Junction (Only for Surveillance)	4	1				
71	Gondal Chowkdi	Traffic Junction (Only for Surveillance)	4		1			
72	Ruda Transport Nagar	Traffic Junction (Only for Surveillance)	4	1				
73	Bedi Chokadi Morbi Road	Traffic Junction (Only for Surveillance)				1		
74	Munjaka Chokadi	Traffic Junction (Only for Surveillance)				1		
75	Bhagvatipara choki	Traffic Junction (Only for Surveillance)			1			
76	Pal Chokadi Eng College Road	Traffic Junction (Only for Surveillance)			1			
77	Jungleswar	Traffic Junction (Only for Surveillance)			1			
78	Morbi Road Octroi Naka	Traffic Junction (Only for Surveillance)				1		
79	Trikon Baug City	City Bus Stop	2	1				
80	Malaviya College	City Bus Stop	2	1				
81	GreenLand Chowkdi	City Bus Stop	2	1				
82	Sorathiya wadi	City Bus Stop	2	1				
83	Gondal Chowkdi	City Bus Stop	2	1				
84	Madhapar Chowkdi	City Bus Stop	4		1			
85	S T Bus Depot	S T Bus Depot	12	2				
86	Junction	Railway Station	4	2				
87	Bhaktinagar	Railway Station	4	2				
88	Commissioner Office	Government Building	4	3				
89	DIG Office Rajkot Range	Government Building	4	3				
90	DIG Office Arm Unit	Government Building	4	3				

91	Police HQ Building	Government Building	4	3				
92	Collector Office	Government Building	4	3				
93	R.M.C Rajkot	Government Building	4	3				
94	Bahumali Bhavan	Government Building	4	3				
95	Old Collector Office	Government Building	4	3				
96	Dist. Court	Government Building	4	3				
97	R & B Rajkot	Government Building	4	3				
98	A.G.Office	Government Building	4	3				
99	Income Tax Office	Government Building	4	3				
100	FSL	Government Building	4	3				
101	Race Course	Garden	10	2				
102	Aji Dam	Garden	10	2	1			
103	Nyari Dam	Garden	10	2				
104	Iswariya	Garden	10	2				
105	Praduman Park	Garden	10	2				
106	Jubilee	Garden	10	2				
107	Sorathiyawadi	Garden	10	2				
108	Jilla Garden	Garden	10	2				
109	University Garden	Garden	10	2				
110	Ruda Opp Bishap House	Garden	10	2				
111	Indira Bridge	Bridge	8	2				
112	Santkabir Under Bridge	Bridge	8	2				
113	Bhagavatipara	Bridge	8	2				
114	Popatpara Nala	Bridge	8	2				
115	Mahilla College	Bridge	8	2				
116	Morbi ByPass	Bridge	8	2				

117	Sandhiya Pool	Bridge	8	2				
118	Rainagar	Bridge	8	2				
119	Keshri Hind	Bridge	8	2				
120	Kishanpara - Amrapali	Bridge	8	2				
121	Civil Hospital	Hospital	8	4				
122	Zanana Hospital	Hospital	8	4				
123	Gundawadi Hospital	Hospital	8	4				
124	A Division	Police Station						
125	B Division	Police Station						
126	Pradumannagar	Police Station						
127	Mahila	Police Station						
128	Bhaktinagar	Police Station						
129	Thorala	Police Station						
130	Ajidam	Police Station						
131	Kuvadva	Police Station						
132	Gandhigram	Police Station						
133	University	Police Station						
134	Malaviyanagar	Police Station						
135	Rajkot Taluka	Police Station						
136	ACP East B-Division	ACP Office						
137	ACP West	ACP Office						
138	ACP Traffic	ACP Office						
139	ACP H.Q.	ACP Office						
140	Reserve Police Inspector PHQ	RPI Office						
141	M T Section	PSI MT Office						
142	P I Wireless	Wireless Office						

143	RTO	RTO Office			1			
144	Raiya Smasan	Entry Exit	4					
145	Shantinagar Chokadi (Raiya Dhar)	Sensitive	4					
146	J K Chowk	Sensitive	4					
147	Azad Chowk	Sensitive		1				
148	Sadguru (RMC Point)	Sensitive		1				
149	Kanaiya Chowk	Sensitive		1				
150	Chamadiay Chowky	Sensitive		1				
151	Sadar Bazar	Sensitive	4	1				
152	Bhistiwad Chowk	Sensitive		1				
153	Asikana Masjid	Sensitive		1				
154	Parsananagar-6	Sensitive		1				
155	Walmiki Wadi Chokadi	Entry Exit			1			
156	Ghanteswar	Entry Exit			1			
157	Sukhsagar Hall	Sensitive		1				
158	Huseni Masjid	Sensitive		1				
159	Faruki Masjid	Sensitive		1				
160	Sagar Chowk	Sensitive		1				
161	Aji GIDC Matel Chowk	Sensitive		1				
162	Next to Matel T point	Sensitive		1				
163	Tariya Steel near Jungleswar Bridge	Sensitive		1				
164	Huseni Chowk	Sensitive		1				
165	Ahir Chowk	Sensitive		1				
166	Devpara Chowk	Sensitive		1				

167	Atika Railway Crossing	Sensitive		1				
168	Dhebar road last rly crossing	Sensitive		1				
169	Praduman Green Ruda-1	Sensitive		1				
170	Rainagar	Sensitive		1				
171	Ronaki Chokadi	Entry Exit			1			
172	Aji Dam Chokadi		4	1				
TOTAL			542	219	27	5	112	56

Annexure B
List of Locations for Wi-Fi Hotspot

Sr. No.	Locations Name
1	Bhaktinagar Circle
2	Sorathiyawadi Garden
3	Bishop House – Prem mandir
4	Bhagwatsinh Garden
5	Astron Chowk Garden
6	Parul Garden East Zone
7	Zoo
8	Nyari Dam Site
9	Sharda Baug
10	Garden opp. Sheth High school
11	RMC East Zone, Central Zone and West Zone Office
12	Aji Dam Garden
13	Nana Mava Stadium

Annexure C
List of locations for LED Display Board/Panels

Sr. No.	Type of Location	Locations Name	Quantity
1	Road/Junction	Mahila College Chowk	1
2	Road/Junction	Kishanpara Chowk	1
3	Road/Junction	Jilla Panchyat Chowk	1
4	Road/Junction	Hospital Chowk	1
5	Road/Junction	Bahumali Bhavan Chowk	1
6	Road/Junction	Bhaktinagar Circle	1
7	Road/Junction	Gondal Chowkdi	1
8	Road/Junction	Nr Crytal Mall, Nr Water Tank, Kalawad Road	1
9	Road/Junction	Zaddus Corner, Kalavawad Road	1
10	Road/Junction	Parevdi chowk	1
11	Road/Junction	Amul Circle	1
12	Road/Junction	Kotecha Chowk	1
13	Road/Junction	Raiya Chokdi, BRTS Bus Station	2
14	Road/Junction	Raiya Telephone Exchange, BRTS Road	2
15	Road/Junction	Indira Circle , BRTS Road	2
16	Road/Junction	KKV Hall , BRTS Road	2
17	Road/Junction	Big Bazar Chowck, BRTS Road	2
18	Road/Junction	Nana mava Chowk , BRTS Road	2
19	Road/Junction	Mavdi Chowk, BRTS Road	2
20	Road/Junction	Umiya Chowk, BRTS Road	2
21	Road/Junction	Goverdhan chowk, BRTS Road	2
22	Road/Junction	Ambedkar Chowk, BRTS Road	2
23	Road/Junction	Punit Nagar Chowk , BRTS Road	2

Annexure D

List of locations for IOT Sensors

Sr. No.	Locations Name
1	Racecourse Junction
2	BRTS West Zone Bus Station
3	Ruda Nagar -2, University Road
4	Housing Board, Amin Marg
5	Lal Bahadur Shashtri Udhyan
6	Narayan Nagar Garden oppo. Satya sai hospital
7	Garden Near WZ Office
8	R.K Nagar nr. Municipal Commissioner Bunglow
9	Jubilee Garden
10	Malaviya Nagar/ Krishna Nagar
11	Airport Road Garden
12	Bhakta kavi Narshinh Mehta Udhyan, Nr. Aradhna Society
13	Balmukund Society Nr, Raiya Road



**Annexure – E:
MANUFACTURER’S AUTHORIZATION FORMAT**

(To be executed on OEM Letter Head by OEM of mentioned items.)

OEM Ref No: -

Dated:- XXXX

To,
The Rajkot Municipal Commissioner
Rajkot Municipal Corporation (RMC)
Rajkot.

Subject: - Authorization to System Integrator for supply & support.

Tender Name: -E - TENDER (No: GIPL/RMC-SmartCity-ICT/16-17/32) issued for “Selection of Implementation Agency for Supply, Installation, Commissioning, Operation & Maintenance of City-wide Surveillance and Wi-Fi Infrastructure at Rajkot City, Gujarat (RAJKOT EYE – WAY PROJECT)”.

Dear Sir,

This is with reference to referenced tender & subject. We certify that (Bidder Name), having their registered office at (Bidder Address) is an authorized partner to bid against your tender enquiry referred above on behalf of us.

We certify that (Bidder Name), we have service centre in India since _____ (Address proof required). Also we certify that we shall not be blacklisted / banned / disqualified / declared ineligible / declared having dissatisfactory performance by any government / quasi-government authority in India for supply of materials / carrying out operations and maintenance work.

All the proposed equipment should not be declared “End-of-Support” by the OEMs for next 7 years and should not be declared “End-of-life” for next two years from the date of bid submission.

Thanking you,
(Seal & Stamp with Date)

Annexure – F: List of Spares to be maintained during Contract Period

Sr. No	Item	Quantity
1	RLVD Camera	2% of each type of Installed cameras or 3 no of each type of installed camera whichever is more
2	ANPR Camera	
3	360° camera	
4	180° camera	
5	IP Camera Type B	
6	IP Camera Type C: PTZ	
7	Wi-Fi Access Points	4% of the Installed Wi-Fi Access Points
8	All type of IOT based Environmental Censors	4% of the Installed Censors (maximum 5)
9	UPS/DC SMPS	2% of the total installed UPS
10	Video Wall Cube	2 piece
11	Junction switches	2% of the total Junction switches

SECTION:8

Technical Specifications

Bidder shall ensure that the goods and services supplied under this project shall fully compliance to all the technical specifications as mentioned below.

1) Online UPS for CCC & DC

S/N	Parameter	Minimum Specification
1	Output Power Capacity	20KVA
2	Technology	True On-line High-Frequency Design UPS with Double Conversion technology, Rectifier & Inverter both to be IGBT based PWM
3	Certifications	ISO 9001:2000 and 14001 Certified OEM (certificate to be submitted) UPS should meet CE and ROHS standards (Compliance to be submitted)
4	Input Voltage Range	160-280 VAC @ 100% load, Three Phase
5	Input Freq. Range	50Hz +/- 3 (auto sensing)
6	Input Power Factor	0.99 (100% Load)
7	Input Protection	Thermal Circuit Breaker
8	Output Voltage	220/230/240 VAC +/- 1%
9	Output Frequency	50Hz ± 0.5Hz
10	Output Waveform	Pure Sinewave
11	O/P Voltage Distortion	<3% for Linear, <6% for Non-Linear Load
12	Output Connections	Output Connections: (1) Hard Wire 3-wire (H N + G)
13	Efficiency (Overall)	>90%
14	Efficiency (Inverter)	> 90%
15	Battery Type	SMF-VRLA (Sealed maintenance free valve regulated lead acid)
16	Battery Make	Exide, Quanta, Panasonic, CSB, Yuasa, Relicell
17	Battery Backup	120min backup on Full Load
18	Communication	Full-Functional SNMP Card should be present; RS 232 & USB port with software for UPS status monitoring
19	Protection	Inherent protection should be provided for Output Short-circuit and Overload, Input Fault, Cold Start, Low battery, Battery Over and Under charge, Battery Disconnect, Battery self-test feature, Over Temperature, OVCD, External Transient Voltage Surge Suppressor, etc.
20	LCD Display	Input Voltage, Input Frequency, Output voltage, Output Current, Output Frequency, Battery Voltage, UPS Status, Load Level, Battery Level, Discharge Timer, Battery Disconnect and Fault Conditions
21	By Pass	Manual and Automatic (Built-in) Bypass switch should be provided
22	Environment	Noise Level – less than 60 dB at a distance of 1 meter
23	Programmable Outlets	UPS should have programmable outlets for control of load segment

24	Operating Temperature	0-45° C
25	Relative Humidity	20-90%RH @0-400 C (Non-condensing)
26	Miscellaneous	ECO Mode Operation with Enable/Disable function
		Cooling: Forces Air Cooling
		Emergency Power Off (EPO)
		BYPASS Mode Operation with Enable/Disable function
		Cables: With all necessary cables and plug and Battery links
		Rack: Suitable Metallic Rack for housing of SMF Batteries to be provided
27	Battery Replacement	The successful bidder has to replace the UPS battery every 2 years for uninterrupted and smooth operations. OEM should confirm battery replacement in UPS at the end of 2nd year and 4th year respectively.

2) Fire Alarm system

S/N	Specification
1)	Shall be a microprocessor based single loop addressable fire detection and alarm system
2)	Must be implemented as per NFPA 72 guidelines
3)	Shall activate the system by automatic Heat and smoke detectors
4)	Shall have break glass units
5)	Shall be UL/EN54 Part 2 and UL/EN54 Part 4 compliant
6)	The system status shall be made available via panel mounted LEDs and a backlit 8 line x 40-character alphanumeric liquid crystal display
7)	All system controls and programming will be accessed via an alphanumeric keypad. The control panel will incorporate form fill menu driven fields for data entry and retrieval
8)	The system should have an option of manual over ride of the call, if required, after verification.
9)	The manual control should consist of: <ul style="list-style-type: none"> • Start sounders • Silence sounders • Reset system • Cancel fault buzzer • Display test • Delay sounder operation • Verify fire condition • Disable loop
10)	Smoke detector should be UL/EN54 part 7 compliant
11)	Heat detector should be UL/EN54 part 5 compliant
12)	Heat detector shall be of the fixed temperature (58° C) or rate of temperature rise type with a fixed temperature operating point.
13)	Control & Monitor module must be provided for integration with 3 rd party systems.
14)	Alarms:

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

3) Junction Box, with adjustable mounting frames

S/N	Parameter	Specification
1	Built	The Outdoor Utility Cabinet will be constructed with a front sheet steel door with 3-point Locking system to ensure the security of the cabinet. Side and Wall Panels shall be double wall constructed, with fixing bolts internal to the cabinet. The Cabinet should have the required frames to mount the required components like, network device, power, UPS, LIU, battery, etc.
2	Utility & IP rating	Should be Made for 24/7/365 Outdoor Applications; The Utility Cabinet shall be IP 67 or better rated. Junction Box design should ensure to keep the temperature within suitable operating range for equipment's and should also avoid intentional water splash and dust intake.
3	Size	The cabinet has to be provided of size suitable for the mounting of the associated network devices, power, UPS and Battery components securely and safely within the cabinet.
4	Power Slot	Minimum 3 x PDU's has to be provided to support the site equipment. PDU type should be as per actual requirement as per Indian standards.
5	Installation	Each Cabinet will be mounted on a raised height Plinth, 600 - 1000 mm high, as per site requirements. FAN Cooling unit shall be inherent in the design.
6	Cable Management	Proper cable management should be provided
		Cable Routing: Power connection cable shall be provided from the nearest access point provided by Power utility company to the Outdoor Utility Cabinet through Power meter enclosure.

4) UPS at Junctions

Item	Minimum Requirement Description
Capacity	1 KVA
Input Range	Voltage Range 155-280 V on Full Load Voltage Range 110-280 V on Less than 70% Load Frequency 50 HZ \pm 3 HZ
Output Voltage & Waveform	220V AC/ 230V AC/ 240V AC
I/P & O/P Power Factor	0.9 or higher power factor
Mains & Battery	Sealed Lead Maintenance Free VRLA type (Lead Calcium SMF batteries NOT acceptable), Mains & Battery with necessary indicators, alarms and protection with proper battery storage stand
Frequency	50 Hz \pm 0.5% (free running), Pure Sine wave
Crest Factor	min. 3:1
Third Harmonic Distribution	< 3%

Input Harmonic Level	< 10%
Overall Efficiency	Min. 90%
Noise Level	< 55 db @ 1 Meter
Backup	2 hours
Certification	ISO 9001:2008 & ISO 14001 certified
Protection	To be provided for overload/ short circuit; overheating; input over/under voltage; output over/ under voltage.
Alarms & Indications	All necessary alarms & indications essential for performance monitoring of UPS like mains fail, low battery & fault detection
Interface	SNMP interface support (for remote monitoring)
Compatibility	UPS to be compatible with DG Set supply and mains supply
Bypass	Automatic Bypass Switch
Technology	True ON-LINE (Double Conversion) with IGBT based inverter and PWM Technology
Support	The system should not be an end of life / end of service product.
Operating Temperature	0 to 50 Degrees Centigrade

5) Poles including mounting/installation

S/N	Parameter	Minimum Required Specifications
1.	Pole type	Galvanized pole as per IS:2629 and Fabrication as per IS:2713
2.	Height	6 meter above ground surface; Bottom section: 1.4 meter; Middle Section: 1.4 meter; Top Section: 3.2 meter
3.	Foundation	Minimum 1 meter so as to ensure that video feed quality is not impacted due to winds in different climatic conditions and from vibration caused due to heavy vehicles on road
4.	Pole Diameter (Outer side)	Bottom section: 97.9mm; Middle Section: 76.2mm; Top Section: 65.2mm
5.	Bottom Base Plate	300mm x 300mm x 6mm
6.	Protection	Lightening arrestor and Earthing
7.	Cantilevers	The pole should support 3 number of cantilever of varying length from 0.5 to 2.0 meters. The cantilever should be fitted such that the can be rotated to change the direction or adjust the angle, if at all required. The Cantilever should be strong enough so as to mount 2 CCTV cameras', if required.
8.	Mounting Facility	CCTV camera on pole or cantilever, Junction Box

6) Video Wall Solution- 55" LED/DLP

S/N	Parameter	Minimum Required Specifications
1.	Configuration	Full HD IPS LED/DLP Display, Direct LED Backlight, Display suitable for use in video wall with bezel to bezel distance not more than 4 mm
2.	Screen Size	55" or higher in segments in 5x3 arrangement
3.	Resolution	Full High definition (1920 X 1080) 16:9 Widescreen
4.	Contrast Ratio	2000:1 or better
5.	Brightness	500 Cd/m ² or better
6.	Refresh Rate	>120 Hz
7.	Response Time	8 ms
8.	Viewing Angle	160 degrees or Higher
9.	Certifications	CE, FCC, UL/ETL
Interface		
10.	Standard Inputs	1x Digital DVI-I ; 1x Digital DVI-D, or Higher
11.	Standard Outputs	1x Digital DVI-D ; 1x CVBS BNC
12.	Control	RS-232/RS-422/IR
Power		
13.	Consumption	Not more than 4000 Watt
14.	Power Supply	AC 100 -240 V~ (+/-10 %), 50/60 Hz
General		
15.	Operating Temperature	0°C - 40°C
16.	Humidity	20% - 90%, non-condensing
Accessories		
17.	Cables	Dual Link DVI-D cable, power cable for daisy chain, AC cable, Remote Controller
18.	Display Controller	Video Distributor, Display controller to control Video wall in a matrix as per requirement with necessary software: Processor specs: Quad core 64-bit, 3.4 GHz CPU or latest RAM: 8 GB DDR3 minimum HDD: Min 500 GB Hard Disk (Hard disk Capacity should be upgradable) Network support: Gigabit Ethernet Controller inbuilt, Support for Add on Network adapters. Videowall Display: Display multiple source windows in any size, anywhere on the wall Accessories: DVD-R, DVD+RW, Keyboard, mouse OS Support: 64-bit Operating Systems Windows / Linux or equivalent industry standard

Video Wall Management Software		
19.	Display & Scaling	Display multiple sources anywhere on display up to any size
20.	Input Management	All input sources can be displayed on the video wall in freely resizable and movable windows
21.	Scenarios Management	Save and Load desktop layouts from Local or remote machines
22.	Layout Management	Support all Layout from Input Sources, Internet Explorer, Desktop and Remote Desktop Application
23.	Multi View Option	Multiple view of portions or regions of Desktop, Multiple Application Can view from single desktop
24.	Other features	<ul style="list-style-type: none"> • SMTP support • Remote Control over LAN • Alarm management • Remote management • Multiple concurrent client • KVM support
25.	Cube Management	<ul style="list-style-type: none"> • Cube Health Monitoring • Pop-Up Alert Service • Graphical User Interface

7) Workstations

Features	Specifications Required
Processor	Fourth Generation Intel Core™ i7 Processor
Chipset	Intel Z87 or higher
Motherboard	OEM Motherboard
RAM	Minimum 4 GB Memory
Graphic s card	Graphics card with 1 GB video memory (non-shared)
HDD	320 GB SATA Hard drive @7200 rpm
Media Drive	NO CD / DVD Drive
Network interface	1000BaseT, Gigabit Ethernet
Audio	Line/Mic IN, Line-out/Speaker Out (3.5 mm)
USB Ports	Minimum 6 USB ports (out of that 2 in front)
Keyboard	104 keys minimum OEM keyboard
Mouse	2 button optical scroll mouse (USB)
PTZ Joystick Controller	• PTZ speed dome control for IP cameras
	• Minimum 10 programmable buttons
	• Multi-camera operations
Monitor	22" TFT LCD monitor, Minimum 1920 x1080 resolution, 5 MS or better response time, TCO 03 (or higher) certified
	For command Control Centers : 3 LCD Monitors, For Viewing centers : 1 LCD Monitor
Operating System	64 bit pre- loaded OS Windows 7 OR Latest with recovery disc

Antivirus Feature	Advanced antivirus, antispyware, desktop firewall, intrusion prevention (comprising of a single, deployable agent) which can be managed by a central server. (Support, updates, patches and errata for the entire contract/ project period)
-------------------	---

8) 24 port L2 switch

Specifications Required
General Requirements: Switch should be rack mountable
Switch should have non-blocking architecture
Switch should have total 16 nos. of 10/100/1000 BaseT Interfaces with additional 4xGigabit uplink ports
Switch Should offer option for Redundant Power Supply (RPS) if required
Switch should support Auto MDI/MDIX and stacking feature with required Stack cables
Switch should support TOR for detecting cable breaks and shorts
Performance Requirements ; Switch should have minimum 80Gbps Data switching capacity
Switch should have minimum 60 MBPS L2 throughput
Layer-2 Requirements
Switch should support minimum 10000 MAC address
Switch should support Jumbo Frames & minimum 1000 VLANs
Switch should support 802.lq VLAN tagging & Voice VLAN
Switch should support link aggregation for minimum 4 ports
Security Requirements
Should support Access control lists to provide L2 to L4 traffic filtering for IPv4 and 1Pv6 Packets by offering Standard ACL, Extended ACL, VLAN ACL, Port based ACL, and Time based ACL
Should support MAC, 802.lx and Web based authentication, with multiple authentication method and concurrent authentication session per port minimum for 80 Users per port
Should support Full Network Access Control features to push Dynamic VLAN and Port based profile to the user ports based on the AAA, LDAP, AD, Radius server authenticated response
Should support Guest VLAN, and should restrict access to specific users or devices based on MAC address learned or statically defined
Should support BPDU port protection, Root Guard, DHCP ARP protection, IP Source Guard, and Unicast Reverse Path Forwarding URPF features
Supports DoS-DDoS protection, Storm Control
QoS Requirements
Support IGMPv1,v2, and v3, PIM-SM / OM, PIM-SSM, Multicast Source Discovery Protocol, Multicast VLAN
Support congestion control mechanism
Management Requirements
Should support encrypted communication between the user accessing the device namely using all access methods CU, GUI, or NMS via features like SSHv2, SSL, and SNMPv3 and Secure FTP/TFTP etc.
Should support features like CDP, LLDP, LLDP-MED
Link activity port transmission speed, port duplex mode, power, link OK, system etc.

Should support Debugging via cli via console, telnet, ssh
Switch should traffic mirroring (port, VLAN)
ACL-based mirroring
IP Tools (e.g. extended ping, extended Trace)

9) Access Control System

S/N	Specification	
Biometric Finger Scan Reader		
1.	Transmission Frequency: 13.56 MHz	
2.	iClass/Mifare Technology.	
3.	The data flow between card & Reader should be encrypted using 64 bit authentication keys.	
4.	Should be configured as a Reader – Enroller, Enroller Only & Reader Only (All three are mandatory)	
5.	Optical Finger print sensor	
6.	Sensor resolution should be of at least 500dpi	
7.	Finger print should be captured in less than 2 seconds and verified in less than 5 seconds.	
8.	Should have fingerprint enrollment software	
9.	Operating temperature: 0° to 45°C	
10.	Operating humidity: 10% to 90% relative humidity (Non-Condensing)	
Smart card Reader		
11.	Transmission Frequency: 13.56 MHz	
Controller		
12.	Reader Inputs	Two
13.	Universal Inputs	Two
14.	Tamper Input	One
15.	Digital Lock Inputs	Two
16.	Processor	50 MHz with 32 MB RAM
17.	Processor For Reader Inputs	Yes (Combined/Dedicated Processor)
18.	Communication	10/100 Ethernet Port
19.	Memory	Minimum 500 personnel Records
20.	Area Lockdown Support	Yes
21.	Real Time Clock	Yes
22.	Encryption	64 bit
23.	Visual Indicator	Yes
24.	Mounting	Wall / Ceiling Mount
25.	Battery Backup	5 hours or more
26.	Technology Compatibility	Wiegand

27.	Card Reader Power	5V DC
28.	Wiring Distance	150 meters (Wiegand)
29.	Indicator LED	Yes
30.	Push Button Switches	Yes (For clearing the memory & Resetting the IP Address)
31.	Enclosure	Yes
32.	Certifications	CE Approved
33.	Operating Temperature	0° to 45°C
34.	Operating Humidity	10% to 80% relative humidity (Non-Condensing)
Access Control Software		
35.	Compatibility with any Windows Operating System	
36.	Compatibility with MYSQL / SQL / ORACLE	
37.	Support for TCP/IP Communication	
38.	Provision for Alarm Monitoring for Battery, Mains Supply, Door Opened too Long, Door Forced Opened, Unauthorized Swipe & Controller Tampering	
39.	Support for unlimited number of Card Database & Transactions	
40.	Specify Card Activation & Expiry Date	
41.	Support for Biometric, Pin & Smart Card Applications	
42.	Management of Dual Access Levels to a single Card	
43.	Remote Locking & Unlocking of Doors	
44.	Remote management of Controllers	
45.	Customization of Door User time for every card Holder	
46.	One Client License	
47.	Two Stages of Alarm Management (Acknowledgement on Receipt & Closure on Investigation)	
48.	Access Privileges on the basis of Time & Date	
49.	Creation of holiday schedules to cover maintenance & Vacations / Holidays	
50.	Permission to activate any control output for a specific event such as alarm	
51.	Programmable Shunt time to control the door opening time	
52.	Area Control by using Hard Anti Pass back, Soft Anti Pass back, Timed Anti Pass back, Occupancy Limit, Multi man principle, Area Lock down, Threat level conditioning.	
53.	Alarm Management	
54.	Automatic User Log off	
55.	Cardholder Management & Enrollment	
56.	Creation & Maintenance of User Database	
57.	Assignment of Access Privileges	

10) CCC Core Router

S/N	Specification
1.	Router should have redundant controller cards and should support stateful switch over Nonstop Forwarding and Nonstop Routing
2.	In case of failure of any single route processor, none of the line card traffic should be impacted
3.	Router should support capacity of minimum 20 GBPS
4.	Router should support 4000 MAC addresses or more
5.	Router should support Redundant Power supply and should also support on line Insertion and removal of the same from day one
6.	Router must support TCP/IP, PPP, Frame Relay, HDLC
7.	Router should support IPv4 and IPv6 From day one
8.	Router should support all standard routing protocols like BGP, MBGP, OSPF v2/v3, IS-IS RIP/RIPv2, static routes, MPLS (L2 & L3), PIM (v1, v2), IGMP (v1, v2, v3) IPv6 tunneling NAT, NTP, etc.
9.	Router should support High Availability (VRRP, or other Proprietary protocol, etc.
10.	Router should support QoS (DSCP, CoS), marking, classification and policing
11.	Router should support traffic Engineering & MPLS-TE with FRR
12.	Router should have dedicated OOB Management port using CLI(SSH), WebUI (SSL), SNMP (v1,v2,v3)fttp etc.
13.	Router should support AAA features using TACACS+ Radius, LDAP, etc.
14.	Router should be NDPP or EAL3 certified at the time of bidding
15.	Router should be supplied with at least 6x10G Interface scalable to additional 2x10G
16.	Router should have redundant hot-swappable power supply support for a fully loaded chassis
17.	Router should be supplied with Indian standard power cable
18.	Router should be supplied with all licenses from day one

11) Internet Router

S/N	Specification
1.	Router should have redundant controller cards and should support stateful switch over, Nonstop forwarding and Nonstop routing.
2.	In case of failure of any single route processor, none of the line card traffic should be impacted.
3.	Router should support capacity of minimum 10 Gbps.
4.	Router should support 4000 MAC addresses or more.
5.	Router should support Redundant Power Supply and should also support On line insertion and removal of the same from day one.
6.	Router must support TCP/IP, PPP, Frame Relay, HDLC
7.	Router should support IPv4 and IPv6 from day one
8.	Router should support all standard routing protocols like BGP, MBGP, OSPF v2/v3, IS-IS, RIP/RIPv2, static routes, MPLS (L2 & L3), PIM(v1, v2), IGMP(v1, v2, v3), Ipv6 tunneling, NAT, NTP, etc.
9.	Router should support High Availability (VRRP, or other proprietary protocol, etc.)

10.	Router should support QoS (DSCP, CoS), marking, classification and Policing
11.	Router should support Traffic Engineering & MPLS-TE with FRR
12.	Router should have a dedicated OOB Management port using CLI(SSH), WebUI(SSL), SNMP (v1, v2, v3), TFTP, etc.
13.	Router should support AAA features using TACACS+, Radius, LDAP, etc.
14.	Router should be NDPP or EAL3 certified at the time of bidding
15.	Router should be supplied with at least 9x1G interface with scalability to additional 6x1G interfaces
16.	Router should have redundant, hot-swappable power supply support for a fully loaded chassis
17.	The Router should be supplied with Indian Standard power cables.
18.	The Router should be supplied with all applicable Licenses from day one.

12) CCC Switch

Sr. No.	System Description & Minimum Requirement
1	<u>Architecture</u>
2	(1) Must have minimum of 08 Modular Slots and Two slot for Supervisor cards. After inserting the IO Modules for the necessary configuration at least 02 slots should be free. If the Bidder has IO Module configuration which consumes more slot bidder should offer chassis with a higher configuration. Switch Fabric Slots should be different.
3	(2) Switch should have distributed switching architecture with passive backplane. Shall have CLOS Architecture or equivalent shared switch fabric capability with minimum four switch fabrics all supporting active switching to support high switching capacity. The switch should support OpenFlow specifications to enable SDN by allowing separation of the data (packet forwarding) and control (routing decision) paths
4	(3) Switch should support more than 3Tbps switching capacity or greater.
5	(4) Switch should have a switching throughput which should be at least 2 Mpps or higher
6	(5) In line with the Blade Sizing the minimum Bandwidth available per slot should be such that it creates a non-blocking architecture ensuring that all devices connected to that blade gets 100% bidirectional through put in line with the maximum port capacity of the card. OEM/SI to attach the Switch fabric calculation with the same. Currently the SI should offer the switch fabric which can cater at least 64 X 40G Ports; 384 X 10G Ports and 384 X 1G Ports to start with. The Switch Fabric should be N+1 Configured ensuring that failure of any Fabric does not impact the overall performance of the Switch.

7	(6) Switch hardware should be ready to support 40 & 100GE I/O modules. By upgrading the S/w and necessary Switch Fabric the switching capacity should be incremented to support 40 & 100G modules in a non-blocking architecture mode. No chassis would be changed at that point of time. The Same Supervisory Modules; Power supply etc. would be used. OEM/SI to give specific compliance for the same.
8	(7) Switch should have suitable Visual Indicators for diagnostics and healthy / unhealthy status of Ports & modules.
9	(8) No Ports or service modules should be populated on Switching Fabric/Management Module
10	(9) Switch should support IPv4 and IPv6
11	(10) All the interface modules should be hot swappable, therefore, no downtime / reboot should be required for addition / removal / change of any of the interface modules.
12	(11) Switch should support link aggregation across multiple switches in a cluster so as to be considered as single virtual link on switch cluster from access/distribution.
13	(12) Switch should support clustering of at least two switches to work as a single entity for access/distribution switches. Both switches should work in active-active for all the VLAN traffic.
14	(13) Two switches when working as a switch cluster as mentioned above should use their own control and data plane. No sharing of control or data plane should happen.
15	(14) There should not be any slot dependency for I/O modules. All kind of I/O modules can go in any of available payload slots
16	<u>Redundancy</u>
17	(1) Must have Redundancy Power Supply Units (PSUs). And preferable these should be Internal redundant power supplies. If Internal redundant Power supplies are not available then the bidder should specifically offer redundancy and should give the technical note on the same.
18	(2) Must have redundant of other components such as fans within network equipment.
19	(3) Redundant CPU cards must support stateful switchover, ensuring synchronization to allow the standby CPU to immediately take over in sub-second time scales in the event of a failure. This is vitally important with the types of broadcast critical applications that may be running over the infrastructure to ensure that services are unaffected.
20	(4) All components (including elements such as I/O cards, CPUs, power supplies and fans) must be hot swappable with zero disruption to traffic forwarding (Unicast or multicast).

21	<u>Resiliency</u>
22	(1) Shall have the capability to extend the control plane across multiple active switches using any Industry standard Protocols making it a virtual switching fabric that will enable interconnected switches to perform as single Layer-2 switch and Layer-3 router
23	(2) Should support IEEE 802.1D Spanning Tree Protocol, IEEE 802.1w Rapid Spanning Tree Protocol and IEEE 802.1s Multiple Spanning Tree Protocol
24	(3) IEEE 802.3ad Link Aggregation Control Protocol (LACP)
25	(4) Ring protocol support to provide sub-100 ms recovery for ring Ethernet-based topology
26	(5) Virtual Router Redundancy Protocol (VRRP) to allow a group of routers to dynamically back each other up to create highly available routed environments
27	(6) Graceful restart for OSPF, IS-IS and BGP protocols
28	(7) Bidirectional Forwarding Detection (BFD) for OSPF, IS-IS and BGP protocols
29	<u>Required Port Densities</u>
30	(OEM/SI needs to plan the blades in such a way that required minimum port densities should be available in a single blade and after the consumption of slots for the same minimum of 02 Slots should be available free)
31	(1) Switch should have minimum 60 numbers of 40G QSFP+ ports.
32	(2) Switch should have minimum 50 numbers of 10G ports with SFP+/XFP ports. In case of XFP interface OEM to confirm that the same is compatibility with SFP+ at the other end.
33	(3) Switch should support the following 1000Base Transceivers as mentioned below
34	(i) SX transceiver module for Multimode Fiber for supporting a maximum distance of 550 mtrs
35	(ii) LX/BX transceiver module for Single Fiber for supporting a maximum distance of 10Kms
36	(4) Switch should support the following 10G Base Transceivers as mentioned below
37	(i) SR transceiver module for Multimode Fiber for supporting a maximum distance of 550 mtrs on OM3 and OM4
38	(ii) LR transceiver module for Single mode fiber for supporting a maximum distance 10 Kms
39	(iii) ER/EW transceiver module for Single mode fiber for supporting a maximum distance 40 Kms SPF+ Cables for Direct Connectivity on UTP should also be available

40	(5) Switch should support the following 40G Base Transceivers as mentioned below
41	(i) SR4 transceiver module for Multimode Fiber for supporting a maximum distance of 550 mtrs on OM3 and OM4
42	(ii) LR4 transceiver module for Single mode fiber for supporting a maximum distance 10 Kms
43	(iii) ER/EW transceiver module for Single mode fiber for supporting a maximum distance 40 Kms SPF+ Cables for Direct Connectivity on UTP should also be available
44	(6) Switch should support the following 100G Base Transceivers as mentioned below
45	(i) 100G- SR4 transceiver module for Multimode Fiber for supporting a maximum distance of 550 mtrs on OM3 and OM4
46	(ii) 100-G LR4 transceiver module for Single mode fiber for supporting a maximum distance 10 Kms
47	(iii) 100-G ER4 transceiver module for Single mode fiber for supporting a maximum distance 40 Kms
48	Maximum Port Densities supported
49	Minimum 16 ports of 100 Gig ports to be supported
50	Minimum 32 ports of 40 Gig ports to be supported
51	Minimum 192 ports of 10 Gig ports to be supported
52	Minimum 192 ports of 10 / 100 / 1000 base-T to be supported
53	<u>Layer 2 features</u>
54	IEEE 802.1Q VLAN tagging.
55	802. 1Q VLAN on all ports with support for minimum 3500 VLANs.
56	Support for minimum 400 k MAC addresses
57	Spanning Tree Protocol as per IEEE 802.1d
58	Multiple Spanning-Tree Protocol as per IEEE 802.1s
59	Rapid Spanning-Tree Protocol as per IEEE 802.1w
60	Self-learning of unicast & multicast MAC addresses and associated VLANs
61	Jumbo frames up to 9000 bytes
62	Link Aggregation Control Protocol (LACP) as per IEEE 802.3ad.
63	Minimum 128 Multi-link Trunks with 08 links per multi-link group.
64	"Port Mirroring" functionality for measurements using a network analyzer for up to 32 ports.
65	Broadcast, Multicast and Unicast storm control on per port basis to prevent degradation of overall system performance occurred due to faulty end stations.

66	Switch hardware should support IEEE 802.1ah MAC-in-MAC encapsulation or IEEE 802.1ad Qin Q.
67	Should support Ethernet (IEEE 802.3, 10BASE-T)
68	Should support Fast Ethernet (IEEE 802.3u, 100BASE-TX)
69	Must support Gigabit Ethernet (IEEE 802.3z, 802.3ab)
70	Must support Ten Gigabit Ethernet (IEEE 802.3ae)
71	Software based standards for Network Device
72	Must support IEEE 802.1d - Spanning-Tree Protocol
73	Should support IEEE 802.1s - Multiple Spanning Tree Protocol
74	Must support IEEE 802.1q - VLAN encapsulation
75	Should support IEEE 802.3x Flow Control
76	Must support auto-sensing and auto-negotiation (Link Speed/Duplex)
77	<u>Layer 3 features</u>
78	Inter-VLAN IP routing for full layer 3 routing between two or more VLANs.
79	IP unicast routing protocols (static, RIPv2, OSPF, BGP).
80	Support for IPv6 routing in future like Static, OSPFv3, , BGP+
81	Virtual Router Redundancy Protocol (VRRP) as per RFC 3768 or equivalent.
82	VRF/VRF-lite virtualization feature
83	PIM-SM multicast routing protocol
84	Minimum 1000 IP interfaces.
85	Minimum 2000 IP multicast streams and 500 active PIM interfaces.
86	Minimum 500k IP forwarding table entries.
87	OSPF Instances: up to 50
88	OSPF Adjacencies: up to 200
89	OSPF Routes: up to 64k
90	RIP Instances: up to 64
91	RIP Routes: up to 05k
92	BGP Peers: up to 50
93	BGP Routes: up to 128k
94	VRF instances : up to 512
95	PIM Active Interfaces: up to 512
96	Should support policy based routing with Flow-based Polices: up to 06k
97	Switch should support IGMP v1/v2/v3 as well as IGMP v1/v2/v3 snooping.
98	Switch hardware should support IEEE 802.1aq standard of shortest path bridging or IETF TRILL. Virtualization feature should be supported using SPB or MPLS or any other protocol. OEM/SI to give detailed noting on how virtualization is possible in the offered product.
99	Must support Static IP routing
100	Must support Open Shortest Path First (OSPF) v2 (RFC 2328)

101	Should support Intermediate system to intermediate system - IS-IS (RFC 1195)
102	Must support Border Gateway Protocol - BGPv4 (RFC 1771)
103	Should support Multi-Protocol Border Gateway Protocol - MP-BGP (RFC 2858)
104	Should support BGP Route Flap Damping (RFC 2439)
105	Should support Policy Based Routing
106	Should support Graceful Restart for OSPF (RFC 3623) / OSPFv3 (RFC 5187)
107	Should support Graceful Restart for IS-IS (RFC 3847 - Restart signaling for IS-IS)
108	Should support Graceful Restart for BGP (RFC 4724)
109	<u>Quality of Service (QoS) Features</u>
110	Must support IEEE 802.1p class-of-service (CoS) prioritization
111	Should have advanced per-port QoS features in both ingress and egress directions. Please specify what is possible for ingress and what is possible for egress.
112	Should be able to classify and mark traffic based on physical port, IP DA/SA, L4 information, IEEE 802.1Q/P COS, IP
113	Precedence (ToS), DSCP, MPLS exp bits switch should support DiffServ as per RFC 2474/2475
114	Must support a minimum of four levels of prioritization per port
115	Should have per-port queue management and congestion avoidance features (e.g. RED / WRED). Please specify features supported
116	Must support rate limiting (to configurable levels) based on source/destination IP/MAC, L4 TCP/UDP
117	Must have the ability to complete traffic shaping to configurable levels based on source/destination IP/MAC and Layer 4 (TCP/UDP) protocols
118	There should not be any impact to performance or data forwarding when QoS features
119	Must support a "Priority" queuing mechanism to guarantee delivery of highest-priority (broadcast critical/delay-sensitive traffic) packets ahead of all other traffic
120	Must support ability to trust the QoS markings received on an ingress port
121	<u>Security Features:</u>
122	Must support multiple privilege levels for remote access (e.g. console or telnet access)
123	Must support Remote Authentication Dial-In User Service (RADIUS) and/or Terminal Access Controller Access Control System Plus (TACACS+)

124	Must support AAA using RADIUS (RFC 2138 & 2139) and/or TACACS+, enabling centralized control of the device and the ability to restrict unauthorized users from altering the configuration
125	<u>Access Control features</u>
126	Should support Access Control Lists (layers 2-4) in hardware.
127	Should support both ingress and egress access control lists per port
128	Should support access list parameters for control based on source and/or destination IP, source and/or destination subnet, protocol type (IP/TCP/UDP etc.), source and/or destination port or any combination of these.
129	By enabling access lists, there should not be any impact on the router performance
130	Should be able to apply access control for SNMP/NTP access (to ensure SNMP access only to Network Management Systems)
131	Should support per-port broadcast, multicast and uni-cast storm control
132	The router should support MD5 authentication for OSPF, IS-IS and BGP.
133	DHCP Snooping to prevent Man in the Middle attacks
134	Switch should support MAC Address based Filters / Access Control Lists (ACLs) on all switch ports
135	Switch should support Port as well as VLAN based Filters / ACLs.
136	Secure Shell (SSH) Protocol, HTTP and DoS protection
137	IP Route Filtering, Anti-spoofing etc.
138	<u>Management Features</u>
139	Switch should have a console port with RS-232 Interface for configuration and diagnostic purposes.
140	Switch should be SNMP manageable with support for SNMP Version 1, 2 and 3.
141	Switch should support all the standard MIBs (MIB-I & II).
142	Switch should support TELNET and SSH Version-2 for Command Line Management.
143	Switch should support 4 groups of embedded RMON (history, statistics, alarm and events).
144	Switch should support System & Event logging functions as well as forwarding of these logs to up to ten separate syslog server for log management.
145	Switch should support on-line software reconfiguration to implement changes without rebooting. Any changes in the configuration of switches related to Layer-2 & 3 functions, VLAN, STP, Security, QoS should not require rebooting of the switch.

146	Switch should have comprehensive debugging features required for software & hardware fault diagnosis.
147	Switch should support Multiple privilege levels to provide different levels of access.
148	Switch should support NTP (Network Time Protocol) as per RFC 1305.
149	Switch should support FTP and TFTP.
150	Switch should have inbuilt element manager accessed via HTTP (Web GUI) or using external management software
151	Must support Network Timing Protocol (NTPv3) and should support the following:
152	• Configuration of more than one NTP server.
153	• Speciation of a local time zone.
154	• Configuring automatic time offset adjustment for daylight savings time.
155	• NTP authentication
156	Extensive debugging capabilities to assist in hardware/software problem resolution. At a minimum, debugging support should include:
157	• Detailed packet level debugging for troubleshooting purposes
158	• Detailed IGP/EGP (OSPF/IS-IS/BGP) for troubleshooting purposes
159	• Detailed Multicast debugging (e.g. IGMP/ PIM) for troubleshooting purposes
160	• QoS debugging for troubleshooting purposes
161	Debugging must not have an impact on performance or data forwarding capabilities of the device
162	It should be guaranteed that the network switch will not enter it's end of life cycle for a minimum of five years
163	The network switch should have a 5-10 year roadmap available covering the future of the equipment (this information should be attached)
164	It is desirable that the device has support for a XML or equivalent interface allowing for future querying, configuration and management options
165	Hardware modules should be simple to access for removal and replacement, allowing for replacement while ensuring continuous system operations and availability
166	Standards
167	RoHS Compliant
168	IEEE 802.3x full duplex on 10BASE-T and 100BASE-TX ports
169	IEEE 802.1D Spanning-Tree Protocol
170	IEEE 802.1p class-of-service (CoS) prioritization
171	IEEE 802.1Q VLAN
172	IEEE 802.3x be on 10 BaseTx / 100 Base Tx / 1000 Base Tx

173	10G Base-SR, 10G Base LR, 10G Base CX
174	IEEE 802.3u 10 BaseT / 100 Base Tx /1000 Base Tx
175	100G Base-SR, 100G Base LR, 100G Base CX
176	40G Base-SR, 40G Base LR, 40G Base CX
177	Switch should support 802.1Br Ethernet fabric for interoperability in future. This is the standard based protocol for interop
178	Switch should be able to integrate with third party SDN controller's like NSX , contrail and Openstack integration for orchestration
179	Should support BFD of min 100 per module. This is required for fast failover
180	Should support MPLS features -LDP, L3VPN, RSVP, VPLS FRR, Virtual routers.

13) Unified Threat Management

Specifications Required
General Requirements:
Should be rack mountable
Must be appliance based and should facilitate multi-application environment.
It should be modular based to accommodate future growth/ expansion
The Firewall should be ICSA Labs for ICSA 4.0 or equivalent certified
The platform should be based on real time, secure embedded operating system
The platform should use ASIC based architecture that is optimized for packet and application level content processing
The proposed system shall support unlimited IP/User license for Firewall / VPN (IPSec & SSL)/ IPS/WCF/AV
Should provide a Http, Https, SSH, Telnet, SNMP based management console for managing and configuring various components of the appliance
Should be IPv6 Ready
Networking & System Performance Requirements:
Should support minimum of 8 no of Gigabit interfaces with 10/100/1000 auto sensing capacity
Should support the standards based Link aggregation technology (IEEE 802.3ad) to achieve higher bandwidth.
Should support IEEE 802.1q VLAN Tagging with about 1024 VLANs supported (in NAT/Route mode)
Should support automatic ISP/link failover as well as ISP/link load sharing for outbound traffic
Should support Dynamic Routing Protocol for RIP1 & 2, OSPF, OSPFv3, BGP4, ISIS, RIPng etc.
Should support Static, Policy Based, and Multicast routing
Should support throughputs of 4.0 Gbps or better for both small & large packets
The firewall should support throughput of minimum 1 Gbps of AES - IPSEC VPN and should support H/W acceleration
should support concurrent session minimum 4,00,000

Should support new session per second minimum 15,000
Should support IPS throughput of 600 Mbps or better
Should support GAV throughput of up to 200 Mbps
Should support Site to Site VPN Tunnels up to 1000
Operating System & Management Requirements:
Should prevent inheriting common OS vulnerabilities
Should reside on either on flash disk or hard disk
Allow multiple OS firmware image for booting options
Should be upgradeable via Web UI or TFTP or equivalent mechanism
Should support easy backup or restore via GUI and CLI to/from local PC, remote centralized management or USB disk
Should support profile based login administration for gradual access control like only Policy Configuration, Log Data Access etc.
Should be able to limit remote management access from certain trusted network or host with corresponding administrator account
The proposed system should be able to facilitate administration audits by logging detailed activities to event log for management & configuration updates
The administrator authentication shall be facilitated by local database, PKI & remote services such as Radius, LDAP and TACAS+ with option of 2 Factor Authentication
The Firewall must be capable of clustering multiple firewalls together into a redundant and highly available stateful configuration for creating HA.
Firewall Requirements:
Should support deploy modes like "Stealth Mode" or "Route Mode" or "Transparent Mode" or "Proxy Mode"
Should support integrated Traffic Shaping / QoS functionality
Should support DHCP server & DHCP Agent functionality
Should support Stateful inspection with optional Policy based NAT (Static OR Dynamic)
Should support Inbound Port Forwarding with Load Balancing
Should support IPv6 ACL to implement security Policy for IPv6 traffic
All internet based applications should be supported for filtering like Telnet, FTP,SMTP, HTTP, DNS, ICMP, DHCP, RPC,SNMP, BGP, IMAP, NFS etc
Should be able to inspect HTTP and FTP traffic when these are deployed using nonstandard port(i.e. when HTTP is not using standard port TCP/80)
High Availability Requirements:
Must support Active-Active and Active-Passive redundancy.
Must support stateful clustering of multiple active firewalls, and load balance the traffic between them to share the load.

IPSEC VPN Requirements:

The IPSEC VPN and SSL VPN capability shall have ICSA or equivalent Certification

The proposed system shall comply/support industry standards, L2TP, PPTP, IPSEC, and SSL VPN with/without additional external solution, hardware or modules. All such components should be supplied if required externally

Should support hardware VPN acceleration (inbuilt is preferred)

IPSEC (DES, 3DES, AES) encryption/decryption

SSL encryption/decryption

The system shall support the following IPSEC VPN capabilities:

Multi-zone VPN supports

IPSec, ESP security

Supports Aggressive and Dynamic mode

Hardware accelerated encryption using IPSEC, DES, 3DES, AES

Support perfect forward secrecy group 1 and group 2 configuration

MD5 or SHA1/2 authentication and data integrity.

Automatic IKE and Manual key exchange.

Supports NAT traversal

Supports Extended Authentication

Supports Hub and Spoke architecture

DDNS support

Should support IPSEC site-to-site VPN and remote user VPN in transparent mode

SSL VPN Requirements:

Should be integrated solution and should not be user based licensing for SSL VPN

Should support for TWO modes of SSL VPN

1. Web-only mode: for thin remote clients equipped with a web browser only and support web application such as: HTTP/HTTPS PROXY, FTP, SMB/CIFS, SSH, VNC, RDP

2. Tunnel mode : for remote computers that run a variety of client and server applications

Network Intrusion Detection & Prevention System Requirements:

The IPS capability shall have ICSA or equivalent NIPS Certification

Should have a built-in Signature and Anomaly based IPS engine

Should be able to prevent DOS & DDOS attacks

Should support Signature based detection using real time updated database

Should support Anomaly based detection that is based on thresholds

Should allow administrators to create Custom IPS signatures

IPS Signatures should be able to update manually or via pull or push technology.

Configurable IPS filters to selectively implement signatures based on severity, target (client/server), protocol, OS and Application types.
Supports automatic security updates directly over the internet without any dependency of any intermediate device
Security check updates should not require reboot of the unit
Supports attack recognition inside IPv6 encapsulated packets
Supports user-defined signatures with Regular Expressions
Supports several prevention techniques including drop-packet, tcp-rst (Client, Server & both) etc. List all prevention options
Antivirus System Requirements
Should be able to block, allow or monitor using AV signatures and file blocking based on per firewall policy
The System should be able to scan Protocols like HTTP, HTTPS, SMTP, SMTPS, POP3, POP3S, IMAP, IM, NNTP etc.
Should be able to allow, block and quarantine attachments or downloads according to file extensions and/or file types
Should support updates of Signatures manually or via pull / push technology.
Should be able to quarantine blocked and infected files to either local hard disk or externally.
Should be able to block or allow oversize file based on configurable thresholds for each protocol types and per firewall policy.
Should be capable scanning Encrypted VPN tunnel traffic originating from the unit for virus
Web & Application Content Filtering System Requirements:
Should have integrated Web Content Filtering solution
Should be able to enable or disable Web Filtering per firewall policy or based on firewall authenticated user groups for both HTTP and HTTPS traffic.
Should blocks web plug-ins such as ActiveX, Java Applet, and Cookies
Should support Web Exempt List & blocking of Web URL, score based web keyword
Should be able to replace the web page when the web page matches the Web Filtering blocking criteria.
Should be able to identify, retrieve and rate the actual URL of the cache content commonly available in search engines such as Yahoo and Google
Should be able to identify, retrieve and rate the image/multimedia files from search engines. If belongs to a blocked category, that content should be replaced by a blank.
Should allow administrators to create multiple new local URL filtering categories besides dynamic categories
Should allow administrators to override Online URL Database ratings with local settings
Should have application control feature
Should have the intelligence to identify & control popular IM & P2P applications like KaZaa, BitTorrent etc.
Should have database of minimum 500 types of application awareness
Data Leak Prevention Requirements
Should have the ability to prevent data loss through SMTP, FTP, HTTP, HTTPS & IM
Should have built in pattern database

14) Server Load Balancer

S/N	Specification
1	Device should support load balancing of both TCP and UDP based traffic using algorithms like round robin, weighted round-robin, least connections, persistent connects, etc
2	Device should provide minimum throughput of 10Gbps
3	Device should provide 4x10G ports scalable to additional 4x10G ports
4	Should support Client availability (Heartbeat) monitoring
5	Should be support High Availability in Active-Active, Active-Passive mode.
6	Should be Manageable using CLI(SSH), WebUI(SSL), SNMP (V1, V2, V3), etc.
7	The management option should allow configuration, operation, firmware upgrade, traffic reporting, error logs, status logs
8	Should support IPv6 from day one
9	Should support static and dynamic routing
10	Should support Global Server Load balancing, URL based Load balancing, HTTP, HTTP redirection, HTTP Layer 7 redirection, DNS redirection, DNS Fallback redirection,
11	Should be able to create and load http/ssl certificates
12	Should be Rack mountable & should be supplied with Indian standard AC(15Amp) powercord.
13	Should support multiple instances having dedicated CPU, memory, SSL & I/O for guaranteed performance.

15) Storage (NAS for Video Feeds)

S/N	Parameter	Specification
1	Storage	<p>Storage period of 30 days (Primary 15 days & Secondary 30 days) The Primary and Secondary storage may be virtualized. Storage Capacity: 2.5 PB useable) Disks should be minimum of 6 TB Active-Active Load Balancing Storage Controllers with 64GB Cache from day one and scalable upto 128GB Cache without replacing existing Controllers To store all types of data (Data, Voice, Images, Video, etc.) Storage should support all industry standard RAID type The proposed Storage should have 6 Gbps Drives (SSD, SAS & NL-SAS) or higher. Modular design to support controllers and disk drives expansion Should be Rack Mountable The controllers / Storage nodes should be upgradable without any disruptions / downtime Licenses for the storage management software should include disc capacity/count of the complete solution and any additional disks to be plugged in the future, upto max capacity of the existing controller/units. A single command console for entire storage system. Should have the functionality of performance, utilization monitoring of storage, disk drives and management software</p>

S/N	Parameter	Specification
		<p>The storage array must have complete cache protection mechanism either by de-staging data to disk or providing complete cache data protection with battery backup for minimum 4 hours</p> <p>Controllers shall be active-active so that a single logical unit can be shared across all offered controllers</p> <p>The storage should have no single point of failure on components like controllers, disks, cache memory, I/O Ports, Power supply, Fan, etc.</p> <p>The Storage should be based on IP address and the time stamp of the feed for video data, images received from camera.</p> <p>The Storage system should replicate the data from primary to secondary in real-time.</p> <p>The solution should be able to transfer and store the data, on need basis, to any other storage irrespective of Make/Model across LAN/WAN within the state.</p>

16) 4 Rack Solution (DC)

Sl. No	Details	Specification
1.	Integrated Server Room Enclosure	The Integrated Data Centre (4 Rack Solution of 42HU) shall be a self-sufficient data centre with rack based infrastructure approach and optimized system solution, power and cooling system should be concurrently maintainable.
2.	Dimension (HXWXD) in Mm	The Integrated Server Room Solution should have a foot print of 1600mm Width, 2100mm Height & 1200mm Depth (minimum)
5	Main MCCB panel, Wall Mount	Data Center electrical delivery path will have 1no of 100A 4P MCCB box wall mountable having suitable cable entry and termination. (Incomer MCCB, 100A, 4 pole, 25kA)
6	Main Electrical Distribution Panel, rack-mount	Data Center electrical delivery path will have 1no, of 19" Rack mounting electrical panel box complying to Indian relevant electrical codes for Panel fabrication and support structure with following specifications. All MCB should be type D.
		Bus-bar : 100A rated TPN copper busbar
		Outgoing :
		· MCB, 25A DP - 4 Nos. (2nos for A/C, 1no Spare & 1no for Enclosure Light).
		· MCB, 63A DP - 3 Nos. (for 10kVA UPS, 1no Spare).
		· Panel box should not use more than 4 U space in the IT Rack.

		<ul style="list-style-type: none"> All mounting & connection accessories - 1 set (includes termination, ferruling, nuts, washers, etc). 4C X 25 sq.mm copper conductor, XLPE unarmoured cable for Main Panel I/C 4R x 1C x 10 sq.mm copper conductor, XLPE unarmoured cable for UPS units. Depth Variable Slide Rail 590-930mm / 80kg. 3C x 2.5 sq.mm copper flexible PVC cable for Lighting, access control, fire detection system and body grounding - 1 box
7	UPS Power Distribution Panel (Rack Mountable)	UPS Distribution Panel : Rack Frame Mountable with 6nos of IEC C19 Outlets, Power Indicator & 3 core 10sq mm cable of 1.5 mtr length with open end.
8	Floor mount covered cable tray supply and installation	<p>Supply and Fixing of Cable Trough of size: 200W x 50H mm with Cover Lid & necessary accessories for fixing.</p> <p>Specification : Cable Trough with Cover Lid is made of 2mm thk Sheet Steel & Powder Coated to Light Grey.</p>
9	Installation, testing & commissioning for electrical works	The scope for installation, testing & commissioning for electrical works including all components indicated in the above line items is in the scope of the bidder.
10	Minimum 7kW Sensible Cooling System for each Rack with Redundancy (N+N)	Outdoor Type Air-conditioning Unit with Redundancy - 7kW
	<ul style="list-style-type: none"> Cooling Output Range: 7 kW 	DX Type Close Coupled (in a rack) Air-conditioning system with high CFM & sensible cooling Indoor and Outdoor units. The system shall not require raised floor & shall have complete hot and cold aisle separation. Cooling capacity should support average density per rack - 3.5kW & should ensure an energy-efficient dissipation of heat. The external unit (condenser) should be designed on the basis of scroll type and for the R 407C refrigerant. The internal unit should not be consumed any rack U space.
	<ul style="list-style-type: none"> maximum Cooling Noise Level 48-49 dB (A) 	

	<ul style="list-style-type: none"> · Voltage 230/1/50 V/Ph/Hz 	The System should include
	<ul style="list-style-type: none"> · External Unit H /W / D 584/846/298 mm 	(i) 2 x Heat Exchanger (evaporator) for placing on the inside of the system
	<ul style="list-style-type: none"> · Refrigerant R 407C 	(ii) 2 x External ODU unit works with R 407C refrigerant
	<ul style="list-style-type: none"> · Injection pipe 10 mm 	(iii) 1 x Sequencing box
	<ul style="list-style-type: none"> · Suction pipe 16 mm 	
	<ul style="list-style-type: none"> · Cooling Operating Range : 55°C 	The cooling system should be with separate indoor units (evaporator) and outdoor units (condenser). The compressor should be part of the outdoor unit to eliminate noise and vibration inside the indoor unit. The cooling system should Include an integrated heat exchanger mounted on the inner side of side walls with 4 fans. The air routing in the Rack should run horizontal, i.e. the cold air exits in front of the IT components and the warm air drawn in at the rear. The sequence controller should run one cooling unit at a time, and perform a changeover, in case of failure of any of the cooling units. Drain for condensation water (without pump). Power connection for outdoor unit: 230 VAC / single phase / 50Hz via Stabilizer.
	Brand : Rittal/APC/Emerson	Supported with N+N redundancy to maintain temperature and humidity profile within ASHRAE TC9.9 standard's revised specified limits.
11	Supply , Installation, Testing & commissioning of high sensible & high CFM close coupled cooling system	The outdoor unit should have scroll type compressors to ensure high energy efficiency. The scope of the bidder includes Installation & commissioning of the High CFM high sensible cooling unit including related works.

12	Copper piping	Refrigerant copper piping with (19 mm / 13 mm thick) closed cell elastomeric nitrile rubber tubular insulation between each set of indoor & outdoor units as per specifications, all piping inside the room shall be properly supported with MS hanger. Transmission wiring between indoor to outdoor unit in a suitable PVC conduit - 1.5 sq.mm 4 core. PVC Drain Piping - 25mm dia. Rigid PVC piping complete with fittings, supports as per specifications duly insulated with 6mm thick nitrile rubber tubular sleeves
13	Refrigerant Gas	Supply of R 407C, refrigerant gas, and charging it, after cleaning the line, compressor oil fill and pre-testing for leakage. Testing the line after charging the gas as per standards and directions
14	Access Control System	Standalone Coded Lock Reader cum Controller. One Reader will open all the Front Doors.
		Access control system - installation, testing and commissioning of Reader, Controller, Ergoform-S handle (electro-magnetic), cabling, etc.
15	Rack-mountable Fire Detection and Suppression system (Master)	Fire detection and suppression master system must be compact enough to occupy only 1U space in each IT rack. 1U Rack Mountable device should have built-in high sensitivity smoke detection with active air-sampling (VESDA). Also the NOVEC 1230 suppression system cylinders must be built-in within the 1U detection device with sufficient quantity. The 1U Fire detection and suppression system should be equipped with fire panel, with actuator, discharge nozzle, piping complete with accessories. The system should include a manual abort option. This device should be monitored using potential free contacts. It should have possibility to expand up to 4 nos. of IT Rack using master & slave configuration.
	Brand : Rittal / APC/Equivalent	
16	Rack-mountable Fire Suppression System (Slave)	Fire detection and suppression Slave unit must be compact enough to occupy only 1U space in each IT rack. 1U Rack Mountable Slave device should have the NOVEC 1230 suppression system cylinders, must be built-in within the 1U device with sufficient quantity. The 1U Fire suppression Slave unit should be communicating with master units for activation and suppression system.
	Brand : Rittal / APC/ Equivalent	
17	Fire detection and suppression - Installation related services	Bidder shall provide installation related services for fire detection system & Novec1230 gas based automated suppression system.

		The design, equipment, installation, testing and maintenance of the Clean Agent Suppression System shall be in accordance with the applicable requirements set forth in the latest edition of the NFPA Standards.
18	42U Server / Network Rack	The Proposed Racks has to be designed to meet the safety requirements of the modern data centre with IP 54 category with min.1400kgs load bearing capacity of Rack. Both the front and rear door should have a comfort handle with different locking options. The rack should be suitable for housing a high performance Indoor cooling unit. Cable entry should be entered via the gland plate without affecting the climatic conditions inside the Rack.
	Brand : Rittal /APC/Emerson Equivalent	<u>Technical specifications:</u>
		Basic Structure: Frame made of sturdy frame section construction, consisting of 9 folded rolled hollow frame section punched in 25mm DIN pitch pattern . All profile edges are radiused. The corners are stiffened with welded MS die-cast, copper coated, corner connectors , removable top & Bottom cover with Cable entry provision. Frames are bayable, scalable and modular. Load carrying capacity: Minimum 1300kgs

		<p>DK PS Rack of Size : 800W X 2000H (42U) X 1200D fitted with Front Glass Door with 130° hinges, Rear Sheet Steel Door with 130° hinges, Set of Side Panel, 2 pairs of 42U 19" L - type angles & special assembly kit for mounting 19" angles & punched sections with "U" Marking Stickers, top cover, bottom cover with cable entry provision, 100mm height base plinth, Baying Kit for PS , Copper Earth bus bar, 2 NOS Vertical Socket Strip with 12nos of IEC C13 Sockets, Indicator switch, 4 mtr power chord with IEC C20 plug for each rack, Ergo-form handle with unique key lock insert, Component Shelf 720mm deep rack, Vertical cable managers with cable loops, Hardware pack of 20 , Foam insert for vertical shielding & installed between racks, Air baffle plate, Metal Shunting Rings 90x60 (pack of 10). The solution should include blanking panels (1 U, ABS Material) for blocking the empty U space in the racks for improved cooling performance Rear Doors must be equipped with Automatic Door Opening system in case of cooling failures.</p>
		Color : RAL 7035
19	Fault Signals	Provisioning of monitoring fault signals
20	Remote Monitoring system with Graphical user interface with e-mail alerts.	<p>The central monitoring system should be 1U rack-mount and should be able to monitor up to 32 sensors / CAN-Bus connection units with option of redundant power supply. The following devices to be monitored : Temperature/Humidity, Water Leakage, Fire Detection & Extinguishing, Air-condition Units, Door access sensor. It should also monitor & control Automatic Door Opening of 2 Doors. It should provide a single TCP IP interface for remote monitoring of all components and generate email alerts and warnings. The central monitoring device should also be connected to Signal Pillar with Audio & Visual alarm extension. The central monitoring system having CAN bus sensor integration technology should be modular and scalable from future expansion point of view. It should be able to operate with Protocols: TCP/IPv4, TCP/IPv6, SNMPv1, SNMPv2c, SNMPv3, Telnet, SSH, FTP, SFTP, HTTP, HTTPS, NTP, DHCP, DNS, SMTP, XML, Syslog, LDAP. The system should have feature to generate SMS alerts in case of future demands.</p>

21	Complete Installation, testing & commissioning	Installation, testing & commissioning of complete Integrated Data Centre.
22	Installation and Training	(i) Installation of Mini Data Centre and the relevant components has to be carried out by qualified technicians
		(ii) 01 day on site training to the user at site

17) Camera Type A- (Box Camera for ANPR, RLVD)

S/N	Parameter	Minimum Specification
1	Image sensor and Effective Pixels (Resolution)	1/ 3" or better, CMOS Progressive Scan & Minimum 2 MP or higher
2	Electronic Shutter	1 to 1 / 8,000 s or better
3	Focus	Manual
4	Automatic Gain Control	Automatic / Manual
5	Multi Focal	5 to 50mm or better
6	Frame Rate	25/30 FPS at 1080p Resolution
7	Codec	H.264, MJPEG or better
8	Minimum Illumination	0.3 Lux@30 (IRE)f1.2 (Colour) & 0.1 Lux @ 30 (IRE) f1.2(B/w)
9	backlight Compensation	Required, Camera should adjust BLC feature automatically depending on the light condition
	Video	
10	Day and Night functionality	Automatic, Color, Mono
11	IR illuminator	External/internal Illuminator with visibility should be at least 50 meter
12	Video Resolution	(1920x1080) 1080p,(1280x960) SXGA, (1280x720) 720p, (800x600) SVGA,(720x480) D1, (704x480) 4CIF, (640x480) VGA, (352x240) CIF
13	WDR	Yes
14	Video Streams	Individually configurable 03 video streams (H.264, MJPEG)
15	Intelligent Video	Motion detection
	Network & Interface	
16	Interface	RJ-45 for 10/100 base-T Ethernet
17	Network Protocols support	IPv4, IPv6, TCP, RTSP/RTCP/RTP, ICMP, UDP,IGMP, DNS, DHCP, ARP, NTP, SNMP
18	Alarm Event (Non-working, Tampering)	Events / alerts send via FTP, HTTP, Pre-Post alarm video buffering.
19	Compliance	ONVIF profile S compliant
20	Security	Password Protection, HTTPS encryption, IEEE 802.1X
	General Camera Features	
21	Operational Temperature °C	0°C to 50 °C

22	Casing	IP66 or better rated housing and Vandal proof rating IK10
23	Power	PoE IEEE 802.3af class0, DC12V, AC24V
24	Certifications	CE, FCC, UL
25	Local Storage (Camera inclusive of memory card of 64 GB)	In the event of failure of connectivity to the central server the camera shall record video internally or on the SD card automatically.

18) Context Camera 5MP

S/N	Parameter	Minimum Specification
1	Image sensor and Effective Pixels (Resolution)	1/ 3" or better, CMOS Progressive Scan & Minimum 5 MP or higher
2	Electronic Shutter	1 to 1 / 10,000 s or better
3	Auto Back Focus	Yes
4	ICR	Auto / Day / Night
5	Lens	5 to 50mm or better
6	Frame Rate	25/30 FPS at 2560x1920p Resolution
7	Codec	H.264, MJPEG or better
8	Minimum Illumination	0.1 Lux (Colour) & 0.01 Lux (B/w)
9	Backlight Compensation	Required, Camera should adjust BLC feature automatically depending on the light condition
Video		
10	Day and Night functionality	Automatic, Color, Mono
11	IR illuminator	External Illuminator with visibility should be at least 50 meter
12	Video Resolution	2560x1920 (5MP), (1920x1080) 1080p, (1280x720) 720p, (704x480) 4CIF
13	WDR	Yes
14	Video Streams	Individually configurable 02 video streams (H.264, MJPEG)
15	Intelligent Video	Motion detection, Tampering alarm, network failure
Network & Interface		
16	Interface	RJ-45 for 10/100 base-T Ethernet
17	Network Protocols support	ARP, IPv4/v6, TCP/IP, UDP, RTP, RTSP, HTTPS, ICMP, SMTP, DHCP, PPPoE, UPnP, IGMP, SNMP, QoS, ONVIF
18	Alarm Event (Non-working, Tampering)	Events / alerts send via FTP, HTTP, Pre-Post alarm video buffering.
19	Compliance	ONVIF profile S compliant
Security		
20	General	Password Protection, HTTPS encryption, IEEE 802.1X
General Camera Features		
21	Operational Temperature °C	0°C to 50 °C
22	Casing	IP66 or better rated housing and Vandal proof rating IK10
23	Power	PoE (802.3 af) OR AC 24V/ DC12V
24	Certifications	CE, FCC, UL

25	Local Storage (Camera inclusive of memory card of 64 GB)	In the event of failure of connectivity to the central server the camera shall record video internally or on the SD card automatically.
----	--	---

19) Camera Type B- Fixed Surveillance Cameras

S/N	Parameter	Minimum Specification
1	Image sensor and Effective Pixels (Resolution)	1/ 3" or better, CMOS Progressive Scan & Minimum 2 MP or better
2	Electronic Shutter	1 to 1 / 100,000 s or better
3	Focus	Automatic / Manual
4	Automatic Gain Control	Automatic / Manual
5	Frame Rate	25/30 FPS for 1920 x 1080
6	Codec	H.264, MJPEG or better
7	Multi focal	3 to 12mm or better, motorized, auto focus
8	Minimum Illumination	0.02 Lux(30 IRE)@f1.2 (Color) & 0.002 Lux (30 IRE) @ f1.2(B/w)
9	High Light and backlight Compensation	Required, Camera should adjust BLC feature automatically depending on the light condition
Video		
10	Day and Night functionality	Automatic, Color, Mono
11	IR illuminator	Internal/External Illuminator with visibility should be at least 50m.
12	Video Resolution	Minimum 2 MP (1920 x 1080) or Better
13	WDR	True WDR 120 dB or better
14	Video Streams	Individually configurable 03 video streams (H.264, MJPEG)
15	Intelligent Video	Motion detection, Tampering Alert, face detection
Network & Interface		
16	Interface	RJ-45 for 10/100 base-T Ethernet
17	Network Protocols support	IPv4, IPv6, TCP/IP, HTTP, DHCP, UDP, DNS, SMTP, RTP, RTSP, SNMP protocols/Should meet all functional requirement of the project
18	Alarm Event	Events / alerts send via FTP, HTTP, Pre-Post alarm video buffering.
19	Compliance	ONVIF profile S compliant
Security		
20	General	Password Protection, HTTPS encryption, IEEE 802.1X
General Camera Features		
21	Operational Temperature °C	0°C to 50 °C
22	Casing	IP66 or better rated housing and Vandal proof rating IK10
23	Power	PoE (802.3 af) OR AC24V/ DC12V
24	Certifications	CE, FCC, UL
25	Local Storage (Inclusive of 64GB memory card)	In the event of failure of connectivity to the central server the camera shall record video internally or on the SD card automatically.

20) Camera Type C: PTZ

S/N	Parameter	Specification
1	Sensor	1/3" CMOS & Minimum 2 MP
2	Min. Illumination	Color: 0.1 lux; B/w: lux 0.01 lux and 0 lux with IR
3	Scanning System	Progressive
4	S / N Ratio	>50dB
5	IR Distance	Inbuilt / External with adequate coverage in sync with PTZ field of view. IR visibility should be minimum 160 mtr.
6	IR Intensity	Automatically Adjust
7	IR on/Off Control	Auto
8	WDR	120 db or better
Lens		
9	Optical Zoom	30X or better
10	Focal Length	4.3 to 129mm
11	Focus Control	Auto/Manual
Pan Tilt Zoom		
12	Pan/Tilt Range	Pan: 0° ~ 360° endless; Tilt: -15° ~ 90°, auto flip 180°
13	Manual Control Speed	Pan: 0.1° ~160° /s; Tilt: 0.1° ~120° /s
14	Preset Speed	Pan: 240° /s; Tilt: 200° /s
15	Presets	Minimum 250 Preset Points
Video		
16	Compression	H.264 / MJPEG
17	Streaming Capability	Minimum 3 Streams
18	Resolution	1080 P or Better
19	Frame Rate	1080P (1 ~ 25/30fps)
20	Day and Night	Automatic, Color, Mono
21	White Balance	Auto / Manual /ATW/Indoor/Outdoor/Daylight lamp/Sodium lamp
22	Noise Reduction	Ultra DNR (2D/3D)
23	Motion Detection	Required
24	Region of Interest	Required
25	Digital Zoom	14X or better
Network		
26	Ethernet	RJ-45 (10/100Base-T)
27	Protocols	IPv4/IPv6, HTTP, HTTPS, 802.1X, QoS, FTP, SMTP, UPnP, SNMP, DNS, DDNS, NTP, RTSP, RTP, TCP, UDP, IGMP, ICMP, DHCP, PPPoE
28	Interoperability	ONVIF Profile S or higher
29	Alarm	2 input / 1 output
30	Local Storage (inclusive of 64 GB memory card)	In the event of failure of connectivity to the central server the camera shall record video locally on the SD card automatically.
31	Certification	CE, FCC, UL
32	Power	Hi-PoE OR AC 24V
General		
33	Working Temperature /	0°C to 50 °C, 80% RH non-condensing within enclosure

	Humidity	
34	IP Rating	IP 66 or better rated Housing & IK10 Vandal Proof Housing
35	Mounting Accessories	For pole and surface mount with L/C Brackets

21) IR Illuminator

S/N	Parameter	Specification
1.	Range	Min 50 meter
2.	Minimum illumination	High Sensitivity @0 Lux
3.	Angle of illumination	Adjustable
4.	Power	PoE, Auto on/off
5.	Casing	IP 66
6.	Operational Temperature	0°C to 55 °C
7.	Certification	CE/FCC/EN/UL

22) Camera Type: 360° camera

S/N	Parameter	Specification
1	Video Compression	H.264 and MJPEG
2	Max Frame Rate	1080p@20ips
3	ONVIF-Compliant	Profile S, G, Q
4	Imager	1/3" CMOS progressive scan
5	Resolution	Edge: (2688x1512) 16:9 Client: (2992x2992) 1:1 MJPEG: (720x720) 1:1
6	Day/Night	Mechanical ICR
7	IR Illumination Distance	15m
8	Motion Detection	4 selectable ROI areas
9	Privacy Zones	1
10	Alarm Input/Output	1 / 1
11	Audio Input/Output	1 / 1
12	Video Streams	Triple
14	Focal Length	1.55 mm
15	Simultaneous Users	3
	Network Interface	
16	Interface	10/100/1000 Ethernet
17	Supported Protocols	IPv4/v6, TCP/IP, UDP, RTP, RTSP, HTTP, HTTPS, ICMP, FTP, SMTP, DHCP, PPPoE, UPnP, IGMP, SNMP, QoS, ONVIF, ARP
18	Security	HTTPS encryption, IEEE802.1X
	General	
19	Power Input	PoE IEEE 802.af, DC12V
20	Operating Temperature	0°C ~ 50°C (-22° ~ 122° F)

21	Enclosure ratings	IP66 &IK10
22	Local Storage (inclusive of 64 GB memory card)	In the event of failure of connectivity to the central server the camera shall record video locally on the SD card automatically.
23	Regulatory	CE, FCC, UL certified

23) Camera Type F: 180°Panaromic camera

S/N	Parameter	Specification
1	Image Sensor	5MP = 1.2MP x 4
2	H-FOV	180°
3	Optical Format	1/3" CMOS
4	Minimum Illumination	Color (Day Mode) : 0.02 Lux B/W (Night Mode) : 0.002 Lux, IR sensitive
5	Full FOV Resolution	Total: 5120 H x 960 V Per Sensor : 1280 H x 960 V
6	Dynamic Range	83.5dB
7	Frame Rates	At Max Resolution : 12fps @ 5120 x 960 1/4 Resolution : 30fps @ 2560 x 480
8	Lens (Remote Focus & P-iris)	CS, F1.2, 5.6mm x 4, IR,H-FOV = 47°
9	Heater	Switch On/Off : On: 17°C (62.6°F), Off: 30°C (86°F)
10	Voltage Input	12V to 35V DC / 24V AC
11	Optics	Remote focus and P-iris control
12	Picture-in-Picture	Simultaneous delivery of full field-of-view and zoomed images
14	Programmable Shutter Speed	Controls motion blur
15	Motion Detection	On-camera real-time, 1024 detection zones (per sensor)
16	Backlight Compensation	Yes
17	Compression Type	H.264 (MPEG-4, Part 10)/Motion JPEG
18	Network Protocols	RTSP, RTP/TCP, RTP/UDP, HTTP, DHCP, TFTP, IPv4, QoS
19	Network Interface	100Base-T Ethernet
20	Multi-Streaming	8 non-identical streams (2 per sensor)
21	Operating temperature	0°C to +50°C w/Heater
22	Power Input	PoE IEEE 802.af, DC12V
	Auxiliary Power	18-48V DC, 24V AC
23	Regulatory	CE, FCC, UL certified

24) LED Display Boards

S/N	Parameter	Specification
1.	LED Type	DIP
2.	Best Viewing Distance(m)	> 10 Meter (5 LED per Pixel)
3.	Pixel Pitch	10 mm

4.	Pixel Density	10,000 Dots/m ²
5.	Brightness	>= 7000 cd/m ² (Adjustable) or better
6.	Refresh Frequency	>= 1000 Hz (Adjustable)
7.	MTBF	> 10,000 Hours
8.	Max Power Consumption	600 Watt/ m ²
9.	Average Power Consumption	200 Watt/ m ²
10.	Viewing Angle	120° Horizontally & 45° Vertically
11.	Color	More than 16.7 million @ 16-bit Processing depth
12.	Color Temperature	R.G.B brightness 256 level adjustable
13.	IP Rating	IP 65 Front & IP 54 Rear
14.	Life Span	> 100000 Hours (After that 50 % Illumination)
15.	Operating Temperature	0 ° C to 55° C
16.	Operating Humidity	10 % RH to 90% RH
17.	OS Platform	Windows 7/ 10
18.	Communication Interface	RJ45/Fiber port
19.	Certification	CE, FCC, UL/ETL
20.	Software Display Controller	<ul style="list-style-type: none"> • Should be able to remotely configure and manage at least 300 LED Screen from a Central location • Should be able to play the selective contents at different LED Screens as per the requirement • Should provide an easy-to-use playlist format for scheduling of content, images, videos, live feeds such as weather forecasts or the news, social media etc. • Assign roles and permissions to allow multiple content creators and managers • Should have an interface for content design with readymade/custom made templates • Should have options for Importing video feeds, Images and contents from other sources such as inputs from Environmental Sensors, Social Media, Camera Feeds etc. • The Hardware for the central Display Controller has to be provided along with the proposed solution • From the scalability point of view, the software should be able to do so without any extra Licensing up to 50 LED Screens

25) Access Points

S/N	Specification
1.	Access Points proposed must include radios for both 2.4 GHz and 5 GHz with 802.11n/ac or newer. The same Access Point must also include 1 nos. of 10/100/1000 Base-T auto sensing RJ45 based Ethernet ports.

2.	It should be compatible and be able to integrate with the Cloud based Controller. Must support SSH & SNMP protocol
3.	Should support Proactive Key Caching or other methods for Fast and Secure Roaming.
4.	Each AP Should support 4 WLANs for SSID deployment flexibility.
5.	AP's Should support Minimum 70 Meters radial coverage & Minimum 50 concurrent users @ each radio channel
6.	AP's Should support "802.3 af" standards i.e. of Power over Ethernet (PoE)
7.	Access point shall support Pole, Wall, and roof mounting options.
8.	The Access point shall be IP65 or above rated for dust and water Ingress protection.
9.	The Access point shall be rated for operation over an ambient temperature range of 0° to 55°C
10.	Should support interference detection and avoidance for both Wi-Fi and non-Wi-Fi interferes

26) Sensors

S/N	Parameter	Specification
Environmental Sensor		
1.	General	They should be ruggedized enough to be deployed in open air areas such as Traffic Junctions, Streets, Parks, Parking Lots etc.
2.		The sensor should be able to communicate its data using wireless technology
3.		The data should be collected in a software platform that allows third party software applications to read that data.
4.		The sensor management platform should allow the configuration of the sensor to the network and also location details etc.
5.	Measurement Parameter	NOX, SO2, CO2, O2 Ambient Light, Sound
6.	Measurement range	Real Time measurement NOX : 0 to 50ppm , 5000ppm SO2 : 0 to 50ppm, 5000ppm CO : 0 to 50ppm, 5000ppm CO2 : 0 to 10% / 0 to 20% O2 : 0 to 10% / 0 to 25% (2 ranges each, maximum range ratio 1: 25 except O2) *Optionally, N2O and CH4 can be measured Temperature: 0 to 100° C Light: up to 10,000 Lux UV: up to 15 mW/ cm2 Sound/Noise: up to 120 dB (A)
7.	Repeatability Error	±0.5% FS
8.	Drift	Zero Drift: <ul style="list-style-type: none"> ±1.0% FS max per week ±2.0% FS max per week if range is less than 200ppm) ±2.0% FS max./month for O2 meter Span drift: <ul style="list-style-type: none"> ±2.0% FS max per week

S/N	Parameter	Specification
		<ul style="list-style-type: none"> ±2.0% FS max per month for O2 meter
9.	Response Time	120 seconds max. for 90% response from the analyzer inlet
10.	Connectivity	USB / Ethernet /Wireless
11.	Operating Temperature	0 to 55 °C
12.	Data Interface	GPS, GSM, Wi-Fi- 802.11 n/ac
Temperature, Humidity Sensor		
13.	Temperature Sensor	Real-time Temperature Range: Indoor -10°C ~ +70°C (+14°F ~ +122°F)
14.	Humidity Sensor	Real-time in Air Humidity Level

27) Managed Outdoor L2 Switch with PoE - 8-port

Sr. No.	System Description & Minimum Requirement
1	8 RJ-45 autosensing 10/100/1000 PoE+ ports
2	1 X RJ45 console port
3	2 X SFP+ 10GbE ports for Uplinks populated with 10GBASE-SR/LR fiber module
4	Should support Switching Capacity of 50 Gbps
5	Should support Throughput of 40 Mpps
6	Should have Dual-flash images for redundant switch software images
7	IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.3z, IEEE 802.3x, IEEE 802.3az, IEEE 802.3ab, IEEE 802.3ad, IEEE 802.1d, IEEE 802.1w, IEEE 802.1q.
8	Support STP, RSTP, MSTP
9	Switch Should Supports 16K MAC Address MAC address auto Learning and auto aging
10	Shall support at least 255 IEEE 802.1Q VLANs, up to 4094 port-based VLAN IDs
11	Shall support GARP VLAN Registration Protocol allowing automatic learning and dynamic assignment of VLANs
12	IGMP snooping v1/v2/v3
13	Static or dynamic Link aggregation
14	Supports IP based
15	IEEE 802.1x
16	RADIUS, TACACS+, Rapid Per-VLAN Spanning Tree (RPVST+), OSPF
17	Multiple User level privilege management and password protection
18	Should support Port mirroring, LLDP
19	Secure Web-management sessions with HTTPS / SSL
20	DHCP Snooping, Option 82
21	Should support BPDU filtering
22	Should support Address Resolution Protocol (ARP), DHCP relay, Static IPv4/IPv6 routing, Link Aggregation Control Protocol (LACP), ease of configuring link redundancy of active and standby links, Virtual Switching

23	CLI, Web and Telnet Facility for management
24	SNMPv1/v2c/v3 through IPv4 and IPv6
25	IPv6 ready from Day 1
26	CE / EN / IEC, FCC, ROHS

28) VMS Software

Features	Specifications Required
Concurrent Licenses	The VMS shall not charge for the number of concurrent clients or camera channels
VMS Hardware	The VMS system shall utilize commercial-off-the-shelf (COTS) computer workstations, servers, networking devices and storage equipment. VMS shall already support IP cameras from at least fifty (50) major Successful bidders. Successful bidders shall clearly list in their proposal the brands and models already integrated into VMS.
Unattended Recording	Recording of all video transmitted to the VMS shall be continuous, uninterrupted and unattended
Motion Detection	The VMS system shall offer the capability of video motion detection recording, such that video is recorded when the NVRMS detects motion within a region of interest of the camera's view. Video prior to the detection of the motion shall also be stored with using the pre-alarm buffer feature of the camera
System Health Monitoring	The VMS system shall manage the video it has been configured to monitor. Loss of video signal shall be configured to annunciate on VMS client by an on screen visual indication alerting operators of video loss
Open Architecture	The VMS software shall have an open architecture supporting IP cameras and encoders from multiple manufacturers providing best-of-breed solutions ranging from low-cost, entry-level features to high-resolution, megapixel features. The VMS system shall be a scalable client – server architecture built using well known operating systems. The Video Management System software shall include multicast and multi-streaming support
Audio Support	The VMS client software shall be able to view live video and audio, recorded video and audio, and be able to configure the complete system all from a single application. The Audio shall be broadcasted through loud speakers from control room to the cameras connected to external speakers. Operator shall be able to select particular camera speaker to enable the public addressing
Uninterrupted Recording	The VMS shall continue to record video and audio at all times during the administration and configuration of any feature. The VMS shall allow for up to 100 cameras or other devices to be connected to each Recording Server and for an unlimited number of Recording Servers to be connected to a single master Recording Server across multiple sites. The system shall support any combination of master and slave servers to provide flexibility and scalability in the overall system configuration
Fully featured Remote Client	The VMS client software shall have the same functionality when connected remotely as it does when it is run locally on the same computer as the server software
User Level based feature access	The VMS client software shall add and remove features based on the permissions of the user and the licensed functionality
Operating System	All of the below should be supported -

Support	1) Microsoft Windows Server 2003/2008/2012
	2) Microsoft Windows 7 (all versions)
	3) Microsoft Windows 8 (all versions)
Combination of OS supported by clients	The VMS software shall allow the user to have any combination of VMS client applications running on any of the supported operating systems be able to connect to any of the VMS servers running on any of the supported operating systems. For example, a VMS client running on Microsoft Windows 7 shall be able to simultaneously connect to four (4) different VMS servers all running on different operating systems, such as Windows Server 2003, Windows XP and Vista
Monitor support per client	The VMS software shall have the capability to run multiple client applications simultaneously on one workstation with multiple monitors. Up to 12 monitors shall be configured on a single workstation with one (1) client application running on each monitor. Because decompressing video is CPU-intensive, the PC workstation shall have multiple core processors, with a recommendation of one core for each VMS client application
Web Client Support	The VMS shall also allow an authorized user to view video through a web client interface. The web client interface shall allow authorized users to view live video, view recorded video, control pan-tilt-zoom (PTZ) cameras and activate triggers. The web client interface shall allow connections to multiple VMS servers simultaneously. The web client interface shall operate without requiring installation of any software
Browser Support	All of the below should be supported –
	1) Internet Explorer 6 and later
	2) Firefox 2 and later
	3) Safari 2 and later
Recording Retrieval	The VMS server software shall record and retrieve video, audio and alarm data and provide it to the VMS clients upon request
Mobile client	The VMS software shall provide at no additional charge a purpose-built mobile application capable of viewing multiple simultaneous live video streams and playing a recorded video stream. Application shall be provided for both iOS and Android operating systems
Data safety	The VMS server shall not decode video for the purpose of repacking it for transmission to clients
Meta data Support	The VMS server software shall record video based on metadata generated by an edge network device. The edge network devices shall generate the metadata and transmit it with the video stream to the VMS server software
Camera Licenses	The VMS shall license the total number of cameras on the system. This license shall be based on the Camera MAC ID and not Server network card Mac ID
VMS server service	The VMS server software shall run as a service. The VMS shall not require any application to be running in order to operate
Map integration	The VMS shall allow the use of maps. The maps will be accessible to users with the appropriate permission levels and display video sources and their status
Wide screen	The VMS shall provide an option to view 16:9 wide video display panels

support	
Digital PTZ	The VMS software shall allow control of PTZ cameras to authorized users and be used to maneuver a PTZ camera. When used on a non-PTZ camera, it shall allow you to digitally pan, tilt, and zoom on any video whether in live or recorded mode
Camera Grouping	The VMS software shall have a feature for viewing logical groups of cameras. This shall allow efficient viewing of cameras in a logical order
Preset Viewing	The VMS software shall have a feature to organize your cameras into preset views. Views are preconfigured arrangements of the video panels so that they may be easily recalled later. A view can save the location of the video streams, audio streams, POS data, maps, and event views. These views shall be accessible in both live and recorded video modes
Video Play Back	The VMS client software shall be used to search for and play back recorded video, audio, and events from VMS servers. All recorded video shall be played back and displayed in a synchronized multi-camera layout. It shall be possible to playback simultaneously 64 cameras on the surveillance system, with a selection of advanced navigation tools, including an intuitive timeline browser
Searching parameters	The VMS software shall support searching through recorded video based on time, date, video source, image region and have the results displayed as both a clickable timeline and a series of thumbnail images
Audio playback	The VMS software shall allow search and play back of audio in synchronization with video
Export	The VMS software shall provide the option of exporting the file in the following formats:
	1) Standalone Exe (*.exe) – includes an executable player with the video and audio data
	2) AVI File (*.avi) – a multimedia container format
	3) MKV File (*.mkv) – a format to play HD video files.
Integrated Video Analytics	VMS shall have the possibility to integrate external Video Analytics systems
	1) Video Motion
	2) Tripwire and Trespass
	3) Left/Missing object detection
	4) Loitering and Crowding management
	5) Video Stitching
	6) Fire and Smoke detection
	7) 3rd party Analytics
	The VMS software shall have the ability to configure each video inputs recording time on an hourly basis. This shall allow the user to schedule when to record on motion, when to record on event and when to not record
Recording Triggers	The VMS software shall be able to send a predefined email based on an event trigger. The VMS software shall also support SSL and TLS connections for transmissions of the mail
Email Trigger	The Video Management System shall incorporate intuitive map functions allowing for multilayered map environment. The map functionality shall allow for the interactive control of the complete surveillance system, at-a-glance overview of system integrity, and seamless drag-and-drop integration with video wall module option. The activation of the VMD or Camera disconnected alarm shall display the alarm location with animated camera's icon shown in the location map, and the pre-defined alarm documents

Map Function	The VMS shall support a central alarm management and monitoring function, providing an alarm / event queue where all incoming events are on display. The alarm queue shall provide, but not limited to, the following information:
Alarm Management	1. Alarm date and time
	2. Alarm status
	3. Current alarm condition
	4. Detector/input name/address
	5. Alarm location
	6. Message priority
	7. Operator who is working on the alarm/event when it was acknowledged
	The VMS shall include support for seamless integration with Access control system and perimeter Intrusion system. The VMS shall provide a documented Software Development Kit (SDK) to allow integration with other application software
Integration	The Video Management System shall support high availability of recording servers. A failover option would provide standby support for recording servers with automatic synchronization to ensure maximum uptime and minimum risk of lost data. Minimum required is N: 1 OR N: N Redundancy
Redundancy	In case of Network Failover, the video should be able to locally store on the Camera, once the network is established the stored video should be able to synchronize with the central storage system

29) Indoor Fixed Dome Cameras with PoE

S/N	Specification
1	Image sensor: 1/3" or better Progressive Scan CMOS 2 MP or better
2	Lens: 3 to 12 mm or better, DC-iris, motorized
3	Field of View: 90.1°~31°
4	Day and Night: Automatic/manual/scheduled
5	Min. Illumination / Light Sensitivity: Color mode: F1.2 @ 0.05 lux Black and white mode: F1.2@ 0.005 lux
6	Light sensor: Senses the level of ambient light to determine when to switch day/night mode.
7	Video Compression: H.264 and Motion JPEG
8	Resolutions and frame rates: 25/30 fps at 1920x1080 (1080p)
9	Protocol Support: IPv4/IPv6, TCP/IP, HTTP, DHCP, UDP, DNS, SMTP, RTP, RTSP, SNMP protocols/Should meet all functional requirement of the project
10	WDR: 120db or better
11	PoE: 802.3af compliant
12	Housing Certification: IP66 or better and IK10 rated
13	Camera Should remote Zoom and Auto focus
14	Camera should support Micro SD/SDHC (along with 128 GB SD card) and other preceding standard SD cards
15	Should be ONVIF profile S compliant
16	Certification: CE, FCC and UL

17	The camera should be automatically discovered and configured when connected to VMS or Network Switch, to set the right network parameters for the video stream on the network
18	All camera should be of same make except multi- sensor camera

30) Blade Enclosure

Sr. No	Features	Specifications Required
1	Description	<ul style="list-style-type: none"> • Blade Server Chassis/Enclosure must be quoted as required by OEM solution architecture at Primary Site. • Blade Enclosure shall support intermix of Intel Xeon, AMD and RISC/EPIC processors based blade servers within the same chassis enclosure. • Blade Enclosure shall support Windows, Linux, UNIX & VMware operating system. • Chassis should not be declared End-of-Sale at the time of bid submission and should not be declared End-of-Support for next 5years.
2	Blade Enclosure	Blade Chassis to accommodate minimum of 14 or more half blade and 7 or more Full Height Hot Pluggable Blade Servers
3	I/O Modules	Minimum Four or more high speed switch bay capable of supporting I/O architectures in Ethernet, Fiber Channel, FCoE and Infiniband.
4	Chassis	Blade Chassis should have a single / dual redundant mid plane where the blades and other subsystems get plug. Blade chassis must be 10Gbps ready and in future blade chassis must support 10Gbps switches without replacing the blade chassis for investment protection.
5	Cooling Modules	Should offer flexibility in connecting to datacenter power enabled with technologies for lower power consumption. Fan Module should be controlled through temperature sensors for achieving variable speed with respect to environmental conditions. Each blade enclosure should have Cooling subsystem consisting of fully redundant hot pluggable fans or blowers. In case of failure the balance fans/blower should ensure the smooth functioning of the blade system with all servers populated till the fan is replaced.

6	Ethernet Switch Modules	<p>Redundant 10Gbps L2/L3 Ethernet switching module to be provided to connect all the blades to the LAN and should be configured to minimize the no. of ports in the external switch as also to reduce the no. of cables coming out of the chassis. There should be minimum 4*10Gbps uplink ports using short range SFP+ modules & 2*1Gbps RJ-45 ports to be provided from each 10Gbps switch to external LAN connectivity.</p> <ul style="list-style-type: none"> • Shall be capable of increasing the number of NICs per connection without adding extra Blade I/O modules and reducing cabling uplinks to the data centre network. • Shall be capable of providing min 16 x 10Gbps downlinks to Blade server NICs. • Shall be capable of providing flexibility in choosing between 10Gbps SR, LR, or LRM fiber and copper SFP+ uplinks. • Shall be capable of providing 10 x 10Gbps uplinks to connect to other Standard Data Center Ethernet switches. • Shall be capable of supporting up to 4 Physical NICs per 10Gbps server communication port, within the server Blade. • Each of the tailoring NIC shall be capable of tailoring the network bandwidth with their own dedicated, optional customized bandwidth per 10Gb downlink connection, optional with customizable speeds from 100Mbps to 10Gbps.
7	I/O Path for all Fabrics	<p>Chassis should have dual I/O connections from every blade server to help provide maximum uptime.</p>
8	Management Modules	<p>Should be configured with redundant hot pluggable management module to manage the blades using GUI. Chassis should be configured with integrated IP KVM switch module for managing the Blade chassis locally as well as remotely. All required System software has to be from the OEM itself. Complete GUI with view of the individual blade chassis, multiple chassis.</p>
9	Deployment & Remote Management	<p>Should support simultaneous remote access of different servers in the chassis. Complete Hardware based Remote Administration from a standard web browser with Event logging, detailed server status, Logs, Alert Forwarding, virtual control, remote graphical console, Remote Power Control / Shutdown, Virtual Media for Remote boot and control</p>
10	Form Factor	<p>Upto 10U chassis</p>
11	CD/Diskette/USB/Optical Drive Support	<p>Must have at least one DVD(R/W) drive per chassis (Internal/External through USB cable).</p>
12	System Panel	<p>LED/LCD indicators to provide power-on, location, over temperature, information and system error conditions</p>

13	Fiber Channel Pass Through Module / Fiber Channel I/O Module	4Gb per port throughput to SAN fabric, should have Optic ports with pre install SFP's delivered in single I/O Bay, 1:1 non blocking architecture, Wire Speed to be configured in Redundancy. 2*16Gbps SAN switches with adequate numbers of 16Gbps SFP modules should be supplied
14	Mid plane	Chassis should have a highly reliable mid plane for providing connectivity of the shared resources to the compute nodes in a highly reliable manner
15	Management Appliance	Also should provide support for remote console management, Power on/off blades, monitoring the power status, temperature, cooling fans status, I/O status, system diagnostic programs etc. provided through the management software.
16	Storage Management	Redundant 16 port 16Gbps SAN switches to be provided with 16 internal ports and 12 uplink ports (from each switch) to connect with external storage.
17	Support for Multiple Platform	Must have support for latest Windows and Linux Operating Systems
18	Power Supply / Power Modules	Must be configured for redundant power supplies, fans. Necessary PDUs to be provided. Power supplies, fans should be capable of reconfigure without manual intervention. The enclosure should be populated fully with power supplies of the available capacity with the vendor to cater the power requirement of offered blades. Power Supplies should support N+N redundancy.

31) Blade Server

Sr.No	Features	Specifications Required
1	CPU	64 Bit, 2 x Intel® Xeon® Processor E5-2690 v4 (2.6GHz, 14-core, 9.6 GT/Sec) Processor or higher
2	No. of CPUs required currently	Min. 28 cores using 2 processor sockets
3	Form Factor	Blade Format
4	Architecture	Intel
5	Cache L3	35 MB of L3 Chache
6	Chipset	Intel Chipset C600 or higher
7	Memory	256GB RAM (per processor socket) using DDR4 2133MHz Registered (RDIMM) memory and upgradeable up to 512GB or more Memory
8	Memory protection Support	Advanced Chipkill/ECC memory protection support, memory mirroring and memory sparing

9	SCSI Controllers	Integrated Hardware Raid Controller to supports Hardware Raid RAID 0 and 1
10	Controller for internal Hard disk devices	SAS/SCSI/SSD
11	Total internal hard disk bays	Two Small Form Factor hot-plug SAS/SATA/SSD drive bays
12	Disk Drives	2 x 600GB 6Gbps SAS/SCSI Hard Disk Drive with 10K rpm or more, If Required for Future Performance then Blade should support atleast up to 2 SSDs
13	Graphics Controller	16MB Flash Video Memory
14	Ethernet Adapter	Dual-port with TCP/IP Stateless Offloading (TOE), Wake on LAN,PXE 2 Offered servers must have 2*Onboard 10Gbps ports
15	Fiber HBA	1 X 16Gbps or higher FC HBA (dual port)
16	DIMM Slots	Minimum 16 slots or more
17	Management console Port	100BaseT Management LAN with web console access (additional licenses need to be supplied)
18	I/O Expansions	2 x PCI Express 3.0 slots
19	Power Supply	Blade Chassis must offer redundancy via N+N power supply
20	Failure Alerting Mechanism	The server should be able to alert impending failures on maximum number of components. The components covered under alerting mechanism should at least include Processor, Memory & HDD.
21	Systems / Server management capabilities	<p>Server should support systems management capabilities like</p> <ul style="list-style-type: none"> • Web-based out-of-band control • SSL and Support • Windows "blue screen" capture • Should support remote CD and Virtual floppy • Automatic Service Restart • Highly secure remote power on/off • System reset control • Support Event notification to system console • Remote connection to LAN console port via SSH and web browser with SSL encryption
22	Operating System Support	Latest Windows Server Operating System i.e. 2008 R2, 2012 and 2016 Ent/DataCenter/Std, Red Hat Enterprise Linux Server Version 6.7 or above,SUSE Linux Enterprise Server 11 or above and Vmware
23	USB	Min. 1 or more External & Min. 1 or more Internal for embedded hypervisor

24	Security	Should support Integrated Trusted Platform Module (TPM) to enable advanced cryptographic functionality, such as digital signatures and remote attestation
25	RAID features (support hardware or software RAID 0 & 1)	Mandatory. RAID controller for RAID 0, Raid 1 configurations with 512 MB cache memory
26	Redundant Cooling Fans	Should have Redundant Cooling Fans

32) Wireless AP

Sr.No	Specifications Required
1	Architecture
1.1	OpenFlow protocol capability to enable software-defined networking
1.2	The Access Point should have 2 nos. of 10/100/1000 Mbps ports
1.3	802.11ac AP should be able to power up using standards 802.3af/at POE input, and at the same time operate in full MIMO mode
1.4	APs should have Dual Radios to support 2.4 GHz 802.11n & 5GHz 802.11ac concurrent users. AP must support 4X4 MIMO with Four spatial stream SU-MIMO for up to 1.5Gbps wireless data rate to a single client device
1.5	AP should be able to handle minimum 250 concurrent users/devices per radio
1.6	AP should have integrated wireless intrusion protection & should provide necessary air-monitoring for spectrum analysis
1.7	AP should provide minimum 24 dBm radio transmit power for 2.4GHz and 24 dBm for 5GHz
1.8	APs can perform encryption / decryption on itself so as not to bottleneck the controller
1.9	SSID support : Minimum 16 or more BSSID per Radio
1.10	Data rate supported with automatic fallback
1.11	The access point should support 802.1q VLAN tagging
1.12	AP should be IPv6 ready from day one
1.13	Antenna: Eight integrated omni- directional antennas for 4x4 MIMO with peak antenna gain of 3.5 dBi in 2.4 GHz and 5.0 dBi in 5 GHz
1.14	Wi-Fi Alliance (WFA) certified 802.11a/b/g/n/ac
1.15	AP should support spectrum analysis to detect RF interference in indoor area
1.16	Should support transmit power tuning by 1 dB change in Tx power

1.17	AP should support polarization diversity to support smart devices in better way
1.18	AP should have -100 dB or better receiver sensitivity
1.19	Operating temp: 0° to 45° C and Humidity: 10 to 90% non-condensing
1.20	Mounting kit should be from the same OEM
1.21	AP should support Authentication via 802.1X, local authentication database, support for RADIUS and Active Directory
1.22	APs should have anti-theft mechanism through a locking system with mounting kit and meshed enclosure
1.23	Web User Interface (HTTP/S) ; CLI (Telnet/SSH), SNMP v1, 2, 3
1.24	Should be managed by Controller or standalone if required
1.25	Support FTP to propagate the configuration file & firmware to the Wi-Fi enabled device
1.26	FCC/CE, UL/IEC, EN 60601-1-2, Wi-Fi Alliance certified

33) Joy Stick

Sr. No.	Technical Description	
1	Components	Joystick
		Pushbuttons
		USB driver
		Direct X Gaming Control
2	Buttons	10 character numeric entry, 16 user definable buttons
3	Joystick Travel	X and Y axis +/- 18°
		Z axis +/- 40°
4	Joystick Material	Shaft: Stainless Steel
		Boot: Neoprene
		Handle: Glass-Filled Nylon
5	Jog/Shuttle Performance	Spring-loaded shuttle ring travel +/- 40°
		Smooth action knob rotates 360°
6	Push Button Lighting	High Efficiency LED
7	Pushbutton Material	Silicon
8	Power	USB Interface (SV DC)
9	Operating Temperature	-13° F – 185° F

10	Operating System	Windows 7, XP, Linux, Mac OSX
11	Regulatory	EN 55024: 1998, EN 55022
		FCC Part 15 Subpart B Class B
		RoHs compliant
12	Connector	USB 2.0 Type A Male, 5 m cable length maximum
13	Compliance	ONVIF
	Security	
	PasswordProtection	Required
	HTTPEncryption	Required
	IEEE 802.1X	Required
14	General	
	Operationaltemperature°C	0°C to 50 °C
	Humidity	0 to 80% RH non-condensing
	IP rating	IP66,NEMA 4X RatedOutdoorHousing
	Power	PoE, AC24V/ DC12V, 100- 230VAC
	Certifications	CE, UN/EN,FCC

34) NMS

Sr. No.	System Description & Minimum Requirement
1	Enterprise Management Solution should provide end-to-end, comprehensive, modular and integrated management of IT infrastructure components to maximize the availability of IT services and SLA performance. The management system needs to aggregate events and performance information from the domain managers and tie them to service definitions.
2	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). The proposed solution must be unified and also generate a comprehensive view of a service with real-time visibility into service status and identify the root cause of various infrastructure problems as well as prioritize resources based on impact. The proposed EMS solution must consist of the following core modules:

3	(1) Network Fault Management System
4	(i) Network Discovery & Reporting
5	(ii) Fault Analysis
6	(2) Configuration Management
7	(i) Advanced IP Services Management
8	(3) Service Level Management
9	(4) Performance Management
10	(i) Network Performance Management and Performance Reporting System
11	(ii) Flow-based Traffic Analysis System
12	(5) Server Performance Monitoring
13	(6) Database Performance Monitoring
14	(7) Web-Application Performance Monitoring
15	(i) Application Performance Monitoring System
16	(ii) End-User Experience Management System
17	(8) Helpdesk Management
18	(9) IT Asset Management
19	(i) Log Record Collection and Management
20	(10) Other Key Functional Requirements from NMS/EMS Suite
21	
22	<u>Network Fault Management System</u>
23	Provide fault and performance management of the network infrastructure that various services operate in. The proposed System will provide the following features:
24	(a) The Network Fault Management consoles must provide the topology map view from a single central console.
25	(b) The proposed Network Fault Management console must also provide network asset inventory reports and SLA reporting for the managed network infrastructure.
26	Network Discovery and Reporting:
27	(a) The proposed solution must automatically discover manageable elements connected to the network and map the connectivity between them.
28	(b) The proposed system must support multiple types of discovery including the following :
29	o IP range discovery – including built-in support for IPv6
30	o Import data - from pre-formatted files (IPs, ranges, strings or ports)
31	o Host Name discovery
32	o Service based discovery – including ping, FTP, JDBC, HTTP etc.

33	(c) 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.
34	(d) The system must be able to support mapping and modelling of the infrastructure grouped by network connectivity, physical location of equipment and user groups or departments.
35	(e) The modelling of network connectivity must be performed using standard or vendor-specific discovery protocols to ensure speed and accuracy of the network discovery.
36	(f) The system should support maps grouped by network topology, geographic locations of the equipments and user group/departments. These should help in understanding physical Network, virtual Network services and the relationships between them.
37	(g) It shall be possible to reduce the set of displayed devices in the topology views by flexible rules, based on the attribute contents stored with each device.
38	(h) The system must provide visualization tools to display network topology and device to device connectivity. The system must also be able to document connectivity changes that were discovered since the last update.
39	(i) The system must provide a user-configurable event to alarm mapping system that sets a differentiation that events do not necessarily need an alarm to be generated.
40	(j) The proposed solution must provide a detailed asset report, organized by vendor name and device, listing all ports for all devices
41	(k) The proposed solution must provide sufficient reports that identify unused ports in the managed network infrastructure that can be reclaimed and reallocated. The proposed management system must also intelligently determine which ports are operationally dormant.
42	(l) The proposed solution must poll all the ports to determine if any traffic has passed through
43	<u>Fault Analysis:</u>
44	(a) 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.
45	(b) The system must be able to 'filter-out' symptom alarms and deduce the root cause of failure in the network automatically.

46	(c) The system should support creating and monitoring of rising or falling thresholds with respect to basic key performance indicators for network, system and application infrastructures and provide immediate notification when service metrics fall outside the baselines.
47	(d) The proposed system must include the ability to monitor and visualize a virtualized system infrastructure by discovering and monitoring virtual machines and providing ability to depict the logical relationships between virtual servers and virtual machines.
48	(e) The proposed solution must detect virtual server and virtual machine configuration changes and automatically update the topology.
49	(f) The proposed system must support enhanced fault isolation to suppress alarms on logical VMs.
50	(g) The proposed solution must have the ability to collect data from the virtual systems without solely relying on SNMP.
51	(h) The proposed solution must support WMI for collecting and isolating Windows host issues.
52	(i) The proposed solution must support SSH polling method to collect and isolate Linux host issues.
53	(j) The proposed solution must support an architecture that can be extended to support multiple virtualization platforms and technologies.
54	
55	<u>Configuration Management</u>
56	(a) The system should be able to clearly identify configuration changes as root cause of network problems.
57	(b) The system should support secure device configuration capture and upload and thereby detect inconsistent “running” and “startup” configurations and alert the administrators.
58	(c) The proposed system should be able to administer configuration changes to network elements by providing toolkits to automate the following administrative tasks of effecting configuration changes to network elements :
59	o Capture running configuration
60	o Capture startup configuration
61	o Upload configuration
62	o Compare configuration
63	(d) The proposed solution must be able to perform real-time or scheduled capture of device configurations.

64	(e) The proposed solution must be able to store historical device configurations captured in the database and thereby enable comparison of current device configuration against a previously captured configuration as well as compare the current configuration against any user-defined standard baseline configuration policy.
65	(f) The proposed system should be able to monitor compliance & enforce change control policies within the diverse infrastructure by providing data & tools to run compliance reports, track & remediate violations, and view history of changes.
66	<u>Advanced IP Services Management:</u>
67	(a) The proposed solution should be able to monitor MPLS – VPNs by automating the provider connection resolution and monitoring the service health with an option to auto- provision service assurance tests to proactively calculate the availability of remote sites
68	(b) The proposed solution should be capable of managing the VPN Service including a complete Service Discovery of all the Devices and components that support each VPN. The solution must be able to automatically configure and provision site-to-site VRF Ping tests on each router that support VPNs to verify the ability to ping each other.
69	(c) The proposed solution should be able to support response time agents to perform network performance tests to help identify network performance bottlenecks.
70	(d) The proposed solution should be able to monitor QoS parameters configured to provide traffic classification and prioritization for reliable traffic transport.
71	(e) The proposed solution should provide the ability to discover, map & monitor multicast sources & participating routers wherein the system should be able to visualize the distribution tree in the topology map.
72	
73	<u>Service Level Management</u>
74	(a) The proposed service management system should 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.
75	(b) The proposed Service Dashboard should provide a high level view for executives and other users of the system. The system should 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.
76	(c) The system must breakdown SLA by the hour and should allow to drill down on each hour to report violations.

77	(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.
78	(e) The Users definition facility must support defining 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.
79	(f) 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.
80	(g) Root cause analysis of infrastructure alarms must be applied to the managed Business Services in determining service outages.
81	(h) SLA violation alarms must be generated to notify whenever an agreement is violated or is in danger of being violated.
82	(i) The system must 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.
83	(j) The system must provide the capability of Advanced Correlation for determining Service health, performing root cause analysis, and fault isolation. This must include applying complex Boolean logic on multiple attributes and infrastructure alarms.
84	(k) The system must provide a real time business services Dashboard that will allow the viewing of the current health of required services inclusive of real-time graphical reports.
85	<u>Deployment Features:</u>
86	(a) The Operations console and associated management system should be deployable in an optimized manner so as to keep the TCO down and also ensuring that the system is scalable and works in tandem with the primary management server.
87	(b) The overall EMS system should be deployed in an optimal gashing to as to keep TCO minimal and also ensure ease of maintainability.
88	(c) The security must be able to permit or restrict operator access to different areas of information based on user security rights assigned by the administrator.

89	(d) The system needs to support concurrent multi-user access to the management system, enabling multiple read-write access to different areas of the management domain and support operator workflows.
90	<u>Integrations:</u>
91	(a) The proposed NMS should provide unified workflow between the fault and performance management systems including bi-directional and context-sensitive report generation.
92	(b) The proposed system should integrate with the performance management system using a synchronized discovery and single sign-on for operators / administrators between them to enable unified Administration and ease of workflow.
93	(c) The system must support seamless bi-directional integration to helpdesk or trouble ticketing system.
94	(d) The proposed system should integrate with the helpdesk system by updating the Asset with information to support viewing history or open issues in helpdesk on the particular managed asset and associate an SLA to the ticket in the helpdesk.
95	(e) The proposed system should allow to attach/describe an asset identifier when submitting a helpdesk ticket.
96	
97	<u>Performance Management</u>
98	This provides a comprehensive end-to-end performance management across key parts of the network infrastructure. It should allow identifying trends in performance in order to avert possible service problems.
99	(a) The proposed performance management system shall integrate network, server and database performance information and alarms in a single console and provide a unified reporting interface for network components. The current performance state of the entire network & system infrastructure shall be visible in an integrated console.
100	(b) The proposed solution must scale to large networks while supporting a single web interface for access to reports. The system must support multiple locations and a distributed deployment for collection and monitoring. Primary instrumentation should exist in the data center.
101	(c) Provide SNMP device management of the network and server infrastructure.
102	(d) Provide flow-based reporting for network troubleshooting and capacity management.
103	(e) Provide Server Performance Monitoring as described
104	(f) Provide Database Performance Monitoring as described

105	(g) Provide Application Transaction Deep-Dive Monitoring for Web-Based Business Applications
106	(h) Provide End-User Response Time Monitoring for Browser-Based Applications
107	<u>Network Performance Management and Performance Reporting System:</u>
108	(a) The Network Performance Management consoles must provide a consistent report generation interface from a single central console.
109	(b) This central console will also provide all required network performance reports (including latency, threshold violations, packet errors, availability, bandwidth utilization etc.) for the network infrastructure.
110	(c) The proposed system shall collect, analyze and summarize management data from LAN/WAN, MIB-II interfaces and various servers for performance management.
111	(d) The proposed system shall identify over-and under-utilized links and assist in maximizing the utilization of current resources
112	(e) The proposed system shall provide Performance of Network devices like CPU, memory & buffers etc, LAN and WAN interfaces and network segments.
113	(f) It shall provide comprehensive health reporting to identify infrastructure in need of upgrades and immediate attention. Capacity planning reports shall identify network traffic patterns and areas of high resource utilization, enabling to make informed decisions about where to upgrade capacity and where to downgrade or eliminate capacity. It should also support 'What if' analysis and reporting to enable understanding the effect of growth on available network resources.
114	(g) The proposed system shall provide easy to read representations of health, utilization, latency and availability.
115	(h) It shall provide Real time network monitoring and Measurement of end-to-end Network performance & availability to define service levels and further improve upon them.
116	(i) The proposed system must have a report authoring capability built-in which will enable complete customization flexibility of performance reports for network devices and monitored servers.
117	(j) The proposed system should provide a real-time performance view for all the managed systems and networks along with the various threshold violations alarms in them. It should be possible to drill-down into the performance view to execute context specific reports.
118	(k) The tool should have the capability to configure different polling speeds for different devices in the managed infrastructure with capability to poll critical devices using 30 second poll periods.

119	(l) The system must provide the following reports as part of the base performance monitoring product out-of-the-box to help network operators quickly identify device problems :
120	o Trend Reports to present a single graph of a single variable (e.g. CPU utilization) for multiple devices across time. This would help network operators & IT managers plan for capacity and identify long drawn problems.
121	o Top N Reports to present a list of elements that exceed / fall below a particular threshold value. This would help network operators to identify elements that share specific performance characteristics (for example, to identify over utilized elements, you would run a Top-N report for all elements whose bandwidth utilization exceeds 90% or availability falls below 95%).
122	o What-If Reports to perform capacity planning by observing the effect of changes in capacity & demand (for example, the report should indicate what the bandwidth utilization would be if the demand was double the historical value).
123	o Executive Summary Report that gives an overall view of a group of elements, showing volume and other important metrics for the technology being viewed.
124	o Capacity Planning Report which provides a view of under-and-over-utilized elements.
125	o Service Level Reports to analyze & display service level information for an enterprise, region, department or business process. This report must show the elements with the worst availability and worst response time-the two leading metrics used to monitor SLAs.
126	o Health Reports to analyze trends calculate averages and evaluate the health of the infrastructure. With this information, operators should be able to determine how efficiently applications and systems are running, whether critical resources are available, and what capacity planning initiatives would make sense.
127	(m) The system must provide capability to measure & generate detailed performance reports for the following common TCP/IP applications:
128	o DHCP: Measure the round trip latency required to obtain an IP address.
129	o DNS: Measure the DNS lookup time including Latency and Packet Loss.
130	o FTP: Measure the time it takes to connect and transfer a file including Latency and Packet Loss.
131	o ICMP Ping: Measure round trip source to destination including Latency and Packet Loss.
132	o Latency and Packet Loss for :
133	(1) POP3

134	(2) SMTP
135	(3) TCP
136	(4) UDP Echo Test
137	(n) The proposed system should be able to auto-calculate resource utilization baselines for the entire managed systems and networks and allow user to set corresponding upper and lower threshold limits.
138	(o) The tool should provide Latency (both one way and round trip times) report for critical devices and links.
139	(p) The proposed system should use intelligent alarm de-duplication and automatic baselining capability to learn the behaviour of the managed infrastructure components over a period of time.
140	<u>Flow-based Traffic Analysis System:</u>
141	(a) The proposed traffic monitoring system must be able to track all flow of traffic on the network and identify malicious behaviour with all IP conversations.
142	(b) The proposed system must use non-intrusive monitoring to reduce the impact on the monitored network and improve scalability.
143	(c) The proposed system must provide details of applications, hosts, and conversations consuming WAN bandwidth to isolate and resolve problems.
144	(d) The proposed system must provide eight-hour, daily, weekly, monthly, yearly, or customizable reporting time periods.
145	(e) The bidder must provide a solution for collecting Flow data from multiple devices simultaneously across the network. The solution must provide the following Flow-based metrics:
146	o Utilization
147	o Flow Count
148	o IP conversation pairs
149	o Router/interface
150	o Protocol breakdown by host, link, ToS or conversation.
151	o IPv6 addresses
152	(f) The proposed solution must be able to monitor and report on a variety of unique protocols (used in the overall deployed solutions) per day and display utilization data for each protocol individually. This capability must be available for each monitored interface uniquely.
153	(g) The proposed solution must keep historical rate and protocol data for a minimum of 12 months (most recent) in its current long term operating database. All data in that database must have a maximum 15 minute window granularity.

154	(h) The proposed solution must keep historical rate and protocol data for a minimum of 30 days (most recent) in its short term operating database. All data in that database must have a maximum 5 minute window granularity.
155	(i) The system must support the ability to specify which hosts, conversations, IP ports, custom ToS matches and interfaces are included or excluded from the web based report.
156	(j) The system must support the ability to create reports that allow the user to search all IP traffic over a specified historical period, for a variety of conditions. The system must have the ability to search all IP traffic without loss or exclusion of any traffic. The system must support search within this period for the following at minimum;
157	o Search for any traffic using a specific configurable destination port, or port range.
158	o Search for any traffic using a specific autonomous system (AS) number.
159	o Search for any traffic using a specific IP subnet mask.
160	o Search for any traffic using a specific IP ToS bit.
161	o Search for any clients or servers communicating with more than a specific number of other unique clients or servers.
162	o Search for any clients or servers that are experiencing more than a specified number of TCP resets per hour within a specified reporting period.
163	o Search for any IPv4 or IPv6 conversation across the entire network.
164	o Search for any protocol in use by a specific host, interface or list of hosts or interfaces.
165	(k) The proposed system must be capable of automatically detecting anomalous behaviour such as virus attacks or unauthorized application behaviour. The system should analyze all Flow traffic and alert via SNMP trap and syslog of any suspicious activity on the network.
166	(l) Flow collection systems must support a minimum of 5 million flows per minute and be capable of storing gathered information in a common database where all long term reporting information is held.
167	(m) The proposed system must spot potential bottlenecks with color-coded indicators for interfaces that breach defined thresholds and durations
168	
169	<u>Server Performance Monitoring</u>
170	(a) The proposed server performance management system shall integrate network performance management systems and provide the unified performance state view in a single console.
171	(b) The current performance state of the entire network and server infrastructure shall be visible in an integrated console.

172	(c) The proposed tool must provide lightweight server agents to ensure availability and performance for target server nodes and deliver scalable, real-time management of critical systems.
173	(d) The proposed tool should be able to monitor various operating system parameters such as processors, memory, files, processes, file systems, etc. where applicable, using agents on the servers to be monitored.
174	(e) It should be possible to configure the operating system monitoring agents to monitor based on user-defined thresholds for warning/critical states and escalate events to event console of enterprise management system.
175	(f) The proposed tool should integrate with network performance management system and support operating system monitoring for various platforms including Windows, UNIX and Linux.
176	(g) It should also be able to monitor various operating system parameters depending on the operating system being monitored yet offer a similar interface for viewing the agents and setting thresholds.
177	(h) The proposed tool should be able to gather information about resources over a period of time and provide historical performance and usage information through graphical reports, which will quickly show performance trends.
178	(i) The proposed solution should support management following parameters:
179	o Processors: Each processor in the system should be monitored for CPU utilization. It should compare Current utilization against user specified warning and critical thresholds.
180	o File Systems: Each file system should be monitored for the amount of file system space used, which should be compared to user-defined warning and critical thresholds.
181	o Log Files: Logs should be monitored to detect faults in the operating system the communication subsystem, and in applications. System agents should also analyze log files residing on the host for specified string patterns.
182	o System Processes: System agents should provide real-time collection of data from all system processes. Using this it should help identify whether or not an important process has stopped unexpectedly. It should provide an ability to automatically restart Critical processes.
183	o Memory: System agents should monitor memory utilization and available swap space and should raise an alarm in event of threshold violation.
184	Feature must be available Database Performance Monitoring

185	(a) The proposed database performance management system shall integrate network and server performance management systems and provide the unified view of the performance state in a single console.
186	(b) It should be able to automate monitoring, data collection and analysis of performance from single point.
187	(c) It should also provide the ability to set thresholds and send notifications when an event occurs, enabling database administrators (DBAs) to quickly trace and resolve performance-related bottlenecks.
188	(d) Database performance management solution for Distributed RDBMS must include hundreds of predefined scans for monitoring various database, operating system and network resources. This should minimize the need to write and maintain custom scripts. If a special monitoring situation exists, you can modify an existing script to meet your requirements.
189	(e) The event management system must send alerts for an array of server conditions, including inadequate free space, runaway processes, high CPU utilization and inadequate swap space.
190	(f) The database performance management solution must support historical archive store for performance information in a compressed time-series form. DBAs should be able to drill down through layers of data to discover the cause of a condition occurring with the databases, operating system or network. These historical reports must also be usable to perform trend analysis and capacity planning.
191	(g) The database performance management solution must have a console to enable users to monitor, analyze and take corrective action from a centralized point. It should also include a platform-independent, browser-based console to monitor performance from remote locations.
192	
193	<u>Web-Application Performance Monitoring</u>
194	<u>Application Performance Monitoring System:</u>
195	(a) The proposed solution must determine if the root cause of performance issues is inside the monitored application, in connected back-end systems or at the network layer from a single console view.
196	(b) The proposed solution must proactively monitor 100% of real user transactions, detect failed transactions, gather evidence necessary for triage and diagnosis of problems that affect user experiences and prevent completion of critical business processes.
197	(c) The proposed solution must provide deeper end-to-end transaction visibility by monitoring at transactional level.

198	(d) The proposed solution must provide a single view that shows entire end-to-end real user transaction and breaks down times spent within the application components, SQL statements, backend systems and external 3rd party systems.
199	(e) The proposed solution must be able to provide root-cause probability graphs for performance problems showing the most probable root-cause area within application infrastructure.
200	(f) The proposed solution must support any combination of operating platforms that support JDKs higher than 1.2 or Application Server (or .NET v1.1 and above) with a single methodology.
201	(g) The proposed solution must provide a real-time application topology map to triage and quickly pinpoint the component causing a performance bottleneck in the end-to-end transaction flow.
202	(h) The proposed solution must gather available performance indicator metrics from all within real-time production environments and real user transactions 24x7 with minimal overhead on monitored applications without sampling.
203	(i) The proposed solution must provide for easy dynamic instrumentation of application code, i.e. be able to enhance out of the box monitoring with extra monitoring definitions without having to restart application or JVM.
204	(j) The proposed solution must allow monitoring granularity of no more than 15 seconds for all transactions.
205	(k) The proposed solution must be able to detect production Memory Leaks from mishandled Java Collections and Sets and isolate exact component creating leaking Collection or Set (or .NET Memory Leaks within the CLR).
206	(l) The proposed solution must provide real-time monitoring of resource utilization like JVM memory usage, Servlets, EJB pools, DB connection pools and Threads.
207	(m) The proposed solution must be able to identify socket and file Input / Output activity from the application.
208	(n) As a means of detecting poorly performing SQL, the solution must be able to proactively record all SQL calls, and report on the slow performing ones.
209	(o) The proposed solution must monitor performance of all stored procedures being executed from within the Java/.NET application.
210	(p) The solution should have provision for automatic transaction discovery, for example by setting up some bounding parameters to describe transactions like the web site, the language, and parameters (such as post, query, and cookies).

211	(q) The proposed solution must provide ability to monitor performance of applications up to the method level of execution (Java/.Net method) 24x7 in production environments with negligible impact on monitored application.
212	(r) The proposed solution must be able to report on any application errors occurred while executing application functionalities and pinpoint exact place of error within the transaction call stack.
213	(s) The proposed solution must provide for at least 2 levels of thresholds which can be set on alerts and provide for actions so that alerts can automatically trigger other processes when thresholds are breached. The proposed solution must not necessitate any changes to application source code.
214	(t) The proposed solution must proactively identify any thread usage problems within applications and identify stalled (stuck) threads.
215	(u) The proposed solution should allow SQL statement normalization by aggregating hundreds of related SQL statements into a single performance metric using regular expressions and pattern matching.
216	(v) The proposed solution must monitor individual web service and performance transaction debugging for web services. The proposed solution must also monitor web services across multiple processes (cross JVM tracing).
217	End-User Experience Management System:
218	(a) The proposed solution should measure the end users' experiences based on transactions.
219	(b) The solution should be deployable as an appliance-based system acting as a passive listener on the network thus inducing zero overhead on the network and application layer.
220	(c) The proposed system must be able to detect user impacting defects and anomalies and reports them in real-time:
221	o Slow Response Time
222	o Fast Response time
223	o Low Throughput
224	o Partial Response
225	(d) The proposed system must be able to provide the ability to create user groups based on application criteria or location and link user ids to user names and user groups.
226	(e) The proposed system must be able to provide user usage analysis and show how user's success rate, average time and transaction count has changed over a specific period of time such as current week versus previous week.

227	(f) The proposed system must be able to provide the ability to detect and alert when users experience HTTP error codes such as 404 errors or errors coming from the web application.
228	(g) The proposed system must be able to provide root-cause probability graphs for performance problems showing the most probable root-cause area within application infrastructure.
229	
230	<u>Helpdesk Management</u>
231	(a) The proposed Helpdesk Management System must provide support for various defined ITIL processes.
232	(b) It must provide flexibility of logging, viewing, updating and closing incident manually via web interface. The web interface console would also offer power-users tips.
233	(c) It must provide seamless integration to log incident automatically via system and network management.
234	(d) It must provide classification to differentiate the incident via multiple levels/tiers of categorization, priority levels, severity levels and impact levels.
235	(e) It must be able to provide flexibility of incident assignment based on the workload, category, location etc.
236	(f) Each escalation policy must allow easy definition on multiple escalation levels and notification to different personnel via window GUI/console with no programming.
237	(g) The escalation policy would allow flexibility of associating with different criteria like device/asset/system, category of incident, priority level, organization and contact.
238	(h) It must provide web-based knowledge database to store useful history incident resolution.
239	(i) It must contain built-in knowledge tools system that can provide grouping access on different security knowledge articles for different group of users.
240	(j) It must integrate with EMS event management and support automatic problem registration, based on predefined policies.
241	(k) It must be able to log and escalate user interactions and requests.
242	(l) It must provide status of registered calls to end-users over email and through web.
243	(m) It must have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues.
244	(n) It must have the ability to track work history of calls to facilitate troubleshooting.

245	(o) It must support tracking of SLA (service level agreements) for call requests within the help desk through service types.
246	(p) It must be capable of assigning call requests to technical staff manually as well as automatically based on predefined rules, and should support notification and escalation over email, web etc.
247	(q) It must have an integrated CMDB for better configuration management & change management process.
248	(r) It must have a top management dashboard for viewing the helpdesk KPI in graph & chart formats.
249	(s) It must support remote management for end-user & allow analysts to do the desktop sharing for any system located anywhere, just connected to internet.
250	
251	<u>IT Asset Management</u>
252	(a) The proposed solution shall provide inventory of hardware and software applications on end-user desktops including information on processor, memory, operating system, mouse, key board of desktops etc. through agents installed on them.
253	(b) It shall have reporting capabilities; provide predefined reports and the possibility to create customized reports on data in the inventory database.
254	(c) It shall provide facility for user defined templates to collect custom information from users at desktops / workstations.
255	(d) It shall provide facility to recognize and provide inventory for custom applications on desktops.
256	(e) It shall provide facility for queries and automated policies to be set up on existing data in database and permit scheduling of data collecting engines to pick up the data at defined intervals.
257	(f) It shall support UNIX, Linux, Apple OSX apart from Windows environment for inventory management.
258	(g) It shall provide file management capabilities for the monitored systems: it should be able to find out specific files and directories on a workstation based on queries.
259	(h) It shall allow collection / restoration of configuration files at remote desktops, using which standardization of configuration can be achieved of all the desktops. e.g. configuration files / settings related to a particular application which involves changing of registry parameters and configuration files
260	(i) It shall display the names of the applications being monitored for usage.

261	(j) It shall support dynamic grouping for enabling assets to be grouped dynamically based on some pre-defined criterions. Like a Group can be able to display how many and which computers have a specific application installed. As and when a new computer get the new application installed it should dynamically get added to the group. Another Example: If a hardware upgrade is taking place, two Dynamic Groups can be created; one to reflect the computers not yet upgraded, the other group, the upgraded computers.
262	(k) It shall be able to use the query tool to identify specific instances of concern like policy violation (presence of prohibited applications/games and old versions etc.), inventory changes (Memory change etc) and accordingly it could perform several actions as reply. These actions could be:
263	o Sending an email
264	o Sound an alarm
265	o Adding the computer to a Group
266	o Message to scroll on Monitor screen of the administrator
267	(l) It shall provide the facility to track changes by maintaining history of an asset. History period shall be configurable.
268	(m) It shall provide a web-based console.
269	(n) It shall be able to collect inventory from add/remove program functionality in Windows environment.
270	(o) It shall support event policies such that pre-defined actions can be triggered when key events occur such as software license violations etc.
271	(p) It shall provide an option to share the database with the proposed service desk solution such that it can leverage information available in Asset management database.
272	(q) It shall support software Package Creation using Generic scripts. The software delivery software should provide a Wizard for auto script builder.
273	(r) It shall support reinstall after crash for the systems which crashes and requires the same set of software after it has been serviced. It should identify such machines and would automatically install the required software.
274	(s) It shall have the intelligence to install a required set of software for any computers added in a particular department/group based on the predefined criteria.
275	(t) It shall ensure that software deliveries run in the background ensuring that the end user cannot click any buttons or change settings.
276	(u) It shall support software distribution to Dynamic groups. Administrators should have the ability to create distribution groups based on relevant criterion. Dynamic Groups to be built using search arguments presented to an asset and inventory management solution.

277	(v) It shall support a wide variety of clients. This includes all desktop systems, including Windows Server and Desktop operating systems, various flavours of UNIX & Linux. It shall also provide inventory collection functionality from mobile operating platforms such as Windows Mobile etc.
278	(w) It shall offer several levels of security for remote control, ranging from defining users with specific rights to requiring a specific IP address and local confirmation before a remote session is enabled.
279	(x) It shall have the ability to perform diverse tasks on multiple remote systems simultaneously, view a host machine from multiple viewers, transfer control between users and allow a host machine to initiate a connection to a viewer.
280	(y) It shall provide users the ability to record a session of remote control for later playback.
281	(z) It shall provide chat functionality between remote control viewer and host as well as a file transfer utility for drag and drop transfer of files between remote control viewer and host.
282	(za) It shall support remote reboot functionality
283	(zb) It shall provide the facility to throttle the bandwidth used by the tool while communicating over the network if required.
284	(zc) It shall provide the facility for encrypting the authentication traffic and additionally encrypt viewer/host traffic as well.
285	(zd) It shall support personalized global address book.
286	(ze) It shall support centralized session management.
287	(zf) It shall provide Windows integrated authentication as well as its own application based authentication option to choose from the agent installed.
288	(zg) It shall manage and preserve desktop software configuration, such as user settings, preferences and data so that it helps in seamless migration or upgrades to new OS such as Vista/Windows 7 etc.
289	(zh) It shall provide a web access console for a comprehensive view of asset management information, including: Computers, Software, Hardware details.
290	(zi) It shall provide support for ITIL support and integration with tools like service desk/helpdesk.
291	(zj) It shall collect and report information such as antivirus signature data and information on host based intrusion prevention system agents.
292	(zk) It shall provide Request Management functionality.
293	(zl) It shall provide Software Inventory features.
294	Log Record Collection and Management
295	(a) The system shall provide a graphical user interface/wizard to rules for normalizing custom log sources or modifying existing integrations

296	(b) The system shall provide automated update mechanism for Content (product integrations and reports). This process shall occur seamlessly and transparently without any customer intervention as part of the subscription update process.
297	(c) The system shall support the following methods for log collection :
298	o Windows Management Instrumentation (WMI) for remote collection from the Windows Event Log
299	o Syslog
300	o Raw Flow data
301	o Text Log (flat file)
302	(d) The system shall provide a mechanism to monitor the current status and relative health of the logging infrastructure.
303	(e) The system shall have the capability to drag and drop building of custom queries & reports.
304	(f) The system shall be capable of operating at a sustained 3000 EPS per collection device. The system shall provide the ability to scale to higher event rates by adding multiple collection devices.
305	(g) The system shall have the capability for updates delivered and applied via an update service provided by the vendor to keep the system up-to-date. This includes the agents and it should be pushed centrally without having to reinstall the agents.
306	(h) The system shall have a secure and preferably embedded log repository to store logs that does not require separate database expertise to administer and manage.
307	<u>Other Key Functional Requirements from NMS/EMS Suite</u>
308	(1) The solution should provide all the EMS modules for Network, Server, Application Performance monitoring and Helpdesk to work in tandem and pre-integrated (Out-of-Box integration)
309	(2) The proposed system should provide correlation between Network, Server and Application automatically.
310	(3) The proposed system should provide Business Service Management functionality to track Service quality by logically grouping Network, Server and Application components.
311	(4) The solution must provide way to define key performance indicators (KPIs) within the Business Service Management module.
312	(5) The solution must provide SLA measurement module to track service quality from both Availability and Performance perspective.
313	(6) The solution must provide pre-defined reports.

314	(7) The solution must provide custom data widgets to create custom dashboards for the teams, so as to visualize and collect real time and historical data from custom widgets.
315	(8) The solution must provide multi-tenancy. Eg. Database Admin should have access to Database monitors only.
316	(9) To make operations efficient, a consolidated dashboard with strong event correlational functionality is desired, to aggregate events from network, servers, and application monitoring solutions and correlate them to identify root cause. This should also allow to automatically prioritize issues based on business impact to citizen services and seamlessly route to appropriate team will all available information.
317	(10) Once problem is detected, the root cause determined by the bridge and a ticket should be created to focus on remediation. Using run book automation the fix should handle automatically or through escalation to a Subject Matter Expert. Using Run Book Automation, the operators should be able to apply a fix with or without manual intervention based on a pre-defined fix available for the cause event
318	(11) The reporting component of EMS must provide out-of-the-box IT performance KPIs and scorecards for key personas at the customer and program management office end. IT should be feasible to have historical data to highlight improvements and negative trends.

35) 48 port Switch

Sr. No.	System Description & Minimum Requirement
1	<u>Architecture</u>
2	Shall be 1U 19" Rack Mountable
3	Shall be configured with dual, hot-swappable power supplies
4	Shall be configured with dual, fan tray slots which shall support front-to-back airflow
5	48 10Gb Ethernet SFP+ ports
6	6 X fixed 40-Gigabit QSFP+ slots
7	4 GB SDRAM & 1GB Flash with packet buffer size of 12MB
8	Shall have switching capacity of 2 Tbps for non-blocking performance on all 10G/40G ports
9	Shall have up to 1.5K Mpps switching throughput delivering wire speed forwarding on all 10G/40G ports
10	Shall provide Latency of < 1 μs (64-byte packets)
11	<u>Resiliency</u>

12	Shall have the capability to extend the control plane across multiple active switches making it a virtual switching fabric, enabling interconnected switches to perform as single Layer-2 switch and Layer-3 router
13	Shall support virtual switching fabric creation across multiple switches using 10G or 40G Ethernet Links. Bidder must provide 2*40Gbps ports cables (if any) to create virtual switching fabric across switches.
14	IEEE 802.1D Spanning Tree Protocol, IEEE 802.1w Rapid Spanning Tree Protocol and IEEE 802.1s Multiple Spanning Tree Protocol
15	IEEE 802.3ad Link Aggregation Control Protocol (LACP)
16	Virtual Router Redundancy Protocol (VRRP) to allow a group of routers to dynamically back each other up to create highly available routed environments
17	Graceful restart for routing protocol
18	Shall provide hitless software upgrade with single-unit In Services Software Upgrade (ISSU) and hitless patching of modular OS
19	<u>Layer 2 and Convergence Features</u> <u>(any additional licenses required shall be included)</u>
20	Shall support up to 4,000 port or IEEE 802.1Q-based VLANs
21	MAC address table size of minimum 128000 entries
22	Shall have the capability to monitor link connectivity and shut down ports at both ends if uni-directional traffic is detected, preventing loops
23	Shall support Jumbo frames on GbE and 10-GbE ports
24	Internet Group Management Protocol (IGMP)
25	IEEE 802.1AB Link Layer Discovery Protocol (LLDP)
26	Multicast VLAN to allow multiple VLANs to receive the same IPv4 or IPv6 multicast traffic
27	Data Center Bridging (DCB) protocols support including IEEE 802.1Qbb Priority Flow Control (PFC), Data Center Bridging Exchange (DCBX), and IEEE 802.1Qaz Enhanced Transmission Selection (ETS) for converged applications
28	FCoE support on all 10G SFP+ ports including expansion, fabric, trunk VF and N ports, aggregation of E-port, N-port virtualization
29	Fabric services support including name server, registered state change notification, and login services; per-VSAN fabric services, FSPF, soft and hard zoning, Fibre Channel traceroute, ping, debugging, and FIP snooping
30	Transparent Interconnection of Lots of Links (TRILL) support to increase the scale of enterprise data centers
31	EVB/VEPA support to provide connectivity into the virtual environment for a data center-ready environment
32	<u>Layer 3 Features</u> <u>(any additional licenses required shall be included)</u>
33	Static Routing for IPv4 and IPv6

34	RIP for IPv4 (RIPv1/v2) and IPv6 (RIPng)
35	OSPF for IPv4 (OSPFv2) and IPv6 (OSPFv3)
36	IS-IS for IPv4 and IPv6 (IS-ISv6)
37	Border Gateway Protocol 4 with support for IPv6 addressing
38	Policy-based routing
39	Multiprotocol Extensions for BGP-4
40	<u>QoS and Security Features</u>
41	Access Control Lists for filtering traffic to prevent unauthorized users from accessing the network
42	Congestion avoidance using Weighted Random Early Detection (WRED)
43	Powerful QoS feature supporting Strict Priority Queuing (SP), Weighted Fair Queuing (WFQ), Weighted Deficit Round Robin (WDRR), SP+WDRR, Ingress Rate Limiting
44	IEEE 802.1X Port Based Network Access Control
45	DHCP Snooping support including Option 82
46	Port security, Directed Broadcast Control
47	<u>Management Features</u>
48	Configuration through secure command-line interface (CLI) over Telnet and SSH
49	1 RJ-45 serial console port and 1 RJ-45 out-of-band management port
50	SNMPv1, v2, and v3
51	sFlow (RFC 3176) or equivalent for traffic analysis
52	FTP and TFTP support
53	Port mirroring to enable traffic on a port to be simultaneously sent to a network analyzer for monitoring
54	RADIUS or TACACS+ for switch security access administration
55	Network Time Protocol (NTP) or equivalent support
56	Shall have Ethernet OAM - Connectivity Fault Management (IEEE 802.1AG) and Ethernet in the First Mile (IEEE 802.3AH) capability
57	Shall support OpenFlow protocol capability to enable software-defined networking (SDN) from Day 1
58	Shall allow the separation of data (packet forwarding) and control (routing decision) paths, to be controlled by an external SDN Controller, utilizing Openflow protocol
59	<u>Environmental Features</u>
60	Shall provide ROHS Compliance
61	Shall be capable of supporting both AC and DC Power inputs

36) UTM Box

Specifications	Mandatory/Optional
General Requirements:	
The Firewall must be appliance based and should facilitate multi-application environment which should support current network traffic as well as future growth	Mandatory
The Firewall should be ICSA Labs certified for ICSA 4.0 and EAL 4 + / NDPP certified, if not the same model	Mandatory
The Firewall should belong to a family of products that attains NSS/NIST Approved Certification and attains IPv6 Ready Phase 2 & IPv6 Certification	Mandatory
The platform should be based on security-hardened, purpose built operating system architecture that is optimized for packet and application level content processing	Mandatory
Be proprietary to prevent inheriting common OS vulnerabilities and should Resided on flash disk for reliability over the hard disk	Mandatory
Should provide a Http, Https, SSH, Telnet, SNMP based management console for managing and configuring various components of the appliance	Mandatory
The proposed system should be able to facilitate administration audit by logging detailed activities to event log for management, configuration changes, updates which also enable Admin to boot firmware on the earlier revision / configuration in case of any errors	Mandatory
The administrator authentication shall be facilitated by local database, PKI & remote server such as Radius, LDAP, AD and TACS+	Mandatory
The Firewall system should have provision of Web Content Filter, Application Control, Antivirus systems and Intrusion Prevention in the same solution	Mandatory
Be proprietary to prevent inheriting common OS vulnerabilities and should Resided on flash disk/Hard disk	Mandatory
Networking & System Performance Requirements:	Mandatory
The Firewall should support a minimum of 16 x GE RJ45, 12x GE SFP (2 published), 2x10G SFP+ Interfaces	Mandatory
The platform should support the standards based Link aggregation technology (IEEE 802.3ad) to achieve higher bandwidth	Mandatory
Should support automatic ISP failover as well as ISP load sharing	Mandatory
The Firewall should support Static, Policy Base, Identity based, Multicast routing and Dynamic routing for RIP1 & 2, OSPF, OSPFv3, BGP4, ISIS, RIPv4	Mandatory
The Firewall should support Static, Policy Based, and Multicast routing	Mandatory
The Firewall should support throughputs of 50 Gbps or better for large packets & 30 Gbps with UDP 64bytes packets	Mandatory
The firewall should support throughput of atleast 20Gbps of AES - IPSEC VPN and should be H/W accelerated	Mandatory

should support concurrent session atleast 10 Mil	Mandatory
Should support new session per second atleast 2,60,000 or above	Mandatory
Should support and IPS throughput of 8GBPS with recommendation profile & atleast 4Gbps with production env. profiles or better with enterprise mix	Mandatory
Firewall Requirements:	Mandatory
The Firewall should support deployment modes as; "Route Mode" or "Transparent Mode" and support web proxy/ssl proxy	Mandatory
The firewall shall be able to handle VoIP traffic securely with "pinhole opening" and support SIP, SCCP, MGCP and H.323 ALGs	Mandatory
The Firewall should support Stateful inspection with optional Policy based NAT (Static OR Dynamic)	Mandatory
The Firewall should support Inbound Port Forwarding with inbound Load Balancing if servers are running in high availability (layer 4)	Mandatory
Should support IPv6 ACL to implement security Policy for IPv6 traffic	Mandatory
All internet based applications should be supported for filtering like Telnet, FTP,SMTP, HTTP, DNS, ICMP, DHCP, RPC,SNMP, BGP, IMAP, NFS etc	Mandatory
Should be able to inspect HTTP and FTP traffic when these are deployed using nonstandard port(i.e when HTTP is not using standard port TCP/80)	Mandatory
The Firewall should support deployment of Virtulization at least for 10 virtual context from the day one without any additional cost / licenses	Mandatory
Virtual context must have all security features for use for every single firewall	Mandatory
IPSEC VPN Requirements:	Mandatory
The IPSEC VPN and SSL VPN capability shall minimally attain Internet Computer Security Association (ICSA) Certification or equivalent certification	Optional
The proposed system shall support industry standards, L2TP, PPTP, IPSEC, and SSL VPN without additional cost for license or solution for VPN client	Optional
Firewall must have atleast 1000SSL VPN client & 5000 IPsec VPN client in Route mode from the day 1	
IPSEC (DES, 3DES, AES) encryption/decryption and SSL encryption/decryption	Mandatory
The system shall support IPSEC site-to-site VPN and remote user VPN in transparent mode without any additional cost for VPN clients	Mandatory
Application control	Mandatory
Atleast 2200+ application signature must be there & it should able to understand welknown application like P2P, Voice, etc without any dependency on the ports	Mandatory
Solution must provide option to create custom signature for applications	Mandatory
Solution should have application throughput of atleast 6Gbps or higher	Mandatory
Threat Protection	Mandatory

Firewall must able to scan http, https, IMAP, IMAPs, FTP, FTPs, POP, POPs, SMTP, SMTPs & MAPI protocols with AV signatures	Mandatory
Threat prevention throughput must be atleast 2.2Gbps after enabling AV, Appcontrol & IPS signatures	Mandatory
SSL VPN Requirements	Mandatory
The Firewall should be integrated solution and there should be no user based licensing for SSL VPN	Mandatory
SSL VPN must have atleast throughput of 3.5 Gbps or higher	Mandatory
The Firewall should support for TWO modes of SSL VPN:1.Web mode,2.Tunnel mode	Mandatory
Traffic Shaping Requirements	Mandatory
The proposed system should have integrated Traffic Shaping functionality including these features:	Mandatory
capable of enable and disable traffic shaping per firewall policy	Mandatory
capable of setting guarantee bandwidth and maximum bandwidth per firewall policy	Mandatory
ability to Tag and Pass Differentiated Service tagging	Mandatory
High Availability Requirements (Future need):	Mandatory
The HA solution should support stateful session maintenance in the event of a fail-over to a standby unit/s.	Mandatory
The HA solution should support both Active/Active and Active/Passive load balancing	Mandatory
The High Availability should be supported in the Firewall from the day one and without any extra license	Mandatory
Network Intrusion Detection & Prevention System Requirements:	Mandator
The IPS capability shall minimally attain Internet Computer Security Association (ICSA) or equivalent standard certification	Optional
Should have a built-in Signature and Anomaly based IPS engine on the same unit and Anomaly based detection should be based on thresholds	Mandatory
Able to prevent denial of service and Distributed Denial of Service attacks on signature	Mandatory
Administrator shall be able to configure DoS policies that are used to associate DoS settings with traffic that reaches an interface based on defined services, source and destinations IP/Range	Mandatory
Configurable IPS filters to selectively implement signatures based on severity, target (client/server), protocol, OS and Application types	Mandatory
Supports at least 6000+ attack signature and should be automatic updates directly over the internet for the newly discovered attacks	Mandatory
Security check updates do not require reboot of the unit	Mandatory

Supports attack recognition inside IPv6 encapsulated packets	Mandatory
Supports user-defined signatures with Regular Expressions	Mandatory
Web & Application Content Filtering System Requirements:	Mandatory
The proposed system should have integrated Web Content Filtering solution without external solution, devices or hardware modules	Mandatory
URL database should have atleast 250+ million sites and 70 + categories in 60+ languages	Mandatory
The proposed solution should be able to enable or disable Web Filter per firewall policy or based on firewall authenticated user groups for both HTTP and HTTPS	Mandatory
Should blocks web plug-ins such as ActiveX, Java Applet, and Cookies	Mandatory
Shall include Web URL block, Web keyword block, Web Exempt List	Mandatory
The proposed solution should be able to replace the web page when the web page matches the Web Filtering blocking criteria.	Mandatory
The proposed solution shall be able to identify, retrieve and rate the actual URL of the cached content commonly available in search engines such as Yahoo and Google.	Mandatory
The proposed solution shall be able to identify, retrieve and rate the image files from image search engines and take appropriate action as configured	Mandatory
The solution shall allow administrators to creat mutiple new local URL filtering categories besides dynamic categories	Mandatory
The solution shall allow administrators to override Online URL Database ratings with local ratings setting	Mandatory
Many web sites use HTTP redirects legitimately; however, in some cases, redirects may be designed specifically to circumvent web filtering, as the initial web page could have a different rating than the destination web page of the redirect. The solution shall be able to rate redirected sites as well.	Mandatory
The solution shall be capable of rating URLs by domain and IP address which sends both the URL and the IP address of the requested site for checking, providing additional security against attempts to bypass the rating system.	Mandatory
Data Leak Prevention Requirements:	Mandatory
Should have the ability to prevent data loss through SMTP, FTP, HTTP, HTTPS & IM and using any application	Mandatory
Full archive features for http, https, ftp, ftps & email protocols	Mandatory
Should have built in pattern database and option to configure new patterns as and when required	Mandatory
Anti-BOT, Mobile Security & ATP	Mandatory
Solution must have facility to integrate with cloud based ATP solution for future use	Mandatory

ATP solution must be from same OEM	Mandatory
It also must have facility to block Bot attacks & also must scan Mobile devices security from day 1	Mandatory
Zero day prevention or Sandboxing	
Proposed solution must integrate with Cloud based sandboxing solution for zero day protection	Mandatory
Proposed Sanbox solution must have different VM for scanning of file to check for Zero day.	Mandatory
Certification	Mandatory
Firewall family must be recommended by NSS DC-IPS report of 2016	Mandatory
Proposed solution must be in a challenger/Leader quadrant of Gartner Enterprise Firewall for atleast last 3 consecutive years	Mandatory
Hardware	Mandatory
Firewall must have atleast 16 Gb of RAM from day 1	Mandatory
Firewall must have atleast 200GB of disk for real time monitoring purpose	Mandatory
Firewall must have redundant power supply from the day 1	Mandatory