

F. No. I-45024/21/2012/IT/MHA-Prov.I  
Bharat Sarkar/Government of India  
Griha Mantralaya/Ministry of Home Affairs  
PM Division/Prov. I Desk

\*\*\*\*\*

26, Man Singh Road, Jaisalmer House  
New Delhi, Dated 29<sup>th</sup> November, 2012

To

The Director General,  
ITB Police, CGO Complex,  
Lodhi Road, New Delhi

*Draft No. 1430 Prov. I  
30/11/12*


**Subject : QRs for Hardware and software of WAN of ITBP**

33 Nos of QRs for Hardware and Software of WAN (except the QRs mentioned in Annexure 'I') of ITBP as per Annexure have been accepted by the Competent Authority in MHA. The draft QRs mentioned in the Annexure 'I' are universally acceptable and do not require approval from this Ministry.

2. ITBP may take procurement action strictly as per the laid down Technical Specifications/QRs.

Encl: As above

Yours faithfully,



(Smt. S. B. Nanda)  
Under Secretary to the Govt. of India  
Tel : 23381278

**DIRECTORATE GENERAL  
CENTRAL RESERVE POLICE FORCE  
CGO COMPLEX, LODHI ROAD, NEW DELHI-110003**  
\*\*\*\*\*

**Subject: QRs for Software/Hardware of WAN of ITBP**

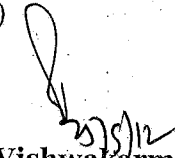
Kindly refer to MHA UO No. I-45024/21/2012-IT-981, Prov-1 dated 03.08.2012 & 14.08.2012 directing to CRPF for formulating/revising Qualitative Requirements of Hardware & Software required for ITBP Force Wide Area Network. Further ITBP Force submitted the Draft QRs vide their letter No. I-45024/21/2012-IT-1258 dated 16.08.2012 to CRPF for perusal of Sub Group of Experts.

2. In accordance with MHA order No.IV-24011/12/2011-Prov-I dated 13.06.2012, the Sub Group of Experts were constituted for formulating/revising the technical specifications for various Hardware, Software etc. required for establishment of ITBP Force Wide Area Network by the nodal agency i.e CRPF.

3. The Sub Group of Experts has examined the QR's from various technical aspects keeping in view the specific requirements of ITBP Force. A total of 41 items have been identified by the Sub Group, found suitable for ITBP WAN.

4. The board proceeding and the technical specifications of various Hardware/Software required for ITBP Force WAN duly signed by Sub Group of Experts and approved by DG, CRPF (Chairman of the Group) is attached herewith for the kind perusal of MHA please.

Encl: 1. Board Proceeding of the Sub Group (02 pages)  
2. List of QR's (1-62 Pages)

  
**(R K Vishwakarma)**

Inspector General (Works & Comn)  
Directorate General, CRPF

*DS (Prov)  
to examine and  
put up  
26/9  
Expedientiously  
ph.  
11/26/9  
Prov II*

**JS (PM), Ministry of Home Affairs, Jaisalmer House, New Delhi -110001**  
No. C.VII-1/2012-ITW-R&D

Dated, the Sep'2012

Copy to: **Directorate General, ITBP, for information please.**

  
**(R K Vishwakarma)**

Inspector General (Works & Comn)  
Directorate General, CRPF

**Proceeding of Sub Group of Experts for 'Formulation of QRs' for various items identified for Establishment of Wide Area Network in ITBP Force**

Proceeding of : Sub Group of Experts.  
Held at : Directorate General, CRPF, Block No.-01, CGO Complex, Lodhi Road, New Delhi-110003.  
On : **04.09.2012** at **1100** hrs.  
By the order of : Directorate General, CRPF order No.**C.VII-1/2012-ITW-R&D** dated **28.08.2012**.  
Purpose : To Formulate/Revise QRs. for various Hardware, Software, etc. required for establishment of Wide Area Network in ITBP Force.

Composition of Sub Group of Experts: -

- |   |   |       |
|---|---|-------|
| 1. Sh. R. K. Vishwakarma, IG (Comn), CRPF | - | PO    |
| 2. Sh. Virendra Agrawal, DIG (Eqpt), CRPF | - | M-I   |
| 3. Sh. S. M. Hasnain, DIG (IT), CRPF      | - | M-II  |
| 4. Sh. Nishith Chandra, Comdt (IT), ITBPF | - | M-III |
| 5. Lt. Col. Vikas Prabhakar, Assam Rifles | - | M-IV  |
| 6. Sh. Ravindra Kumar, SC(Eqpt), NSG      | - | M-V   |
| 7. Sh. Pawan Kumar, DC, BSF               | - | M-VI  |
| 8. Sh. Subhash Chandra, AD, SSB           | - | M-VII |

In pursuant to CRPF order No.C.VII-1/2012-ITW-R&D dated 28.08.2012, the Sub Group of Experts held meeting in the Conference Hall of CRPF Directorate General on 04.09.2012 at 1100 hrs for formulation/revision of technical specifications for various hardware, software etc. required for establishment of Wide Area Network in ITBP Force.

2. At the outset, ITBP Force apprised about their requirement which were understood by the Sub Group of Experts. Representatives of NIC and all major OEMs were also present in the meeting. Technical specifications of various hardware & software items were discussed in detail.

3. Members of Sub Group and representatives of various OEMs deliberated upon all the technical specifications of required hardware & software. Representatives of various OEMs suggested some changes although there had been some contradictions as well. The representatives of user department i.e. ITBP Force were also available who explained the requirements of their users of various services.

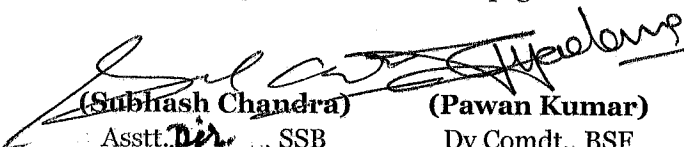
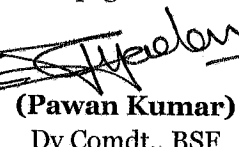
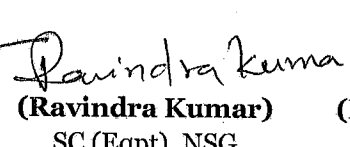
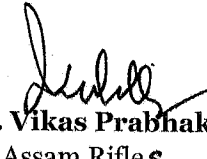
4. It was also understood by the group that technical specifications drafted by ITBP Force in accordance with their requirement and in consultation with IT Industry after a pre-bid meeting have also been deliberated in CCTNS experts in PMO, DIT and prima facie found adequate by NIC to meet the proposed solution for ITBP Force.

5. After interaction with the representatives of IT Industry, Sub Group had an internal meeting and went through the points suggested by IT Industry as well as members of the group. Inputs obtained during the meeting have been duly deliberated, and necessary changes have been incorporated considering user requirement and viability of proposed solution. It was ascertained that more than one leading OEM are complying in each item. A copy of technical specifications for various hardware / software required for ITBP Force WAN duly signed by Sub Group of Experts and approved by DG, CRPF, is attached herewith, as appendix Aa to Z as given below: -


S/N	Item Description	Appendices
1	16 KVA Online UPS	Appendix-"Aa"
2	2 KVA Line-Interactive UPS	Appendix-"Ab"
3	Virtual Tape Library	Appendix-"B"
✓ 4	Back-up Software	Appendix-"C"
✓ 5	Storage with 6TB Usable and Replication Software	Appendix-"D"
6	SAN Switch	Appendix-"E"
7	Blade Server 2 CPU	Appendix-"F"

8	Blade Server 4 CPU	Appendix-"G"
9	Blade Server Chassis	Appendix-"H"
✓ 10	OS and Other Software with CAL	Appendix-"I"
11	Core Switch with Cat-6 Jack Panel for DC/DR	Appendix-"Ja"
12	Access Switch with Cat-6 Jack Panel for Remote Locations	Appendix-"Jb"
13	Firewall	Appendix-"K"
14	IPS	Appendix-"L"
15	UTM (Firewall, IPS, SSL & Gateway A/V)	Appendix-"Ma"
16	UTM (Firewall, IPS, Gateway Antivirus & SSL) for all Offices at R/Loc	Appendix-"Mb"
17	Core Router for DC/DR	Appendix-"Na"
18	Router for Multiple Offices at Remote Locations	Appendix-"Nb"
19	Router for Single Office at Remote Location	Appendix-"Nc"
20	Internet Router for Directorate General	Appendix-"Nd"
21	Bandwidth Optimizer for DC & DR	Appendix-"Oa"
22	Bandwidth Optimizer for Multiple Offices at Remote Locations	Appendix-"Ob"
23	Bandwidth Optimizer for Single Offices at all Remote Locations	Appendix-"Oc"
24	Radio/Voice Gateway and Licenses for Remote Locations	Appendix-"P"
25	Radio Server at DC	Appendix-"Q"
26	E-Mail Security Appliance at DC	Appendix-"R"
27	Voice/IP (IPPBX) Server with Licenses, Video & No-Video IP Phones	Appendix-"S"
28	Video Conferencing System with End Points	Appendix-"T"
✓ 29	EMS	Appendix-"U"
30	65" Display for Network Operation Control	Appendix-"V"
31	Network Terminal with Windows-7 Professional OS	Appendix-"W"
32	42U Server/Network Rack with KVM Switch and 15U Network Rack	Appendix-"X"
33	Database Encryption Hardware	Appendix-"Y"
34	Structured Cabling/Accessories at DC/DR and Remote Locations	Appendix-"Z"


6. The proposal has been examined keeping in view the specific requirement of ITBP Force and found suitable. Changes in the specifications have been incorporated as per the latest available technology in the market. ITBP Force may also consider changes in the specifications before finalization of RFP & tendering process. Since proposal has been considered on case basis according to requirement of ITBP Force and therefore, MHA is requested not to fix QRs of these equipment so as to leave flexibility with CAPFs for up-gradation in future.

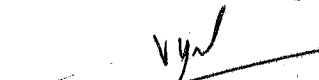
**(Subhash Chandra)**      **(Pawan Kumar)**      **(Ravindra Kumar)**      **(Lt. Col. Vikas Prabhakar)**  
 Asstt. Dir., SSB      Dy Comdt., BSF      SC (Eqpt), NSG      Assam Rifle S



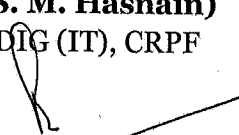
**(Nishith Chandra)**  
 Comdt (IT), ITBPF



**(S. M. Hasnain)**  
 DIG (IT), CRPF



**(Virendra Agrawal)**  
 DIG (Eqpt), CRPF



**(R. K. Vishwakarma)**  
 Inspector General (Comn), CRPF

Approved / Not Approved



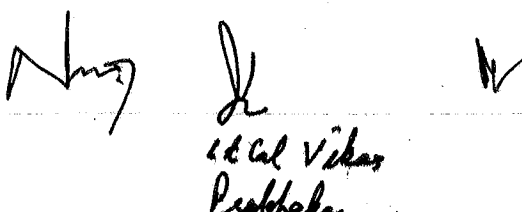
**(K. Vijay Kumar)**  
 Director General, CRPF

**TECHNICAL SPECIFICATIONS FOR VARIOUS HARDWARE**  
**SOFTWARE REQUIRED FOR WAN OF ITBP FORCE**

**Appendix-"Aa"**

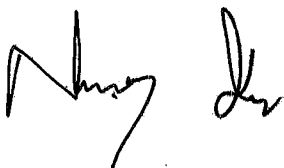


**1. Technical Specifications for 16 KVA UPS**

Description	Parameters Required	Compliance
<b>General</b>		
Type	3-Phase	
Construction	Modular	
Configuration	N+1	
Form Factor	Rack Based	
Technology	True Online Double Conversion	
Individual Hot Swappable Power Modules (Mandatory)	Min rating of each Module: 16 KW. The Qty of module will depend upon the total capacity requirement.	
Scalability	Should be able to scale with similar sized power modules in the same rack to take care of future without any downtime	
Wave Form	Sinusoidal	
Make of Battery	Only Standard Brands - Amron, Exide	
Type of batteries (Sealed Maintenance Free)	12V - Valve-regulated / sealed maintenance free	
Type of rectifier	IGBT Based	
Type of Inverter	IGBT based	
Modular Hot Swappable Power Distribution Modules	Required	
<b>Back-up Environment</b>	02 Hrs Back-up on full load	
Operating temperature	0° to 40° C	
Storage temperature	0° to 45° C	
Relative Humidity	0 - 95% non-condensing	
Protection Class	IP20	
Noise level @ 1 Mt. distance	<61 dB	
Equipment Cooling	Forced Air Cooling	
<b>Communication</b>		
Interface Port	RS232, Ethernet	
SNMP card	Required	
<b>Maintenance &amp; Controls</b>		
Built In Static Bypass	Yes, Enabled, hot swappable	
Built In Static Switch - Inverter	Required at Inverter Output	
Built In Maintenance Bypass	Yes, Manual	
Control Panel	Multi Function LCD Status and Control Console	
Alarm	Audible and Visible Alarm for Faults	
Redundant Power Module Controllers	Yes. Hot swappable.	
Emergency Power Off	Yes	
Life Cycle Monitoring of Fans , DC /AC Capacitors ,Batteries	Yes	


  
 Page 1 of 62

Standards		
Safety	EN50091-1, IEC 62040-1-1	
EMC Emission	EN50091-2, Class A, IEC 62040-1-2	
Design	EN50091-3, IEC 62040-1-3	
EMC Immunity	ENS50082-2	
Low Magnetic field radiation	EMF as per ICNIRP	
Operation	24 x 365 Continuous Operation	
<b>General Characteristics</b>		
Efficiency of the UPS		
AC/AC total efficiency @ 25% load	>92 %	
AC/AC total efficiency @ 50% load	>94%	
AC/AC total efficiency @ 75% load	>94%	
AC/AC total efficiency @ 100% load	>95%	
Dimensions in mm (L X B X H)	Rack Mountable	
Weight in Kgs	Vendor to Specify	
Online Thermal Dissipation (BTU/Hr.)	Vendor to Specify	
Cable entry - Bottom	Top/Bottom	
Degree of protection	IP 20	
Battery Self Discharge Test	Required	
<b>Input Electrical Characteristics</b>		
Nominal Input Voltage (3 Phase)	400V	
Input Voltage Range (3 phase)	340 to 460 V	
Input Frequency	50 Hz $\pm$ 3 Hz	
Input Power factor @ 50 to 100% load	Unity	
System power walk- in	Minimum 10 secs (Adjustable)	
<b>Input Current harmonic distortion ( THD)</b>		
THD @ 25% Load	$\leq$ 8%	
THD @ 50% Load	$\leq$ 5%	
THD @ 75% Load	$\leq$ 4%	
THD @ 100% Load	$\leq$ 3%	
Maximum current drawn during battery charging & inverter with nominal power (In Amps)	By bidder	
Rectifier DC voltage ripples	<1%	
Maximum Charging time	8 - 10 hrs.	
<b>Output Electrical Characteristics</b>		
Nominal Output Voltage	400 V, 3 Phase, Neutral & Ground	
Static output voltage variation	$\pm$ 1%	
Output waveform	Sinusoidal	
Dynamic output Voltage variation when load varies from 0 - 100% & vice versa.	$\pm$ 2% on 0 to 100% or 100 to 0% load step changes, recovery time <100 msec	
Output power factor to be delivered (KW )	0.8	
Output Voltage variation at balance load	$\pm$ 1%	
Output Voltage variation at unbalance load	$\pm$ 5%	
Output Voltage adjustment - 100% unbalance load	$\pm$ 3%	
Output frequency	50Hz $\pm$ 0.5 Hz	

<b>Phase Displacement:</b>		
-at 100% balanced load		+/-1%
-with mains synchronization adjustable to		+/-2%
Steady State Voltage		±1%
Transient Load Voltage		± 5%
Response time to 100% load Step		<100 msec
Output power factor compatible		0.8 Lag - Unity 0.9 Lead
<b>Overload capacity</b>		
For 60 minutes		110%
For 10 minutes		125%
For 1 minutes		150%
For 200 m sec		225%
THDv		< 2%
Short circuit capability		2.7 times peak current for 150 msec
Crest Factor		>3:1
<b>Bypass arrangement</b>		
Static Bypass Switch		Automatic without Fuse
Rated Voltage (3 Phase with neutral)		400V
Voltage variation		±10% (Adjustable)
Nominal Frequency		50Hz
Maintenance bypass switch		Manual
Bypass Overload Capacity		
@110% Load		30minutes
@125% Load		10minutes
@150% Load		30Seconds
Break Time / make Time		No Break Transfer
<b>Battery details</b>		
Modular Hot Swappable Batteries		Yes
Back-up		Depending on requirement
VAH of the battery		By Vendor , supported by calculation
Design Life of battery		≥ 5 - 6 Years
Battery temperature sensor		Required
Individual Battery Monitoring		Required
No. of Batteries provided		By Vendor
Battery Monitoring in UPS		Required
Battery Mounting		Rack Mounted
Battery Breaker		MCCB based
Dimensions of battery cabinet(LXBXH)		By Vendor
Weight of battery with racks		By Vendor
Base Frames for UPS & Batteries		Required

**2. Technical Specification for 2 KVA Line-Interactive UPS**

Technical Specifications	Compliance
<b>UPS 2 KVA</b>	
<b>Output</b>	
Output Power Capacity: 1980 Watts / 2200 VA	
Max Configurable Power: 1980 Watts / 2200 VA	
Nominal Output Voltage: 230V	
Output Voltage Distortion: Less than 5% at full load	
Output Frequency (sync to mains):47 - 53 Hz for 50 Hz nominal,57 - 63 Hz for 60 Hz nominal	
Crest Factor: up to 5:1	
Waveform Type: Sine wave	
<b>Input</b>	
Nominal Input Voltage: 220v AC	
Input Frequency: 50/60 Hz +/- 5 Hz (auto sensing)	
Cord Length: 2.5 meters	
Input voltage range for main operations: 140 - 230V	
Input voltage adjustable range for mains operation: 151 - 302V	
<b>Batteries &amp; Runtime</b>	
Battery Type: Maintenance-free sealed Lead-Acid battery with suspended electrolyte: leak proof	
Backup Time: 2 Hours bckup on Full Load	
<b>VAH :Min 2016VAH</b>	
<b>Communications &amp; Management</b>	
Interface Port(s): RS-232,	
Interface Quantity: 1	
CoWESTI panel: LED status display with load and battery On Line: On Battery: Replace Battery and Overload Indicators	
Audible Alarm: Alarm when on battery: distinctive low battery alarm: configurable delays	
Emergency Power Off (EPO): Yes	
<b>Surge Protection and Filtering</b>	
Surge energy rating: 510 Joules	
Filtering: Full time multi-pole noise filtering: 0.3% IEEE surge let-through: zero clamping response time: meets UL1449	
<b>Environmental</b>	
Operating Environment: 0 to 45 °C	
Operating Relative Humidity: 0 to 95%	
Operating Elevation: above MSL	
Storage Temperature:0 to 45 °C	
Storage Relative Humidity: 0 to 95%	
Audible noise at 1 meter from surface of unit: <45 dBA	
Online Thermal Dissipation: 275.00 BTU/hr	

Handwritten signatures and initials, including a large signature on the left and several smaller initials or signatures to the right.



**3. Technical Specifications for Virtual Tape Library**

S/N	Specifications	Compliance
01	Should be able to interface with different server platforms and operating systems simultaneously via NFS v3, CIFS and FC	
02	Should support LAN, SAN & NDMP backup solutions simultaneously	
03	Must support inline data duplication technology at block level using variable block length technology	
04	Must support VLAN tagging	
05	Must support both LAN D2D backup and VTL backup at the same time	
06	Must support single management pane for multiple storage arrays for ease of management	
07	Should be provided with 6TB capacity on NL-SAS/ SATA (7200 RPM) disks	
08	Must have the ability to perform different backup or restore jobs simultaneously.	
09	Must support for de-duplicated and encrypted Replication of data over Local or Wide Area Networks	
10	Must support 10Gb Ethernet connectivity	
11	Must support point-in-time copies of a LUN or volumes with minimal performance impact	
12	Must supports communications and data transfers through 2x4GB FC SAN, 4 x 1 Gb Ethernet LAN	
13	Should support capacity on demand feature that allows the storage allocation associated with a virtual tape cartridge to be consumed upon write, and not creation	
14	Should support auto support remote health check for OEM to monitor the system health.	
15	Should support above 2TB/hr backup throughput.	
16	Should support single storage pool and load balancing across multiple storage controllers	
17	Should support different retentions for primary and DR backup storage	
18	Must support global and target based de-duplication which Should also support de-duplication at backup server level	
19	Must protect against lost data in power fail and software crashes	
20	must support Data compression using lz, gz or gzfast	
21	must support selective replication to sub share level replication, must support schedule throttle of network bandwidth depending on the utilization of the WAN bandwidth	
22	Must support simultaneous replication process while backup is running	
23	Replication Should support bi-directional, many-to-one, one-to-many, and one-to-one replication	
24	Should support recovery from replica.	
25	Must support ACL for CIFS/NFS/telnet/http/https/ftp/ssh	
26	Must support 64 virtual tape libraries, 128 virtual drives, 20,000 slots & 1,000,000 virtual tapes or more	
27	Should support Link Aggregation Control Protocol (LACP)	
28	Should have SNMP and command line support.	
28	Should have min 3.6TB usable capacity with Hot Swap drive and scalable to 8.4TB usable.	
30	Should support IP Aliasing.	


31	Should support 256 bit AES encryption at rest.	
32	Should support retention lock feature which ensures that no data is deleted accidentally.	
33	Should have inbuilt NDMP tape server.	
34	must support RAID 5/6 technologies	

**Appendix-"C"**

**4. Technical Specifications for Backup Software**

S/N	Specifications	Compliance
01	Should be available on various OS platforms such as Windows 2000/ NT, Linux and UNIX platforms and be capable of supporting backup / restores from various platforms including TRU64 UNIX, HP-UX, IBM AIX, Linux, NetWare. Both Server and Client software should be capable of running on all these platforms.	
02	The backup solution should also support online LAN Free SAN based backups of databases through appropriate agents, Important Applications being Oracle, Microsoft SQL Server, Exchange, SharePoint and Data Protection Manager; IBM DB2 UDB; Informix; Lotus Notes/Domino; SAP R/3; Sybase; Meditech; EMC Documentum.	
03	SAN based Backup agents should be provided for 2 Nos exchange servers and Database servers (MS SQL) in active passive mode and LAN based agents for bare metal backup of remaining servers	
04	The backup software should integrate with VCB and VADP based VMware backups with de-duplication enabled, should also support CBT based incremental backups and restores of VMware virtual machines.	
05	Must provide coordinated Disaster Recovery with the SharePoint Volume Shadow Copy Service (VSS) Writer	
06	Must provide selective granular backup and recovery for SharePoint	
07	Ability to backup data from one server platform and restore it from another server platform to eliminate dependence on a particular OS machine and for disaster recovery purposes.	
08	Software should have full command line support on above mention operating systems.	
09	The backup software should be able to encrypt the backed up data using 256-bit AES encryption on the backup client and should not demand for additional license, any such license if needed should be quoted for the total number of backup clients asked for.	
10	Must support dissimilar system hardware restore on multiple platforms including Windows, Solaris, Linux, HP-UX, and AIX.	
11	Should have built-in Alert support. This feature should support e-mail, SNMP broadcast messages etc.	
12	Must support wizard-driven configuration and modifications for backups and devices	
13	The backup software should support industry standard Common Device Interface for advanced device reporting and handling.	
14	Software should have Multiplexing backup facility. Backup multiple clients' data on the tape simultaneously.	
15	Software should have Multithreading/Multi-streaming backup facility, Backup of more than one streams of data from client to the backup server.	
16	Should have cross platform Domain Architecture for User management and should also have role based User management.	
17	Should have firewall support.	
18	Must support de-duplicated backup and recovery for Microsoft Hyper-V using VSS at the host (parent partition) to protect both the host and guest (child partition). The quoted software should also support backup and recovery with VSS for applications running within a Microsoft Hyper-V Child Partition. Application being Exchange, SQL, SharePoint and Active Directory	

19	Should have in-built scheduling system and also support check-point restart able backups..	
20	The Backup software should have the ability to report inactive files, which will help the customer decide what to backup/archive.	
21	Should support software distribution of upgrades.	
22	Should support backups for clustered servers and support industry popular clusters like Sun cluster, Tru 64, HP service guard, EMC cluster, HACMP? i.e. should have the ability to backup data from clustered servers from the virtual client, backing up data only once and giving consistent backup in case of failover of nodes.	
23	The software should support virtual platform like VM Ware, Citrix Xen Server and Hyper V, licensing of such environments should be based on physical hosts not on the number of virtual instances.	
24	Should support clustered configurations of the backup application in a cluster. I.e. backup application should failover as a highly available resource in a cluster, should not have additional licensing cost implication for clustered hosts.	
25	Must support backup / recovery of raw SCSI volumes	
26	Pricing of the software should not to be dependent on the number of CPUs of the client machines. Upgrading the client machines and increasing CPU should not have any commercial implications in terms of renewing licenses or buying additional licenses.	
27	Should have the optional ability of staging the backup data on a disk and then de-stage to a tape based on the policy for faster backups.	
28	Should support advanced backup to disk backups where backups and restores from the backup media (disk in this case) can be done simultaneously.	
29	Should have the ability to configure retries for backups of a client in case the client is not available on the network due to reboot or network failures.	
30	Must support proxy-based off-host backup workflows – including LAN-free for virtual servers for Microsoft Hyper-V environment.	
31	Should support NDMP multiplexing of NDMP and non NDMP data to the same tape and should also support NDMP backup to disk.	
32	The backup software should support backup and restore of NDMP data to media server attached tape/VTL.	
33	The software should support bare metal recovery of UNIX and windows servers (if this functionality requires any additional hardware the same should be quoted)	
34	Should integrate with third party VTL which has data de-duplication capabilities.	
35	Should have the capability to do data de-duplication at the block level and then do backup (appropriate module should be quoted)	
36	The backup software should understand virtual operating environments and should be licensed per physical host not guest OS.	
37	Must support for off-host proxy-based backup including network and LAN-free with block-level backup and restore of unlike operating systems.	
38	Must support source capacity based licensing which should have no impact in case if the number of processor are increased in the server being backed up.	
39	Agent/Modules for Databases such as MS SQL, Oracle, Exchange, Lotus, DB2, Informix, Sybase should be per host and should not demand for new type of licenses in case of number of CPUs are increased.	
40	Quoted Backup software must support more than 1 worker/storage/media server which works as worker to receive backup data from clients and write data to tape.	
41	Backup software must support Robotic/automated Tape library, the licensing of such library should be on the number of slots and not on the drive counts so as to avoid buying new licenses when additional drives are added to improve performance.	
42	Must feature integrated client de-duplication for file systems and applications.	


43	Must enable de-duplication and traditional backup from a single software agent and/or module footprint.	
44	Must provide efficient de-duplication ratios beyond single instance storage at the client, storage node (media server) and target device levels.	
45	Tapes must be self-describing to ensure data can be recovered even in the case of loss of central indexes.	
46	Must support Hardware and storage array based snapshot backup for off host zero downtime and zero load on the primary backup client.	
47	Must Support Continuous data protection for select set of servers or dataset.	

**Appendix-"D"**

**5. Technical Specifications for Storage: 6TB Usable & Replication Software**

Features	Specifications	Compliance
Rack Mount	The Proposed SAN Array must be rack mounted capable	
Controller	The Proposed SAN Array should be configured with dual Controller	
Front & Back End FC Connectivity	Proposed Array should have at least 4 Nos. of 8Gbps FC ports and 2 no. of 01 Gbps iSCSI front end ports and minimum 8 backend SAS Lanes across controllers.	
Cache	Should have minimum 16 GB memory across controllers	
Required Disk Space	Should be configured with 6TB usable capacity. 4TB Using 600GB 15K RPM SAS drives on RAID5 and 2TB on RAID 10 using NL SAS drives. The array should be scalable to minimum 120 drives	
RAID	The Proposed SAN Array should support RAID Levels: RAID 0,1+0, 4 or 5 & 6 or DP	
OS Support	Support for Windows, Linux or other UNIX flavour.	
Redundancy	Provision for Redundancy of Disk Drives, Controllers, Fans & Power Supplies	
Cache Data Backup	In case of power failure, the SAN array must be provided with cache protection mechanism to ensure no loss of data in cache for minimum 72 hours	
Management Software	The SAN Management software should be array based and provide GUI/ Web Based Management with complete Reporting features like LUN Usage, Empty Space	
Snapshot Software	Snapshot and cloning software should be provided for entire array	
Remote Diagnostics	The Proposed SAN Array should support Web Based; Email facility for remote service to report errors and warnings .	
Replication	The array should be provided with all the necessary hardware and Software for replicating to remote site	

**Appendix-"E"**

**6. Technical Specifications for SAN Switch**

S/N	Specifications	Compliance
1	Switch architecture must be configured with 02 Nos. fully populated/activated 08 FC Ports from day one on each and should be upgradeable to 48 Fibre Channel ports each with minimum port speed 8Gbps	
2	Should have dual Fans and Hot plug power supplies	
3	Should have GUI/ web based Fabric Manager for administration and configuration	
4	Should have inbuilt diagnostics features like Power on Self-Test, FC trace route, FC Ping etc.	

*Handwritten signatures and initials*

5	The switch must support Radius authentication when managing from GUI, console or telnet to prevent unauthorized access and must support Secure Shell (SSH) encryption to provide additional security for Telnet sessions to the switch.	
6	The switch must be able to support port aggregation up to 4 physical Fibre Channel ports to provide aggregated links. The ports aggregation must not be limited to ports within the same module. The switch must support the aggregation of any ports from any module	
7	Switch should protect existing device investments with auto-sensing 1, 2, 4Gbps capabilities and all the ports should auto-negotiate to 4Gb /2Gb FC speeds.	
8	All the SAN Switch Components should be field replaceable units	
9	SAN Switch should support Virtual Fabrics or equivalent feature	
10	SAN Switch should enable partitioning of a physical SAN into logical fabrics	
11	SAN Switch should enable isolation of logical fabrics by application	
12	SAN Switch should provide advanced zoning capabilities	
13	SAN Switch should allow performance monitoring capabilities	
14	SAN Switch should have support for web based management	
15	Relevant S/w with Licenses for integration of Servers with Storage	
16	Should support FCIP.	

**Appendix-"F"**

**7. Technical Specifications for Intel Blade Servers: 2CPU**

Features	Specifications	Compliance
Make & Model	ONLY REPUTED BRANDS	
Processor	Should be populated with 2 Nos of Intel Xeon E5-26XX (10M/ 4Core/ 2.4 GHz) processors, Chip Set C600.	
Memory	Should be populated with 16GB RAM per CPU and should be scalable to minimum 512 GB	
Memory Protection	Advanced ECC with multi bit error protection	
Cache	10 MB L3 Cache per Processor	
HDD Support	Should support SAS and SSD hard drives	
HDD	2*300GB 15k rpm SAS SFC with RAID 1 for all servers	
Controller	Integrated SAS raid controller with RAID 0,1	
Graphic Controller		
Networking features	Should have dual 1Gbps Ethernet ports for LAN connectivity	
Blade server connectivity to SAN	Should have a 4 port 10Gbps FC HBA for connectivity to SAN	
Bus slots	Min. of 2 PCI-e x8 based mezzanine slots	
OS support	Should support Microsoft windows server, windows server hyper-v, RHEL, SLES, Solaris 10 for X86/x64 based systems; VM Ware ESX server	
Manageability	Should supplied with enterprise version of management suite that can monitor and manage all the servers from the vendor deployment on our data centre	
Remote management	i It should be possible to manage the server and get access to critical information about the health of the server from any remote location with just the help of a standard web browser (internet explorer) ii Hardware based and OS dependent remote management. Remote management should support remote power on/off of the server	

*(Handwritten signatures)*

	iii Should be possible to remotely manage each blade server individually. Should support access rights for administrators for each blade server individually. Should be able to manage multiple blades in the same enclosure at the same time	
Power Supply	From Blade Chassis	

***Appendix-"G"***

**8. Technical Specifications for Intel Blade Servers: 4CPU**

Features	Specifications	Compliance
Make & Model	ONLY REPUTED BRANDS	
Processor	Should be populated with 4 Nos of Intel Xeon E5-46XX (2.7GHz/8-core/20MB) processors and should be scalable to 4 processors	
Memory	Should be populated with 32 GB RAM in each CPU and should be scalable to minimum 1TB	
Memory Protection	Advanced ECC with multi bit error protection.	
Cache	24 MB L3 Cache per Processor	
Chipset	Intel C 600 Chipset	
Graphic Controller	8 MB Graphic Memory	
HDD Support	Should support SAS and SSD hard drives	
HDD Populated	2 x 300 GB 15k rpm SFF SAS with in RAID 1 for all servers.	
Controller	Integrated SAS raid controller with RAID 0,1	
Networking features	Should have dual 1Gbps Ethernet ports for LAN connectivity	
Blade server connectivity to SAN	Should have a dual port 8Gbps FC HBA for connectivity to SAN	
Bus slots	Min. of 2 PCI-e x8 based mezzanine slots	
OS support	Should support Microsoft windows server, windows server hyper-v, RHEL, SLES, Solaris 10 for X86/x64 based systems; VM Ware ESX server	
Manageability	Should supplied with enterprise version of management suite that can monitor and manage all the servers from the vendor deployment on our data centre	
Remote management	i) It should be possible to manage the server and get access to critical information about the health of the server from any remote location with just the help of a standard web browser (internet explorer)	
	ii) Hardware based and OS dependent remote management. Remote management should support remote power on/off of the server	
	iii) Should be possible to remotely manage each blade server individually. Should support access rights for administrators for each blade server individually. Should be able to manage multiple blades in the same enclosure at the same time	
Power Supply	From Blade Chassis	

Four handwritten signatures and initials are present at the bottom of the page. From left to right: a large signature, a smaller signature, a set of initials, and another signature.

**9. Technical Specifications for Blade Server Chassis –**  
*(As required to populate the quoted servers)*

Features	Specifications	Compliance
Description	Shall provide common resources for the Blade Servers like power, System Management, Cabling, Ethernet Management and extension, External fibre Channel Storage switching and connectivity. Chassis with all redundancy features. All components to be provided by the OEM and to be fully redundant	
Blade Bays and I/O bays	Sufficient Chassis to be provided to accommodate min 8 full height Blade Servers or 16 half height blade servers. Minimum 6 I/O bays with minimum 3 fabric support.	
Mid-Plane	Passive mid-plane for providing two-way communication paths for Ethernet, Fibre Channel, KVM Switches, Power Supply and Management Signals and should be able to support with minimum throughput of 5 Tb/s	
Ethernet Switch Module	4 No's of LAN switches supporting with sufficient no. of 10Gbps ports for External LAN connectivity	
SAN Switch	2 No's of 8 Gbps FC switches for SAN connectivity	
Management Modules	Dual redundant management modules to communicate with the system management processors on the blade server. The Management Modules shall be capable of providing KVM Connectivity for the Blade servers housed inside the chassis, Real time, actual power cons. Status/Inventory/Alerting for Blades, Chassis Infrastructure, & IOMs; Centralized Configuration; GUI & CLI; SSL/SSH ; Power/Thermal Monitoring; Dynamic power engagement; Temperature monitoring; Persistent WWN/MAC - Should allow customers to lock a WWN/MAC address into a specific blade slot. A unique pool of WWN/MAC's are stored in the Chassis IP address per remote management card; Virtual Media & vKVM; Security - Local & AD. Management modules should be fully redundant with no common components/modules. Failure of any component should not compromise management capability.	
Cooling	Hot swap variable speed blowers/fans for Cooling the chassis fully redundant and all populated	
Power Module	Sufficient number of power supplies for N+N or N+1 redundancy	
Form Factor	Up to 10U - 19 "Rack Mountable with 28" depths.	
System	Shall provide support for remote console management, power on/off blades, modules shall monitor power status, operating system, temperature, disks, blowers, power modules system diagnostic programs provided through the management s/w. Real Time Power/Thermal Monitoring and Management	
System Panel	Interactive colour LCD/LED panel for local trouble shooting & wizard based setup	
	Control panel display to show health of the systems including power-on, over temperature, other information and system error conditions. Front Control Panel to allow one KVM connection for all blades	
Ports	Front VGA & 2 USB ports for KVM	
Optical Disk	Chassis based or USB based DVD Drive to be configured which can be shared among all blade servers	
Certifications	EAL-3, UL Certifications	
KVM Support	Blade Chassis should have Dual Redundant Local ports for Keyboard, Video & Mouse along with Management Module.	
CD/Diskette/USB	Chassis or USB based CD-ROM/DVD-ROM which can be used by the blade servers. The chassis should have minimum Two USB 2.0 ports.	

**10. Details of System & Server Software**  
(CAL as per AR)

S/No.	Item/Specification	CAL	Compliance
1	Windows 2012 Data Centre or Latest	CAL as per Actual Requirement	
2	Windows 2012 Standard or Latest		
3	MS SQL Server 2012 Enterprise or Latest		
4	MS Exchange 2010 or Latest		
5	MS Lync 2010 or Latest		
6	MS SharePoint Server 2012 or Latest		
7	MS System Centre 2012 Data Centre or Latest		
8	MS System Centre 2012 Client Management Suite or Latest		

**11. Technical Specifications of Core Switch for DC & DR**

S/N	Specifications	Compliance
1.	Switch shall be chassis-based and modular in nature, rack mountable with minimum of 10 I/O slots or more for interfaces and two for switching engines.	
2.	The switch shall have redundant power supply.	
3.	The switch shall have a minimum 400 Gbps half duplex of Switching fabric and 300 Mpps at 64 byte. The performance of switching fabric should not degrade below 400 Gbps in case of failure of active processor.	
4.	Switch should have Non-stop forwarding and Stateful Switchover functionality.	
5.	Switch should provide the mechanism to perform software upgrades and downgrade without taking switch out of service.	
6.	Shall have hardware based ACL and multicast management.	
7.	Shall support IPV6 in hardware.	
8.	Support for at least 4000 active VLAN	
9.	Should support IGMP snooping v1, v2 and v3.	
10.	Switch should support 60 K or more MAC	
11.	Switch should support 10,000 ARP entries	
12.	Should be able to discover directly connected devices on layer 2 network without any configuration and provide device Id, interfaces, traffic details.	
13.	Provides a mechanism to detect connectivity issues with both fibre and copper cabling. Ensures that a partially failed link is shut down on both sides, to avoid L2/L3 protocol convergence issues.	
14.	Should support LLDP exchange link and device information in multi-vendor networks.	
15.	Support for Detection of Unidirectional Links and to disable them to avoid problems such as spanning-tree loops.	
16.	Should support minimum 128K IPv4 and IPv6 unicast and multicast routes.	
17.	6 port 10 Gigabit Ethernet interfaces (with Short reach module)	
18.	2 x 24 Port SFP based Gigabit interface module (24 Sx SFP)	
19.	2 x 48 port 10/100/1000 module	
20.	Should be supplied with Cat 6 Jack Panel and Cat 6/Fibre Structured Cabling as applicable - all UL listed.	
21.	Should be EAL-2 certified or higher.	



## 12. Technical Specifications for Access Switch

S/no	Features Required	Compliance
1.	Multilayer routing switch, enterprise class intelligent service delivered to the network edge and should be at least EAL2 certified	
2.	Intelligence – Layer 3	
3.	No of 10/100/1000 Base T POE Ports – 24 and should have four SFP ports. At least two LX SFP transceivers to be provisioned from Day-1.	
4.	Switching Fabric Bandwidth (Backplane) – At least 108 Gbps	
5.	Forwarding rate = 40 MPPS	
6.	No of MAC address >=4000	
7.	VLAN >= 255	
8.	Link Aggregation should support link Aggregation control protocol (LACP) which allows the creation of Ethernet channelling with devices that conform to IEEE 802.3ad	
9.	User authentication – Should support 802.1x allowing dynamic port based security providing user authentication	
10.	Traffic control – to be supported	
11.	Spanning tree protocol / Rapid spanning Tree Protocol – Should support IEEE 802.1w rapid spanning tree protocol (RSTP). Backward compatible with spanning tree protocol (STP) fast start mode spanning tree enable / disable port	
12.	Layer2 switching – should support 802.1D, 802.1w, 802.1s, 802.1q	
13.	IGMP Snooping – Should support IGMP snooping on layer 2 interface	
14.	Flash memory – Minimum 8 MB	
15.	Basic static routing – should support basic static routing from day one	
16.	Stacking technology – should support stacking, possible to manage up to at least 3 switches	
17.	Dynamic host configuration protocol – Should support dynamic host configuration protocol	
18.	Stacked units should behave as a single spanning tree mode	
19.	Should be supplied with Cat 6 Jack Panel and Cat 6/Fibre Structured Cabling as applicable - all UL listed.	

## 13. Technical Specifications for Firewall

S/N	Specifications	Compliance
1.	The firewalls are required to be installed in High Availability and should have at least 4 GE & 2 x 10 GE	
2.	Firewalls should have active/active and active-passive modes support	
3.	The firewall operating system should be optimized for running advanced security services such as stateful firewall/NAT and IPSec.	
4.	Firewall should not drop any sessions during fail-over from active to redundant.	
5.	The Firewall should have a minimum throughput of 5 Gbps and maximum of 1,000,000 sessions	
6.	Firewall should be EAL 3 or higher	
7.	The Firewall should support IPv4 and IPv6 routing	
8.	The Firewall should support VRRP	
9.	Firewalls should support AAA using RADIUS or TACACS	
10.	Firewalls should support Packet Filters, & Stateful Firewalling	

11.	Firewalls should support Network attack detection, DoS and DDoS protections	
12.	Firewalls should support Tunnels (GRE, IP-in-IP, and IPSec), DES (56-bit), 3DES (168-bit), AES (256-bit) encryption support	
13.	Firewalls should have role based access mechanisms.	
14.	Firewalls should support Network address translation (NAT).	
15.	Firewall should have Console, Telnet and Web for management	
16.	Firewalls should support Software upgrades	
17.	Firewalls should support SNMPv2 and SNMPv3	
18.	Should have redundant power supplies	

**Appendix-"L"**

**14. Technical Specifications for IPS**

S/N	Specifications	Compliance
1.	Should be an appliance based solution	
2.	Should have a throughput of minimum 5 Gbps of traffic	
3.	Should support a minimum of 1 million concurrent sessions	
4.	Should have redundant power supplies	
5.	Should protect the network form known and unknown network and application layer attacks, DoS attacks, malwares, worms, network viruses, spyware etc.	
6.	The system should be able to detect, respond to and report any unauthorized activity	
7.	IPS Solution should detect and remove invalid packets running through the system	
8.	IPS Solution should be able to detect and block against DOS/DDOS based attacks	
9.	IPS Solution should detect Zero Days attacks by protocol or application anomaly methods	
10.	The device should monitor the network traffic on the local LAN segment for signs of attack like Denial of Service attacks, pre attack probes	
11.	The sensor should be capable of dropping; a single packet, an entire TCP flow, all traffic from a possible attacking source	
12.	It should support traffic normalization to ensure that IP traffic such as fragments are reconstructed correctly before being evaluated, dropped or forwarded	
13.	Should able to support failover mechanisms to avoid any single point of failures	
14.	The system should work in a non-intrusive mode and be able to monitor all of the major TCP/IP protocols, including IP, Internet Control Message Protocol (ICMP), TCP, and User Datagram Protocol (UDP)	
15.	The IPS should allow enforcement of policy decisions based on content detected at the application layer	
16.	The IPS should be able to perform RFC compliance checking for major TCP/IP protocols	
17.	The IPS should allow the user to make policy-based decisions to permit or deny certain types of traffic, such as the use of Peer to Peer traffic that can potentially consume precious network bandwidth	
18.	The system should do stateful decode application-layer protocols such as FTP, SMTP, HTTP and Telnet	
19.	The IPS OEM should provide periodic signature updates. This signature updates should be easily downloadable from the OEM website through the Internet	
20.	Log the event with the security event management system and able to monitor 3 or above segments (Gigabit ports). It should be EAL3 certified or higher	

*Handwritten signatures and initials*

**15. Technical Specifications for UTM**

S/N	Specifications	Compliance
1.	The Firewall should be Hardware based, Reliable, purpose-built security appliance with hardened operating system that eliminates the security risks associated with general-purpose operating systems	
2.	Firewall appliance should have at least 2 x 10G interfaces & 4 x Gigabit Ethernet interfaces and should scale up to 16 GE interfaces in future.	
3.	Firewall stateful throughput should be 6 Gbps and should scale up to 20 Gbps in future	
4.	Firewall should have 3DES IPSec throughput of 1.5 Gbps and should scale up to 7 Gbps in future	
5.	Firewall should support more than 1000 site-to-site VPN Tunnels or higher	
6.	Firewall should support 190,000 firewall sessions per second	
7.	Firewall should support 3.0 Million concurrent firewall sessions or higher	
8.	The firewall shall belong to product family which minimally attain Internet Computer Security Association (ICSA) Firewall Product Criteria 4.1 Certification and EAL 3 or higher	
9.	The Firewall should have integrated or external SSL VPN solution to cater to 2000 SSL VPN concurrent users	
10.	The Firewall Appliance should be proposed with IPS & Antivirus functionality from day 1	
11.	IPS throughput should be more than 3 Gbps with at least 3,000 signatures	
12.	Firewall should support minimum 1.7 Gbps of Antivirus throughput or an external appliance to be proposed for Gateway Antivirus solution which should not degrade the performance	
13.	The antivirus solution should be able to block, allow or monitor the following services HTTP, HTTPS, SMTP, SMTPS, POP3, POP3S, FTP & FTPS	
14.	The proposed system shall have the ability intercept and inspect content of SSL encrypted traffic of the following protocols: HTTPS, IMAPS, POP3S & SMTPS	
15.	Should have support for both IPv4 & IPv6 routing	

**16. Technical Specification for Remote site UTM**

S/N	Specifications	Compliance
1.	The Firewall should be Hardware based, Reliable, purpose-built security appliance with hardened operating system that eliminates the security risks associated with general-purpose operating systems	
2.	Firewall appliance should have at least 8 Ethernet interfaces (2 x GE + 6Fast Ethernet interfaces or higher)	
3.	Firewall stateful throughput should be 1.5 Gbps or higher	
4.	Firewall should have 3DES IPSec throughput of 140 Mbps	
5.	Firewall should support more than 200 site-to-site VPN Tunnels and 800 VPN Client to Gateway tunnels or higher	
6.	Firewall should support 8500 firewall sessions per second or higher	
7.	Firewall should support 1,100,000 concurrent firewall sessions or higher	
8.	The firewall shall belong to product family which minimally attain Internet Computer Security Association (ICSA) Firewall Product Criteria 4.1 Certification or EAL 3 or higher	
9.	The solution should have either integrated or external SSL VPN solution to cater to at least 50 SSL VPN concurrent users	

10.	The Firewall Appliance should have integrated IPS, Antivirus, Anti-spam, Web content filtering & Application control functionality from day one	
11.	IPS throughput should be 200 Mbps with at least 3,000 signatures or higher	
12.	Firewall should support minimum 180 Mbps of Antivirus throughput or higher	
13.	The proposed system should be able to block, allow or monitor only using AV signatures and file blocking based on per firewall policy based or based on firewall authenticated user groups with configurable selection of the following services HTTP, HTTPS, SMTP, SMTPS, POP3, POP3S, FTP, FTPS etc.	
14.	The proposed system shall have the ability to detect, log and take action against network traffic based on over 1,000 application signatures	
15.	The proposed system shall have the ability intercept and inspect content of SSL encrypted traffic of the following protocols: HTTPS, IMAPS, POP 3S & SMTPS	
16.	The appliance should have inbuilt storage for logging & reporting or separate appliance to be provided for logging.	
17.	The device should support IPv4 & IPv6 routing	

**Appendix-"Na"**

**17. Technical Specifications for Core Router**

S/N	Specifications	Compliance
1.	The router should have at least 6 slots and all the slots should be universal and should be EAL3 or higher	
2.	Router should have 4 x 10 G distributed across two slots	
3.	Router should have 2 x STM-1 & 2 x E3 distributed across two slots	
4.	Router should have 5 Ethernet interface supporting 10/100/1000 Mbps distributed across two slot	
5.	Router should have at least three slots available for future use.	
6.	Router should support ATM interface for legacy integration	
7.	Router should have 20 Gbps at least and forwarding performance of 30 Mpps at 64 byte.	
8.	The router shall have 1+1 redundancy in control & forwarding plane and power supply	
9.	Router should support cRTP for voice traffic or equivalent	
10.	Router must have netflow for traffic analysis & management	
11.	Router must have network address translation	
12.	The router shall support in-service software upgrades and in-service software downgrades.	
13.	The router shall have relevant high availability features such as non-stop forwarding, graceful restart, modular operating system etc. to provide high uptime.	
14.	If any of the services on the router works on a module, at least two of those modules shall be quoted to ensure redundancy of the solution.	
15.	Router should support RIP v1/v2, OSPF v1/v2/v3, BGP-4, MPLS feature from day one for IPv4 & IPv6	
16.	Router should support multicast features like IGMP v1/v2/v3, PIM etc.	
17.	Should support V.35, E1, E3, STM-1/4/16, 10GE interfaces	

*(Handwritten signatures and initials)*

## 18. Technical Specifications of Router for Multiple Offices at Remote Locations

S/N	Specifications	Compliance
(a)	General – Multi-service access router should support secure intranet & Network access with VPN & Firewall protection along with VLAN and should be EAL3 certified or higher. It should be possible to run all the services together like Security, MPLS, IPv6 and other services	
(b)	CPU – Should be have at least 500 MHz speed	
(c)	Memory – Flash memory should be minimum 8 MB and expandable at least to 32 MB or more and DRAM should be at least 4 GB or more	
(d)	Physical ports	
(i)	Router should have at least 4 10/100 /1000 Ethernet ports	
(ii)	Router should have at least 2 E1 ports with v.35 interface	
(iii)	Router should have one console port	
(iv)	Router should have at least 2.5 MPPS forwarding capacity at 64 byte	
(v)	Router should support ATM interfaces like E1 / E3 for legacy integration	
(vii)	Router should have redundant power supply	
(e)	Expansion for future use – Router should have minimum three expandable slot	
(f)	Router must have following	
1	Frame relay protocol	
3	PPPOE (service / client) Protocol	
4	Router should support HDLC Protocol	
5	Router should support 802.1q Protocol	
6	Router should support MPLS Protocol	
8	Router should support NAT	
9	Router should support IGMPv3	
10	Router should support DHCP (Server / client / relay)	
11	Router should support IP multicast	
12	Router should support cRTP or equivalent	
13	Router should support netflow	
14	Router should support GRE	
15	Router should support multicast	
(g)	Routing – Router must have	
1	Router should support static Routing	
2	Router should support RIPv2	
3	Router should support OSPFv3	
4	Router should support BGPv4	
(h)	Security feature – Router must have	
1	a. Router should support firewall and IPS	
2	b. Router should have IPSEC 3DES & AES, MPLS VPN. IPsec should be hardware accelerated to offload the router CPU.	
(i)	(c) Physical environment	
1	a. Router should be operable from 0' to 40'C under normal conditions	

**19. Technical Specifications of Router for Single Office at Remote Locations**

S/N	Specifications	Compliance
(a)	General – Multi-service access router should support secure intranet & Network access with VPN & Firewall protection along with VLAN and should be EAL3 certified or higher. It should be possible to run all the services together like Security, MPLS, IPv6 and other services	
(b)	CPU – Should be have at least 500 MHz speed	
(c)	Memory – Flash memory should be minimum 8 MB and expandable at least to 32 MB or more and DRAM should be at least 4 GB or more	
(d)	Physical ports	
(i)	Router should have at least 4 10/100 /1000 Mbps Ethernet ports	
(ii)	Router should have at least 2 E1 ports with v.35 interface	
(iii)	Router should have one console port	
(iv)	Router should have at least 1.5 MPPS forwarding capacity at 64 byte	
(v)	Router should support ATM interfaces like E1 / E3 for legacy integration	
(vii)	Router should have redundant power supply	
(e)	Expansion for future use – Router should have minimum three expandable slot	
(f)	Router must have following	
1	Frame relay protocol	
3	PPPOE (service / client) Protocol	
4	Router should support HDLC Protocol	
5	Router should support 802.1q Protocol	
6	Router should support MPLS Protocol	
8	Router should support NAT	
9	Router should support IGMPv3	
10	Router should support DHCP (Server / client / relay)	
11	Router should support IP multicast	
12	Router should support compress RTP or equivalent	
13	Router should support netflow	
14	Router should support GRE	
15	Router should support multicast	
(g)	Routing – Router must have	
1	Router should support static Routing	
2	Router should support RIPv2	
3	Router should support OSPFv3	
4	Router should support BGPv4	
(h)	Security feature – Router must have	
1	a. Router should support firewall and IPS	
2	b. Router should have IPSEC 3DES & AES, MPLS VPN. IPsec should be hardware accelerated to offload the router CPU.	
(i)	(c) Physical environment	
1	a. Router should be operable from 0' to 40'C under normal conditions	

*Handwritten signatures and initials*

**20. Technical Specifications for Internet Router**

This will not be used for any other service and therefore bidder should propose dedicated router. The specs are as below: -

S/N	Specifications	Compliance
1.	Router should be handled 1 Gbps of Internet traffic and should it should be possible to upgrade up to 3 Gbps internet traffic	
2.	The router should have 4 GE and must have at least 1 slot free to accommodate future requirement like E1, E3 or STM-1.	
3.	Router should be EAL 3 certified or higher	
4.	Router must have netflow for traffic analysis & management	
5.	Router must have network address translation	
6.	The router shall have modular operating system	
7.	If any of the services on the router works on a module, at least two of those modules shall be quoted to ensure redundancy of the solution.	
8.	Router should support RIP, OSPF & BGP, MPLS feature from day one for IPv4 & IPv6	
9.	Router must have following	
a)	Frame relay protocol	
b)	PPPOE (service / client) Protocol	
c)	Router should support HDLC Protocol	
d)	Router should support 802.1q Protocol	
e)	Router should support MPLS Protocol	
f)	Router should support NAT	
g)	Router should support IGMPv3	
h)	Router should support DHCP (Server / client / relay)	
i)	Router should support IP multicast	
j)	Router should support compress RTP or equivalent	
k)	Router should support netflow	
l)	Router should support GRE	
m)	Router should support multicast	
10.	Routing – Router must have	
a)	Router should support static Routing	
b)	Router should support RIPv2	
c)	Router should support OSPFv3	
d)	Router should support BGPv4	

**21. Technical Specifications for WAN Optimization for DC & DR**

S/N	Specifications	Compliance
1	Should support minimum Bandwidth throughput of 400 Mbps or more towards WAN and shall have minimum 48 GB of memory	
2	Should support minimum of 55000 Optimized TCP Connections from Day one	
3	In case of WAN outage or centralized application server not being available, the solution should be able to provide Read-only view of the files / content.	
4	Should be capable to support minimum 700 remote locations WAN optimization Devices	

5	Solution should offer authentication, authorization, and accounting (AAA) integration with external authentication providers such as Microsoft Active Directory, RADIUS, and TACACS etc.	
6	Should have 3-TB Usable HDD data storage with RAID-5 redundancy and HDD should be hot swappable	
7	Should have redundant and hot swappable power supplies.	
8	Should support at least 8 numbers of Inline Gigabit Ethernet Ports	
9	Should have support for optional 2 Numbers of 10 Gigabit Ethernet Ports and also should support Gigabit Sx Fibre port.	
10	All data on the WAN Optimization storage disk at DC/DR should be secured with 256 bit AES encryption and automatic key management. All private keys and SSL certificates should be stored in the central management device at DC/DR and same should not be distributed to the branch devices.	
11	The solution should be able to optimize application protocols like encrypted MAPI (EMAPI), Citrix, ICA, Signed SMB v2, HTTPS, HTTP and should be able to optimize and accelerate live video streaming and VOD.	
12	The device should be deployed in total transparent mode in the network and should preserve IP & TCP header information of the devices in the network so that not to disturb network service like QoS, Netflow, Access Control List (ACLs in router & firewall) and IP Service Level Agreements (SLAs)	
13	Should have redundant power supply	
14	Device should be IPv6 ready from day one	

**Appendix-"Ob"**

**22. Technical Specifications for Bandwidth Optimization for Multiple Offices at Remote Locations**

S/N	Specifications	Compliance
1	WAN Optimization solution to be provided at each location with the device having minimum of 4 GB of Memory for caching /data de-duplication to reduce traffic across WAN	
2	The Device should be able to support at least 30 Mbps or more WAN Bandwidth & 500 numbers of Optimized TCP Connections from day one and upgradable to 1000	
3	The solution should support Centralized Policy based management.	
4	The Solution should be transparent so that it can work with the Firewall, ACL, VPN, IPSEC and other networking devices in LAN / WAN Environment without disturbing existing environment	
5	The solution should have Binary increase congestion control for TCP traffic (BIC-TCP).	
6	Should have memory based caching	
7	Should have 500-GB HDD data storage with RAID-0 & 1 redundancy and HDD should be hot swappable	
8	All data on the WAN Optimization storage disk at DC/DR should be secured with 256 bit AES encryption and automatic key management. All private keys and SSL certificates should be stored in the central management device at DC/DR and same should not be distributed to the branch devices.	
9	The solution should be able to optimize application protocols like encrypted MAPI (EMAPI), Citrix, ICA, Signed SMB v2, HTTPS, HTTP and should be able to optimize and accelerate live video streaming and VOD.	

*Handwritten signatures and initials*



10	The device should be deployed in total transparent mode in the network and should preserve IP & TCP header information of the devices in the network so that not to disturb network service like QoS, Netflow, Access Control List (ACLs in router & firewall) and IP Service Level Agreements (SLAs)	
11	Should have redundant power supply	
12	Device should be IPv6 ready from day one.	

**Appendix-"Oc"**

**23. Technical Specifications for Bandwidth Optimization for Single Office at Remote Locations**

S/N	Specifications	Compliance
1	WAN Optimization solution to be provided at each location with the device having minimum of 4 GB of Memory for caching /data de-duplication to reduce traffic across WAN	
2	The Device should be able to support at least 20 Mbps WAN Bandwidth & 300 numbers of Optimized TCP Connections from day one and upgradable to 800	
3	The solution should support Centralized Policy based management.	
4	The Solution should be transparent so that it can work with the Firewall, ACL, VPN, IPSEC and other networking devices in LAN / WAN Environment without disturbing existing environment	
5	The solution should have Binary increase congestion control for TCP traffic (BIC-TCP).	
6	Should have memory based caching	
7	Should have 500-GB HDD data storage with RAID-0 & 1 redundancy and HDD should be hot swappable	
8	All data on the WAN Optimization storage disk at DC/DR should be secured with 256 bit AES encryption and automatic key management. All private keys and SSL certificates should be stored in the central management device at DC/DR and same should not be distributed to the branch devices.	
9	The solution should be able to optimize application protocols like encrypted MAPI (EMAPI), Citrix, ICA, Signed SMB v2, HTTPS, HTTP and should be able to optimize and accelerate live video streaming and VOD.	
10	The device should be deployed in total transparent mode in the network and should preserve IP & TCP header information of the devices in the network so that not to disturb network service like QoS, Netflow, Access Control List (ACLs in router & firewall) and IP Service Level Agreements (SLAs)	
11	Should have redundant power supply	
12	Device should be IPv6 ready from day one	

**Appendix-"P"**

**24. Technical Specifications for Radio/Voice Gateway for Offices at Remote Locations**

S/N	Specifications	Compliance
1.	Remote locations are required to provide Survivability Call Control functionality so that the Survivability system can provide fall back call control service in case the Edge locations loses all connectivity to the main Call Control cluster. It is expected that the survivability call control system will provide a minimal set of essential telephony features to the end-users that could be a subset of the feature that are available from the main call control cluster.	

2.	Each location should support IP phone of region configured	
3.	Should support variety of interface like FXS, FXO, E&M, T1/E1 to connect to PSTN	
4.	Should have at least One Channelized E1/PRI Interface at 53 locations, Two Channelized E1/PRI Interface at 06 locations, Three Channelized E1/PRI Interface at 02 locations, and Four Channelized E1/PRI Interface at 01 location	
5.	Radio gateway should have at least Two E&M ports at 53 locations, Four E&M ports at 07 locations, Six E&M ports at 01 location, an Eight E&M ports at 1 location	
6.	Gateway should have conferencing services to support multiparty audio / video conference for at least 4 conferences of 4 participants at 53 locations, 6 conferences of 4 participants at 07 locations, and 8 conferences of 4 participants at 02 locations	
7.	Voice gateway should register at least - 20 IP Phones from day one and expandable up to 100 IP Phones in future at 53 locations, 40 IP Phones from day one and expandable to 200 IP Phones in future at 07 locations, 80 IP Phones from day one and expandable to 400 IP Phones in future at 02 locations and 73 IP Phones from day one and expandable to 700 IP Phones in future at 01 location.	
8.	Gateway should have redundant power supply	

**Note:** - Scope for channelized E1/PRI interfaces, E&M ports, conferencing services and IP phones registration at serial No.4, 5, 6, & 7 above respectively are subject to change since these are dependent on the number of offices at a particular location which may vary at the time of tendering.

**Appendix-"Q"**

**25. Technical Specifications for Radio Server at DC for Integration with Land System**

S/N	Specifications	Compliance
1.	The system should be a communication and collaboration platform that can provide inter-operability among Land Mobile radios, fixed-line public switched telephones, mobile phones, PCs, and IP phones.	
2.	The inter-operability system should support both point-to-point and point-to-multi-point communications among all the aforementioned terminals to facilitate smooth collaboration for units and individuals in different locations as well communication media over an IP network.	
3.	The system need to be based on IP technology so that it can ride on the converged IP infrastructure.	
4.	The ability for users to also respond to incidents or emergencies by using client software on their PCs, boosts organizational responsiveness as well as operational efficiency and effectiveness.	
5.	PC users should have communication access not only to PTT radio channels, but also to broadcast channels, direct two-way channels to other online PC users (point-to-point PTT connections), direct dial channels for dial-out to preconfigured public switched telephone network (PSTN) or IP phone numbers, or VTGs that are comprised of multiple channels and communication device types such as mobile phones and IP phones.	
6.	System should have gateways with E&M interface which has the features and functionality that makes it a TDM to IP gateway for analog and digital audio devices connected to the router port. The audio received on the voice port should be encoded with a standard audio codec, such as G.711 or G.729. Those audio samples should be packaged in standards-based Real-Time Transport Protocol (RTP) packets suitable for transport on an IP network. Now, these audio packets can be sent across the network to other gateways with different brands of radio systems either individually (unicast) or as a group (multicast).	

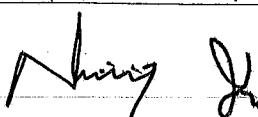
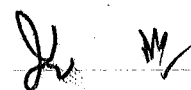
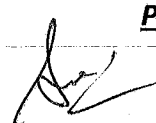
*[Handwritten signatures]*

7.	Administrator should be allowed to make policies with the intuitive web interface.	
8.	When an incident occurs, administrator can activate the policy from any Web browser-in the command centre.	
9.	Dispatchers who do not have access to the Web should be able to activate the policy from a phone by dialling a number and then entering the code for that policy.	
10.	There should be a provision for Policies to be activated automatically at a certain time of day.	
11.	System should be able to keep record of notification status so that the dispatcher can determine which people were reached and are available.	
12.	There should be a provision to check before admitting callers to a virtual group, the system validates that they are calling from a phone number that has been added to the system, and then authenticates the user based on a password.	
13.	The system along with the ability to dial out to PSTN phones and cell phones, should also allow dispatchers to patch in personnel who are outside of radio range, including off-duty personnel.	
14.	The system should allow authorized dispatcher or incident commander to activate a pre-established policy, including notification and talk group establishment from any Web browser or phone.	
15.	The system should support guaranteed message delivery using multiple channels, including cell phones, paging, and e-mail, enabling first responders to share crucial incident details with command even if the radio channel is overloaded during an emergency.	
16.	The system should have means to facilitate interagency collaboration while providing each participating entity the ability to selectively share and maintain control of its own resources.	
17.	The system should offer a dynamic mechanism with secure control and logical segmentation of the management, visibility, and access to system resources so that organizations can function fully independent and autonomously from on another.	
18.	The system should have the ability to share resources across organizational boundaries so that participants can share agreed-upon resources, such as channels or dispatchers, across operational views to facilitate collaboration among agencies, departments, or locations.	
19.	The system should allow organization to create separate operational views for its own resources, sharing resources only when needed for incident response.	
20.	The system should provide administrative console for system administration, and dispatch console for dispatch operation such as setting up talk groups that span tactical radio, IP phone, PC, fixed telephone, and mobile phone.	
21.	The dispatcher or operations manager should be remotely able to manager the availability of the channels on the push to talk client software over an IP network.	
22.	The system shall include multi-channel push-to-talk client software on touch-screen desktop or notebook PC for communication from the office or remote sites	
23.	Authorized users should be able to download the push-to-talk client software as operations or incidents require. This capability should allow users to quickly and easily participate in communications groups from any location.	
24.	The push to talk client software should be able to participate and monitor multiple communication channels simultaneously. It should be easy to add channels to push-to-talk client software as the need arises.	

*Handwritten signature*

*Handwritten signature*

25.	All the push-to-talk client software users should have communication access not only to PTT radio channels, but also to broadcast channels, direct two-way channels to other push-to-talk client software users (point-to-point PTT connections), direct dial channels for dial-out to preconfigured public switched telephone network (PSTN) or IP phone numbers, or Virtual Groups that are comprised of multiple channels and communication device types such as mobile phones and IP phones.	
26.	In case of primary interoperability Server be unavailable, push to talk client software users can continue to communicate and operate in an offline mode or log in to an alternate interoperability Server.	
27.	Push-to-talk client software should have following features :	
	a. Voice Replay	
	b. All Talk	
	c. Channel Select	
	d. Channel Recorder	
	e. Listen Only Channels	
	f. Volume control	
	g. Channel Names	
	h. Channel Colours	
28.	Push-to-talk client software should be able to support G.711 and G.729 as voice codecs	
29.	System should have Push To Talk Capable wired IP Phone which should allow users to communicate over and monitor broadcasts of channels of communications.	
	a) With a push of a single button on the phone, a user should be able to communicate over a channel to other users monitoring that channel.	
	b) It should be easy to add channels as the need/incidents arise.	
	c) The Push to talk capable wired IP Phone user should have communication access not only to PTT radio channels, but also to other such IP Phones users, or groups made up of multiple channels and communication device types such as mobile phones and IP phones	
	d) Users should have the capability to choose from a list of communication channels to participate and monitor.	
	e) In case of primary interoperability Server be unavailable, push to talk capable wired IP Phone users can continue to communicate over the selected channel and operate in an offline mode	
	f) These IP Phones should have the capability to monitor channels in listen-only mode even if permission to talk is not provided.	
30.	<b><u>Operating Condition.</u></b>	
	a) <b><u>Reliability.</u></b> The proposed equipment must be designed to cater for 24-hours around-the-clock operation.	
	b) <b><u>Maintainability.</u></b> Because there should be minimum down-time for all the components, factors such as ease of replacement, mean-time-to-repair (MTTR) has to be incorporated in the system design and proposal.	
	c) <b><u>User-Friendly.</u></b> The system server should be based Linux or Unix OS. At the same time, the administrative and dispatch console should be would wide web based, the multi-channel PTT SW client should operate on Windows XP OS. The IP phone should provide menu-driven interface.	
	d) <b><u>Upgradeability.</u></b> Each part of the system produced should be modular and easily re-configurable and upgradeable. The system should be based on an open system concept.	

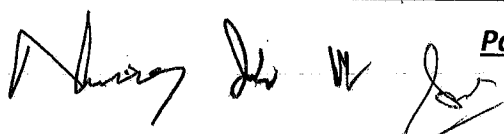
31.	The system shall have proper interfaces to all the PTT radios used by the FESA.	
32.	The system shall have the capability to support either E1 or FXS/FXO as interface to PSTN.	
33.	One complete set of necessary HW and SW that support the following should be provided	
	i PTT radio interfaces	
	ii PTT capable IP phones	
	iii Multi-Channel PTT client Software	
	iv Operational views for different units	
	v Virtual Groups	
	vi Dial In/ Dial out ports	
34.	<b>System Server</b>	
	The system server shall be supplied and equipped to support the following features and capabilities:	
	a) Operating System should be open system such as Unix or Linux.	
	b) Secure world wide web-based interface for system administration and dispatch operation setup.	
	c) The server needs to be able to support no less than 1000 users.	
	d) System log for the activities of the components, users, and PSTN dial-in and dial-out.	
	e) Status of components, channels and users.	
	f) At least 3 different system privileges for the users.	
	g) Capability to coordinate all the components of the system to dynamically combine different channels and users into a single channel.	
	h) IVR (Interactive Voice Response) and SIP trunk support for PSTN, Mobile phone, and IP phone dial-in and dial-out.	
	i) IETF RFC 2833 compliant in-band DTMF support for dial-in and dial-out calls	
	j) Dial in access to Channels.	
	k) Dial-out/Notify to bring in people. The notification can be through email, sms, or pagers.	
	l) Policy invocations and change PIN functionality	
	m) Integration with SMTP mail server to permit notification engine within the system to provide emergency notification by emails.	
	n) Integration with SMS gateway to permit notification engine within the system to provide emergency notification to all cell phones.	
35.	The system should have policy engine to provide the functions of notification to multiple end devices, such as, radio, IP Phone, cell phone, PSTN phone, PC using multiple media – audio and text.	
36.	The system should have the capability to integrate with 3 <sup>rd</sup> party system, such as, IP video surveillance, alarm management system, command & control system and so forth using open and standard protocol like http. Such http driven integration permit end user to do ad hoc on-the-fly policy based integration with any 3 <sup>rd</sup> party system without any forklift of system upgrade, modification, and so forth.	
37.	The system should have policy engine to permit end user to drive event based notification over different medias to many different devices	
38.	Licenses for integrating proposed HF/VHF devices/stations.	

Handwritten signatures and initials, including a large signature on the left and several smaller initials and signatures to its right.

## 26. Technical Specifications for Email Security Appliance

S/N	Feature	Specifications	Compliance
1.	Email GatewaySolution	The solution should be appliance based	
2.	Operating System - Threading Model	The operating system should use stack-less threads to use less system resources in order to deliver more concurrency and leave more RAM available for caching file system data and eliminate the risk of security holes and system crashes from stack overflows.	
3.	Operating System and MTA	The solution should use their own operating system and MTA on appliance and not open source operating system and MTA.	
4.	File System	The file system should be proprietary built and optimized for Messaging Queuing.	
5.	File System Redundancy	The file system on the appliance should provide Data Integrity During Failure	
6.	Inbound and Outbound Traffic Control	The solution should support both inbound and outbound traffic control on single appliance	
7.	MTA Vulnerability	There should not be any known vulnerability of MTA.	
8.	MTA Design	The MTA should have been built by stack-less programming language that helps to improve the overall performance of the MTA by opening more threads resulting in more number of concurrent TCP connections.	
9.	Mail Queue Handling	The MTA should maintain separate queues for each destination domain to avoid single queue issues.	
10.	MTA Retry Schedule	The MTA should have the ability to set the retry schedule on a per domain basis.	
11.	MTA connection capabilities	The MTA should be able to send multiple messages per connection and be able to open multiple connections per host.	
12.	MTA RFC Support	The MTA should support RFC 2821 compliant Simple Mail Transfer Protocol (SMTP) to accept and deliver messages.	
13.	MTA performance (burdened)	Each appliance provisioned should be able deliver burdened (all engines like AV/Anti-spam/End User quarantine enabled) performance of at least 30,000messages per hour of 21 KB message size.	
14.	Concurrent SMTP sessions	Should support up to 3,000 concurrent SMTP sessions	
15.	Denial of Service Defense	The solution should have ability to perform SMTP session control and traffic rate limiting (down to number of recipients) according to sender's IP address/range, domain or email reputation. The solution should be able to assign maximum SMTP sessions per IP address on appliance	
16.	Directory Harvest Attack Prevention	The solution should be able to communicate with Open LDAP, Active Directory or other LDAP servers to identify invalid recipients	
		The solution should perform SMTP conversational bounce for invalid recipients (prevent Non-Delivery Report Attack)	
		The Directory harvest prevention should control the maximum number of bounces per hour due to invalid email recipients according to sender's IP address/range, domain and email reputation	
		The directory harvest attack prevention should allow administrator to define limit on no. of invalid recipient requests that can be accepted.	

17.	Reputation Based Filtering at SMTP conversation level	The reputation based filtering should have one of the biggest web and email traffic monitoring network for sender reputation	
		The reputation filtering should be used by majority of largest ISP's in the world	
		The reputation filtering should assign score to every connecting IP/Domain identifying bad, suspected and good senders	
		The solution should allow administrator to apply policies such as blocking known bad senders, throttling suspicious senders and allowing trusted senders based on reputation score assigned from reputation database	
		The reputation based scoring architecture should function at TCP conversation level and not after acceptance of email, to increase the overall performance & availability of the messaging infrastructure	
		The reputation score for every sender should be arrived after analyzing at least 120 smtp & web parameters for complete & accurate understanding of senders	
18.	Manual Whitelist/Blacklist/Suspect List	The solution should support creation of customized sender groups and apply customized mail flow policies to each sender group. Blacklists (IP, Domain, Reputation) Whitelists (IP, Domain, Reputation) Third party RBLs/ORBLs Sender and Recipient address whitelist and blacklist	
19.	Email Throttling	The solution should be able to block, accept, reject and TCP refuse based on:- - Sender IP, IP range - Domain - Email Reputation score from reputation filtering - DNS List - Connecting host PTR record - Connecting host PTR record lookup fails due to temporary DNS failure - Connecting host reverse DNS lookup (PTR) does not match the forward DNS lookup (A)	
20.	Traffic Rate Control	Rate limit control by IP address, domain and sender's reputation Maximum Recipients per period traffic control Ability to define traffic flow based on time period	
21.	Email Traffic Monitor and Attack Detection	Real-Time Mail Flow Monitoring (provide details of traffic flow down to per domain and IP address)	
		Statistics on Invalid Recipients, Stopped by Reputation, Spams and Viruses Detected, and Cleaned Messages (Per Domain and IP address)	
		Could provide real-time last hour, last day, last week and last month statistics on blocked messages by rate limit, rejected connection, spams and virus messages detected, and also received byte count according to IP address or domain	
22.	Bounce Verification (Misdirected Bounce Handling)	To combat misdirected bounce attacks, the solution should support bounce verification tag to replace envelope sender for all outgoing messages; if a bounce arrives that doesn't contain the tag then it is discarded. Legitimate bounces should be delivered	



23.	Multiple Host Identities	The solution should support assigning different IP addresses on single appliance to allow different host identities and also own traffic flow policy and sender groups (each IP address represents one department or one faculty MX host)	
		Each IP address should be able to respond with different SMTP response and banner	
		The solution should support customized SMTP banner, hostname and response code per IP address or sender group	
24.	Support for Multiple Domains	The solution should support multiple domains per IP address or multiple domains using different IP address on single appliance	
25.	User Policy Management	The solution should support Per User or User Group Policy (Based on sender/recipient address/domain or LDAP group, i.e. single email to multiple recipients can be processed with different policies)	
		Should have single view of all user policies for easier management	
26.	Fine-grained Mail Policies	The policy at SMTP conversation level should be able to perform reverse DNS domain lookup and assign policy per sender basis.	
		Per Sender Policy settings on:- Maximum Messages per connection Maximum Recipients per message Maximum message size Maximum Concurrent sessions per IP address TLS enforcement and preferred option SMTP Authentication enforcement and preferred option	
27.	Attachment Filtering	File attachment detection by true file type, file size, file name, file extension and MIME type	
		Ability to quarantine, duplicate and quarantine, strip attachment, BCC or redirection of email to another host or another recipient, replacing the whole message or just attachment with predefined message notification template	
28.	Sender Verification	Sender Verification based on connecting IP address DNS PTR record and also envelope sender address	
29.	LDAP support	Should support LDAP routing, masquerading, recipient address verification and SMTPAUTH over LDAP	
		LDAP should be query based and not synchronization based for better performance. The solution should support chain LDAP queries.	
30.	LDAP	The solution should support chained LDAP queries that will run in succession.	
31.	LDAP Referrals	The solution should support LDAP referrals i.e. When using LDAP referral's, the original query gets referred to another LDAP server.	
32.	LDAP Caching	The solution should support LDAP caching on the appliance.	
33.	Quarantine Access Control	Per quarantine area access control and ability to control user name and password of quarantine areas so that some quarantine areas can only access by authorized personnel (e.g. "Confidential" Quarantine Area for Security Administrator, HR, etc.)	
34.	Content Filters	The solution should support both command line and GUI content filters to allow complex policy control requirements. The solution should support content filtering at global and per user level along with weighted content dictionaries for intelligent key word scanning in message body.	



35.	Data Loss Prevention	The appliance should support comprehensive data loss prevention policies through a simple interface that enables mail administrators to ensure that confidential information is not sent out over email. This DLP module should be on-box and should have at least 100 ready to use DLP templates.	
36.	Email Encryption from Gateway to End Recipient User	The appliance should support policy based encryption of outbound email at the gateway without the need or complexity of managing certificates or client side software.	
37.	Image Analysis capability	The appliance should support Image Analysis capability if needed in order to detect adult or pornographic content in emails.	
38.	Trusted Relay	The solution should support trusted relay so that original senders' IP address can be identified from "Received" headers or other email headers (when appliance is not first layer mail gateway)	
39.	Multi-layer Anti-spam filter	Reputation Filtering (Sender IP/domain) Reactive Anti-spam Filtering context-sensitive detection technology email and web reputation technology	
40.	Anti-spam Filter	Integrated anti-spam filter within the appliance Allow per user or user group to use different anti-spam vendor engines	
41.	Spam Rules Configuration & Management	The spam rules should be able to update automatically at least every 5 minutes	
42.	Real Time Attack Detection and Policy Change	Real-Time Mail Policy Change on Possible Spammers and Hackers (by Per Domain and IP address) so as to change the policy to block/throttle those bad senders	
43.	Quarantine	On-box quarantine for administrator	
		Individual User/Password Access Control per Quarantine Area	
		End User Quarantine Support with LDAP/AD/IMAP/POP authentication support	
44.	Hardware Appliance for End User Quarantine and Management	On-box and off-box End User Quarantine option	
		Management Appliance option for End User Quarantine	
45.	Plugin Support	Outlook Plugin support for reporting missing spams, false positives, phishing and virus emails	
46.	Virus scanning	The solution should have dual virus scanning support available and the anti-virus engines should be Integrated within the appliance	
47.	Virus Outbreak Filter	The solution should provide virus outbreak prevention(zero day virus protection) on abnormal increase of emails with specific email attachments or URL's	
48.	Outbreak Quarantine	Automatic quarantine and release of quarantined messages not falling into new virus/worm characteristics upon outbreak rule update and before virus signature update)	
49.	Signature/Rules Update Period	Configurable update period down to at least every 5minutes automatically	
50.	File scanning	The solution should support attachment and Compressed File scanning	

51.	Reports and logs	Graphical monitor of both incoming and outgoing email flow for last hour, last day, last week and last month	
		Log of Each Email's Processing	
		Mail Flow Report (e.g. able to list out all messages to a specific recipients within certain time period, with details how the messages are received, processed and delivered/dropped)	
		Mail statistics and throughput	
52.	Multiple DNS Servers	Support both Internet Root DNS servers or local DNS servers	
		Support multiple DNS servers according to destination domain(s), i.e. DNS A server for Domain A, and DNS B server for Domain B	
53.	Message Tracking	Centralized message tracking based on sender and/or recipient address/domain, subject, time period, message event for multiple appliances	
54.	System monitoring	The solution should support following for system monitoring:- SNMP v2/v3 support MIB-II XML Syslog	
55.	Report API support	The solution should support API to build customized reports	
56.	Alerts	Email-based SNMP Trap	
57.	Configuration Interfaces	Web UI (HTTP and HTTPS) CLI (SSH and Telnet) File transfer (SCP or FTP)	
58.	Configuration files	XML/text based files archived or transfer	
59.	Centralized management	The solution should support centralized management for managing and configuring multiple appliance without the need for additional dedicated management console	
		The solution should allow policies to apply based on cluster, group or per machine	
60.	Remote Support	The solution should have support for: Built-in command to consolidate diagnostic information and configuration and send to customer support Ability to enable remote tunnel support for remote diagnosis	
61.	Support	Remote support from parent company should be available. The parent company should provide Toll Free Support, Email Support and should also provide Support Portal access.	
62.	Updates	System updates (able to upgrade and restore email service within 5 minutes) Automatic Spam definition updates Automatic Virus definition updates	
63.	Outbound Mail Monitoring	Real-Time Outbound Mail Flow per IP/Domain Distinct Message Queue Per Destination Domain	
64.	Destination Domain Rate Control	The solution should support domain-based Delivery Rate and Session Control	
65.	Footer or Disclaimer	The solution should support addition of different footers or disclaimers based on sender domain or sender email address/group	
66.	TLS Support	The solution should support outbound SMTP over TLS based on destination domains or system-wide	
67.	Outbound SMTP Authentication Support	The solution should support outbound SMTP authentication	

68.	Multiple IP Address Delivery Support	Multiple IP address support (up to 4 IP addresses) allow emails to be sent by different IP addresses based on email sender, subject, size, recipient, etc.	
69.	Domain Key Signing	The solution should support policies to sign outgoing emails based on domain key and allow to sign by different domain keys based on sender domain	
70.	Bounce Management	The administrator should be able to define different bounce profiles for destination domains (retry frequency, maximum retry period, etc.) to minimize bandwidth for non-important emails	
71.	End user Safe-list and Block-list	The solution should have support for end user to create block/black and safe/white lists. Safe/white lists allow a user to ensure that certain users or domains are never scanned with anti-spam scanning engines, while block/black lists ensure that certain users or domains are rejected or quarantined	
72.	External Authentication	The solution should have provision to authenticate users using RADIUS or LDAP for logging into appliance for management purpose	
73.	Outbound Spoof verification	If SMTP authentication is used to send messages, the solution should have facility to check messages with spoofed headers.	
74.	Patch Support	Patch installation should support for new release	

**Appendix-"S"**

**27. Technical Specifications for Voice/IP (IPPBX) Server**

**A) IPPBX**

1. The IP telephony system should be a converged communication System with ability to run TDM and IP on the same platform using same software load based on server and Gateway architecture. The system should be capable of supporting Analogue and IP Telephones. The single IP EPABX system should be provisioned to support up to 10000 stations (any mix/percentage of Analog/IP) to achieve the future capacity. All the users to be managed in a single database, which is managed centrally, no multiple databases. CLI facility for all users should be provisioned from day 1. It should be equipped with 750 numbers IP Phone licenses and 3000 numbers of Analog Phones licenses from day one.
2. The system should be based on server gateway architecture with external appliance server running on Linux OS. No card based processor systems should be quoted.
3. The voice network architecture and call control functionality should be based on SIP.
4. The Communication Server/Call Server would be deployed in a active-active configuration over the distributed IP infrastructure (LAN/WAN). The call control system should be fully redundant solution with NO single point of failure & should provide 1:1 redundancy. Both the servers should do call processing all the time and act as backup in case of the failure of one server.
5. The system to have distributed architecture and the centralized control for all the IP PBX entities in the network. It should be possible to have centralized applications like voice mail, UC for the network users.
6. The communication feature server and gateway should support IP V6 from day 1 so as to be future proof.
7. It is required to provide Survivable Call Control functionality so that the survivable system at the remote location shall provide fall back call control service in case the remote site loses all connectivity to the main Call Control system placed at HQ datacentre. It is expected that the survivability call control system will provide a minimal set of essential telephony features to the end-users that could be a subset of the feature that are available from the main call control system.
8. It should be possible for the IP phone to be connected on the same line which is connected to the computer i.e. Single wire to desk.

9. Call control server/ appliance should be Intel based hardware with necessary configuration to support the desired expandability. No proprietary hardware is acceptable.
10. The system software version offered should be the latest release as on the date of supply of EPABX as available globally.
11. The offered solution must provide a standard based mechanism for QoS implementation.
12. System should allow direct registration / profile creation of SIP endpoints onto it and perform all functions of Proxy/ Registrar / Redirect etc.
13. In progress PSTN Calls at each of the locations should not be interrupted in the event of any WAN link failure or a call control server failure.
14. Quality of Services (QoS) would be configured to administer the call and ensure voice traffic get priority over normal traffic.
15. The System should support Call Admission Control to configure number of calls that can be active between locations —inter-cluster and intra-cluster.
16. Should support LDAP integration for directory synchronization & user authentication.

#### **Support for call-processing and call-control.**

1. Should support signalling standards/Protocols – SIP, MGCP, H.323, Q. Sig.
2. Voice CODEC support - G.711, G.729, G.729ab, G.722, ILBC
3. Video codecs: H.261, H.263, H.264, and Wideband Video Codec
4. Video telephony support (H.323, and SIP)
5. Support for configuration database (contains system and device configuration information, including dial plan)
6. Having inbuilt administration web based administration. No additional thick client for administration on the Admin PC. Should also support HTTPS for management.
7. Should support 6 party ad-hoc conferencing.
8. IP Phone Address Book Synchronizer—allows users to synchronize Microsoft Outlook or Outlook Express address books with Personal Address Book.
9. Should provide Single Number Reach (Simultaneous Ring on IP phone and user defined alternate phone) for all the IP phone users.

#### **System Management & monitoring**

1. The System should have GUI support web based management console
2. System should provide management tool to monitor system performance, device status, device discovery and CTI applications.
3. Should provide alert notifications for troubleshooting performance
4. It should support secure HTTPS & TCP to troubleshoot system problems.
5. Generate various alerts in the form of e-mails, for objects when values go over/below pre-configured threshold levels.
6. Should monitor the system in real-time on a set of preconfigured parameters.
7. It should be possible to configure the sample interval rate for the applicable performance monitoring.
8. The management platforms must provide different levels for accessing the system based on the role being played by the user who is accessing the system. The administrator should have the highest authority.
9. Should provide a daily summary report of key monitoring parameters like Call Activity (No of calls attempts and completed), Device status (Number of registered phones / gateways / trunks per server), server status (load on server resources), alert status etc.

#### **Security**

1. The protection of signalling connections over IP by means of authentication, Integrity and encryption should be carried out using TLS.
2. The password and Access Control must include the following:
  - a. Passwords to prevent the possibility of an aggressor to easily read or deduce system or account access password.
  - b. Password aging with Configurable time periods.
3. System should support MLPP feature.
4. Proposed system should support SRTP for media encryption and signalling encryption by TLS.

5. Secure HTTP support for Call Server Administration, Serviceability, User Pages, and Call Detail Record Analysis and Reporting Tool. Should support Secure Sockets Layer (SSL) for directory.
6. The administrator logging on to the call control server needs to authenticate by suitable mechanism such as User Login Information and Passwords/ Radius Server.

**End user / system Features required:**

- 1) Extension mobility
- 2) Message-waiting indicator (MWI)
- 3) Hunt groups
- 4) Dial-plan partitioning
- 5) The system should support at least 12 digit numbering scheme.
- 6) Distributed call processing
- 7) Hotline and private line automated ring down (PLAR)
- 8) Interface to H.323 gatekeeper for scalability, CAC, and redundancy
- 9) Multi-Level Precedence and Pre-emption (MLPP)
- 10) Q.SIG (International Organization for Standardization [ISO])
- 11) Secure HTTP support for Call Server Administration, Serviceability, User Pages, and Call Detail Record Analysis and Reporting Tool.
- 12) Secure Sockets Layer (SSL) for directory
- 13) Phone Security: TFTP files (configuration and firmware loads) are signed with the self-signed certificate of the TFTP server. The Call Server system admin will be able to disable http and telnet on the IP phones
- 14) SIP trunk (RFC 3261) and line side (RFC 3261-based services)
- 15) SIP trunk Call Admission Control (SIP CAC)
- 16) Time-of-day, day-of-week, and day-of-year routing and restrictions
- 17) The proposed system should support automatic route selection (ARS) and least Cost routing (LCR) features to route the calls based on priorities related to user profile, tariff, and network availability, along the most cost-effective path. This service will be transparent for users and irrespective of the physical carrier connection.
- 18) **Distinctive Ringing.** The system should provide audibly different station ringing patterns to distinguish between internal and external calls

**User Features**

1. Abbreviated Dial
2. Call back busy, no reply to station
3. Call park and pickup
4. Call status per line (state, duration, number)
5. Calling Line Identification (CLID)
6. Calling party name identification (CNID)
7. Direct inward dial (DID)
8. Direct outward dial (DOD)
9. Directory dial from phone—corporate, personal
10. Directories—missed, placed, received calls list stored on selected IP phones
11. Distinctive ring (on net vs. off net)
12. Shared Line support
13. Message waiting indication ( Visual and Audio )
14. Multiple line appearances per phone
15. Music-on-hold
16. Station volume controls (audio, ringer)
17. Transfer
18. Video (SIP and H.323)
19. Boss-secretary feature support
20. On-hook dialling
21. Call waiting
22. Call Conference.

### **Presence Services for IP phone users:**

The bidders should provide a "presence" application for all IP Phones users, so that they can see the availability status of his contacts in their buddy list.

- a. The common supported status for this application should be available, busy, idle, away etc."
- b. Should provide network based presence. This means that the user should be able to see the communication channel on which the other user is available; like chat, phone, video, email etc. If the remote user has not logged on to the presence client, primary user should be able to contact the person through phone, email etc.
- c. Should support the users to see other user's IP phone's on/off hook states
- d. The instant messaging application should support manual setting of user status to: Available, Away, Do Not Disturb (DND), Logged Off etc.
- e. Should support management of contact list, IM history, and personal settings.
- f. Shall provide support for open protocols like XMPP.
- g. Presence based desktop application shall allow escalation of Instant Message to Audio call and further to Video call
- h. Should support management of contact list, IM history, and personal settings from Presence based desktop application
- i. Presence based desktop application shall support logging of Instant Messages for compliance purpose if any.
- j. Should provide SSH and HTTPS access to management platform for enhanced security.
- k. Should support click to call, click to Video and click to conference features.

### **Video Telephony Features and Support:**

The call control system should provide integrated video telephony features to the users so that user with IP Phone / Soft phone and video telephony end point should be able to place video calls with the same user model as audio calls.

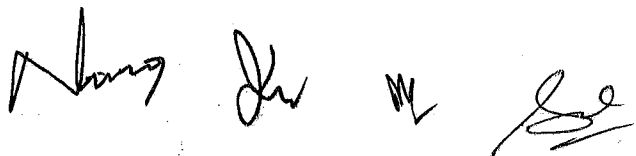
- a. The users should be able to transfer video calls as audio calls
- b. It should be possible to have multiparty video call through the conferencing system.
- c. Call-Server should provide a common control agent for signalling, configuration, and serviceability for voice or video end points.
- d. Call control system should handle CODEC and video capabilities of the endpoints, bandwidth negotiation to determine if video/audio call can take place.

## **B) IP Phones:**

### **B-1) Video IP Phone**

The IP Video phone should meet the following requirements –

- (a) Have high-resolution 640 x 480 pixel backlit display with 5" or higher LCD Screen with integrated video Camera.
- (b) Have Intuitive user interface and keypad for quick access to all IP phone and video services
- (c) Have an integrated 2-port 10/100/1000 Ethernet switch.
- (d) Support Bluetooth 2.0 or above and RJ-9 interface for headsets.
- (e) Should have 3 or more programmable line keys.
- (f) Should have 4 or more programmable soft keys.
- (g) SIP support for signalling.
- (h) Audio Codec Support: G.711, G.729.
- (i) Video Codec Support: using H.264 up to 30 fps.
- (j) It support XML based applications for productivity enhancement.
- (k) Should support VPN client on Phone.
- (l) Full-duplex speakerphone with high-definition voice support for handset, headset and speaker



**B-2) Non Video IP PHONE**

The phone should meet the following specifications

- (a) The phone should be a SIP based
- (b) Should have 320 x 160 or better pixel-based display.
- (c) Should have full duplex speaker phone and dedicated headset port with RJ-9 interface.
- (d) It should support G.711, G.729a/b audio compression codecs.
- (e) Should provide the directory services to the user by displaying the missed, received and dialed call details including the caller ID and calling time.
- (f) Should have 3 or more programmable line keys.
- (g) Should have 4 or more programmable soft keys.
- (h) Should have at least 10 fixed feature keys.
- (i) Should support IEEE 802.3af POE, and external AC power adapter option.
- (j) The phone should have two 10/100/1000BASE-T Ethernet ports, one for the LAN connection and the other for connecting to PC/laptop.
- (k) The phone should support QoS mechanism through 802.1p/q.
- (l) The phone should support XML based services and applications.

Note: - The End to End IP Voice Network solution should be provided from same OEM.

**Appendix-"T"**

**28. Technical Specifications for Video Conferencing System:**

SN	Features	Specifications
1	<b>VIDEO</b>	
	<b>(a) Signal System</b>	The system should support PAL and should be a point-to-point system with codec, Full High Definition 1920x1080p camera with a minimum of 10xzoom, MIC, remote control, cable and power supply.
	<b>(b) Standards and Protocol</b>	H.263, H.264 or better
	<b>(c) Resolution</b>	The system should supports video resolution from 4CIF (Common Intermediate format), VGA, SVGA, HD-1080p @25fps. The PC resolution should be 720p OR 1080P
	<b>(d) Frame Rate</b>	25fps / 30 fps
	<b>(e) Band Width</b>	<b>Option – 1</b> Up to 4Mbps point to point on IP <b>Option - 2</b> Up to 2 Mbps ISDN ( Internal/External) Note:- User department may select any of the option or combination of these as per their requirement.
	<b>(f) Video Inputs</b>	The system should have 2 Video Inputs to connect 1XHD camera and 1 for PC DVI (Digital Video Interface)
	<b>(g) Video Outputs</b>	The system should have 2 video outputs 2XHDMI (High-Definition Multimedia Interface)/DVI for connecting two HD displays :DVI
	<b>(h) Graphics</b>	Native 16:9 widescreen, Advance screen layout, Intelligent video management local auto layout
	<b>(i) Picture in picture</b>	Should support picture in picture (PIP)
2	<b>AUDIO</b>	
	<b>(a) Standards &amp; Protocol</b>	G.711,G.722,G.722,1 or better
	<b>(b) Features</b>	CD-Quality audio or Equivalent or Higher
		Instant Adaptation Echo Cancellation or Equivalent or Higher
		Automatic Gain control (AGC)or Equivalent or Higher
Automatic Noise suppression (ANS)or Equivalent or Higher		

	<b>(c) Audio Inputs</b>	The system should have 2 Audio inputs (2XRCA Phone connectors ) or Equivalent or Higher
	<b>(d) Audio Outputs</b>	The system should have 2XRCA Phono or Equivalent or Higher
	<b>(e) Lip synchronization</b>	Active Lip Synchronization or Equivalent or Higher
<b>3</b>		<b>NETWORK</b>
	<b>(a) Features</b>	The system should support IPv4 & IPv6 The system should have features such as QoS / RSVP Standards or equivalent or higher , Packet loss based down speeding TCP/IP, DHCP (Dynamic Host Configuration Protocol), Auto Gatekeeper discovery, Dynamic Layout/lip sync buffering, DTMF (Dual tone multi frequency signaling tone, Date and Time.
	<b>(b) ITU-T standards</b>	DUAL STREAM:- The system should have capability to support H.239 in both H.323 and SIP mode
	<b>(c) Net work Protocols</b>	The system should have H.323 and SIP capability
	<b>(d) Interfaces</b>	IXLAN/Ethernet (RJ-45) 10/100 and 1 USB
<b>4</b>	<b>Camera</b>	Should have PTZ Feature
	<b>(a) Image sensor</b>	1/3 CCD / CMOS or equivalent
	<b>(b) Pan</b>	+/- 75° or more
	<b>(c). Tilt</b>	+ 10° /- 15 ° or more.
	<b>(d) Focus</b>	Automatic / Manual.
	<b>(e) Total field of view</b>	250° or better'
	<b>(f) Horizontal view angle</b>	65 ° or better
	<b>(g) Zoom ratio</b>	10x Zoom optical or better
<b>5</b>	<b>Remote Commander</b>	IR/ Wireless
<b>6</b>	<b>Microphone</b>	360 voice pickup microphone
<b>7</b>	<b>MULTI CONTROL UNIT</b>	
	<b>(a) Dimension</b>	The MCU must be up to 2/3 Units rack solution provided with all the necessary accessories to integrate into a 19" rack.
		Option -1: - 24 ports @ 4Mbps with HD 720p resolution should be supported on the same chassis/module without cascading with rate matching. 24 ports MCU with HD 720p resolution must be supported half of its capacity i.e. 12 ports at HD 1080p resolution from day one. Option 2: - N Ports@ 4Mbps with HD 1920x1080p resolution should be supported on same chassis/module without cascading with rate matching and should be capable to support increased proportionate Nos. of video sites on reduced bandwidth. Note: - One of the above mentioned Option may be selected by user department and Number of Port may vary depending on requirement of user department.
		ii) The MCU should additionally support with a minimum of 10 audio only participants.
		iii) The MCU should be accompanied with external/internal 2 PRI- ISDN gateway on same chassis or different chassis, Flexible design enables streamlined traffic flow and mass scale for converged IP Networks. (User department can extend the scalability to N PRI internal/external depending upon their requirement. Where N is to be decided by user)
	iv) The system should be HD enabled supporting. HD 720p @ 25 frames in continuous presence mode and it should support 1080p	
	<b>(b) Capacity</b>	v) The MCU must support 2 Nos of 10/100/1000 Mbps Ethernet.

*Mary*

*M*

*[Signature]*



<b>(c) Audio support</b>	Audio Codecs G.711, G.722 G.722.1 or better
<b>(d) Video Support</b>	Video codec H.263, H.264 or better
<b>(e) Gatekeeper,</b>	MCU shall support an embedded/external Gatekeeper, Management tool scheduling and address book, MCU shall have the capability to connect the PC/laptop for presentation sharing over LAN/IP network.
<b>(f) No of conferences</b>	MCU should support multiple conferences as per the virtual MCU port capacity with flexible resource Capacity by using 24 / N ports. Conferencing highlights personnel layout, auto layout, border for active, speaker indication, lecture and presenting mode, conference profiles
<b>(g) Continuous presence view</b>	MCU should support 16 Continuous Presence (CP) on a single screen.
<b>(h) Interactive keypad</b>	MCU shall have a built- in auto- attendant from whom users can select conferences to join or start a new conference. This shall be operated using either DTMF or' FECC (For End and Camera Control),
<b>(i) Dynamic CP layout</b>	The MCU should support dynamic layouts wherein layout should adjust based on the participants joining the calls. MCU shall support Automatic down speeding and packet error/lose concealment methods to ensure optimum video, and audio quality. The MCU must provide standards based on method of compensating and correcting for packet loss of media streams.
<b>( j) Chairperson View</b>	It should have chairperson/Administrator view.
<b>(k) Far End Camera Control (FECC) and volume control</b>	It should be possible to control far end camera with a facility to increase or decrease volume of end point.
<b>(l) H-239 Support</b>	The MCU shall support H. 239/ chair control
<b>(m) Dial- out capability</b>	Should dial out automatically to all participants, retry dial out conferences to complete call setup and should report specific failures. MCU shall support dual video H.239 and ability to send content to legacy protocols that do not support H.239 through it main video.
<b>(n) Dial- in Capability</b>	Should offer robust software driven dial-in and/or dial out capability. MCU shall' have in built /external capability to support PC based desktop clients for 12 PC users or more.
<b>(o) Security</b>	The MCU should support one level or more of conference password-Chair Person and Participant password. The administration of the Video endpoint should be through Web interface using HTTPS/HTTP (Hyper Text Transfer Protocol Secure)
<b>(p) Other Features</b>	i) MCU shall provide HD quality in continuous presence to all HD endpoints connected and deliver this even if SD or HD end points or port of the conference. MCU have the ability to enhance the resolution even from the SD or ED Endpoints and send to HD participants. The solution shall support standard definition, and high definition in both voices activated and continuous presence mode without loss of functionality or capacity.
	ii) MCU shall support communication up to 4 Mbps per port using both H.263 and H.264 video.
	iii) MCU shall support conferences that permanently exist but use no resources/port if no. Participants are in the conference. The functionality gives end user the flexibility to
	Directly join the conference without having to depend or wait for the system administrator/operator. The MCU must support ability to terminate two different non-routable networks, so that video calls from either network can be connected into a single conference without compromising on the security
	v) MCU shall provide a built- in web Interface, for configuration and administration.

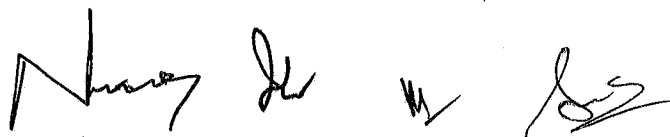
*M...*

*J...*

*W*

*[Signature]*  
Page 37 of 62

		vi) MCU shall support 2 access level/user privileges from administrator to simple guest.
		vii) MCU shall have a built- in/external address book and built in/ external scheduling.
		viii) The MCU shall support scheduled conferences and ad-hoc conferencing mode at the same time for all the 24 / N ports of the system.
		IX) MCU shall support a predefined and unique PIN for each conference.
		x) MCU shall allow users to create conferences on the fly from their end points without the need of Administrator /operator
		xi) The MCU shall support a mix of resolution in both voice activated mode and Continuous presence. Each end point shall receive at the maximum of its capacity without reducing the capacity of another.
		xii) MCU shall be capable of supporting H.323,SIP, and H.235 in the same conference. at any band with resolution.
	<b>(p) Other Features</b>	
	<b>(q) Centralized Recording</b>	Option-1: -The MCU server either internally or externally should be able to record' the ongoing conference on HD 720p / 1080P for 5 or more Simultaneously Conference. Option-2: -The MCU should support recording appliance based server in future which should be capable to record video conferencing sessions.
	<b>(r) Lync Connectivity (Optional for User Department)</b>	It should support Video Conferencing with Microsoft Lync. The Lync Client should be able to show the presence of Multiple Video Conference Endpoints/Lync Clients. Port Capacity 20 Lync Client simultaneously at VGA resolution.
	<b><u>Desktop-based Video Endpoint with Inbuilt MCU</u></b>	<b>Optional Item</b> <i>(To be selected by CAPFs as per their requirement)</i>
<b>8</b>	a)	The system should be an OEM integrated system with at least 24 inch and above LCD/TFT screen, 1920x1200 resolutions (16:9), integrated camera (1080p) and with inbuilt speakers for audio output.
	b)	The system should be full high definition (1920x1080P) from day one.
	c)	The Codec should be an inbuilt part of the offered system and should not be an external entity.
	d)	The system should, be capable to connect 1+3 multiparty from day one.
	e)	The camera should also function as a document camera for projecting hard objects and system should function as a PC monitor and should have 1080p resolution from day one.
	f)	The system should be operated using a Touch Screen Panel for call initiation, disconnection, data sharing etc.
	g)	The system should be accompanied with handset for private conversations.



**29. Enterprise Management System (EMS)**

S/N	Specifications	Compliance
	<b>General</b>	
1	The proposed NMS solution should be able to monitor 300 devices from day One and scalable to support monitoring of any size of IT infrastructure.	
2	The proposed helpdesk management system should be able to meet the requirement of vendor escalation (by sending automated mail to the concerned service provider) for entire ITBP infrastructure. This should allow any number of ITBP users to open tickets in the central helpdesk management system. This helpdesk management system must work as central and single point of contact for all IT service management requirement of ITBP.	
3	The proposed helpdesk management tool should be able to manage 04 seater helpdesk from day One and scalable to any number of helpdesks in future.	
4	System Performance Management System should monitor all the proposed servers under this project from day One and should be scalable to monitor any number of servers in future.	
5	All the proposed software modules should be from same OEM for seamless integration.	
	<b>Network Management System</b>	
1	<b>Network Management</b> – which will provide fault and performance management of the network infrastructure that various services operate in.	
2	Ø Proposed management system should be able to integrate well with other network element managers available in the system or should be able to discover all the devices from various vendors from the central place to ensure centralized view and management.	
3	Ø Proposed Solution should be recognized in the leader's quadrant by leading analyst including Gartner, IDC, and EMA Radar etc.	
4	<b>The proposed Network Fault Management System should provide the following features:</b>	
5	The Network Fault Management consoles must provide the topology map view from a single central console.	
6	The proposed Network Fault Management console must also provide network asset inventory reports and SLA reporting for the managed network infrastructure.	
7	The proposed solution must automatically discover manageable elements connected to the network and map the connectivity between them.	
8	The proposed system must have options for multiple types of discovery including the following:	
9	IP range discovery – including IPv6	
10	Import data - from pre-formatted files (IPs, ranges, strings or ports)	
11	Seed router based discovery – Using route tables and SNMP MIBs	
12	Trap-Based Discovery – whenever new devices are added with capability to exclude specific devices based on IP addresses / IP Address range	
13	The proposed fault management system must also utilize IPNet To Media (ARP) table during router discovery for quick subnet discovery.	
14	The proposed fault management system must have exclusion of specific IP addresses or IP address ranges from trap based discovery.	
15	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.	
16	The system must be able to have mapping and modelling of the infrastructure grouped by network connectivity, physical location of equipment and user groups or departments	

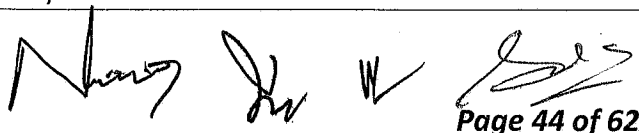
17	The modelling of network connectivity must be performed using standard or vendor-specific discovery protocols to ensure speed and accuracy of the network discovery	
18	The discovery should be able to identify and model router redundancy using vendor-specific protocols (like VRRP and HSRP support for Cisco devices) so that alarms generated from these virtual addresses are automatically excluded.	
19	The system should have mapping grouped by network topology, geographic locations of the equipment and user group/departments. These should help in understanding physical Network, virtual Network services and the relationships between them.	
20	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.	
21	The system must also have manual modelling adjustments to allow administrators to customize the structure, the layout and relationship between modelled elements.	
22	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.	
23	The system must provide user-configurable discovery control to manage the frequency and scope network discovery, configured using a graphical user interface	
24	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	
25	The proposed solution must have Network segmentation by supporting IPSEC / GRE Tunnels as well MPLS Layer 3 VPNs (e.g. VRF) & VLANS.	
26	The proposed solution must provide a firmware exception report that identifies devices within a group with a user-specified firmware level.	
27	The proposed solution must determine device availability based on whether the device was reachable via SNMP or ICMP. The proposed solution must also provide an outage editor that will be used to exclude outages from the availability calculation with an option to indicate the reason.	
28	The proposed solution should provide out of the box root cause analysis with multiple root cause algorithms inbuilt for root cause analysis.	
29	The system must use advanced root-cause analysis techniques and policy-based condition correlation technology for comprehensive analysis of network faults.	
30	It should have a strong event correlation engine which can correlate the events on the basis of event pairing, event sequencing etc.	
31	The system must be able to 'filter-out' symptom alarms and deduce the root cause of failure in the network automatically	
32	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.	
33	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.	
34	The proposed solution must detect virtual server and virtual machine configuration changes and automatically update topology	
35	The proposed system must support enhanced fault isolation to suppress alarms on logical VMs when physical servers fail	
36	The proposed solution must have the ability to collect data from the virtual systems without solely relying on SNMP	
37	The proposed solution must support a an architecture that can be extended to support multiple virtualization platforms and technologies	

38	The system should be able to clearly identify configuration changes as root cause of network problems	
39	The system should support secure device configuration capture and upload and thereby detect inconsistent "running" and "start-up" configurations and alert the administrators.	
40	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:	
41	Capture running configuration	
42	Capture start-up configuration	
43	Upload configuration	
44	Write start-up configuration	
45	Upload firmware	
46	The proposed fault management solution must able to perform "load & merge" configuration changes to multiple network devices	
47	The proposed fault management solution must able to perform real-time or scheduled capture of device configurations	
48	The proposed fault management solution must 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.	
49	The proposed fault management solution must also support a self-certification option to support device configuration load and capture thereby enabling users to "self-certify" devices not supported.	
50	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.	
51	The proposed fault management solution must also support a self-certification option to support device configuration load and capture thereby enabling users to "self-certify" devices not supported.	
52	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.	
53	The proposed solution should be able to support response time agents to perform network performance tests to help identify network performance bottlenecks.	
54	The proposed solution should be able to monitor QoS parameters configured to provide traffic classification and prioritization for reliable VoIP transport. The proposed solution should discover and model configured QoS classes, policies and behaviours.	
55	The proposed solution should provide the ability to discover, map & monitor multicast sources & participating routers wherein the system should be able visualize the distribution tree in the topology map.	
56	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.	
57	The proposed Service Dashboard should provide a high level view for executives and other users of the system	
58	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.	

59	<ul style="list-style-type: none"> <li>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. Presently, business services shall include E-mail, Internet Access, Intranet and other business services hosted.</li> </ul>	
60	<ul style="list-style-type: none"> <li>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.</li> </ul>	
61	<ul style="list-style-type: none"> <li>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.</li> </ul>	
62	<ul style="list-style-type: none"> <li>Root cause analysis of infrastructure alarms must be applied to the managed Business Services in determining service outages.</li> </ul>	
63	<ul style="list-style-type: none"> <li>SLA violation alarms must be generated to notify whenever an agreement is violated or is in danger of being violated.</li> </ul>	
64	<ul style="list-style-type: none"> <li>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.</li> </ul>	
65	<ul style="list-style-type: none"> <li>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.</li> </ul>	
66	<ul style="list-style-type: none"> <li>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.</li> </ul>	
67	<ul style="list-style-type: none"> <li>The system must provide a historical reporting facility that will allow for the generation of on-demand and scheduled reports of Business Service related metrics with capabilities for customization of the report presentation.</li> </ul>	
68	The proposed NMS should provide unified workflow between the fault and performance management systems including bi-directional and context-sensitive navigation, such as	
69	Navigate from the Topology View to At-a-Glance or Trend Reports for any asset	
70	Navigate from the Alarm View to At-a-Glance, Trend or Alarm Detail Reports	
71	The proposed fault management 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	
72	The system must support seamless bi-directional integration to helpdesk or trouble ticketing system	
73	The proposed network fault management system should integrate with the helpdesk system by updating the Asset with CI 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	
74	The proposed network fault management system should attach an asset identifier when submitting a helpdesk ticket. In case the asset is not found in the helpdesk database, it should be automatically created prior to submitting the ticket.	
75	<b>Performance Management</b> – Provide 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.	




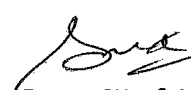
76	The proposed performance management system shall integrate network and server performance information and alarms in a single console and provide a unified reporting interface for network components. The current performance state of the entire network & system infrastructure shall be visible in an integrated console.	
77	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 centre.	
78	The performance management system is to provide all of the following capabilities for the ongoing performance monitoring, troubleshooting and reporting in the network and applications:	
79	The Network Performance Management consoles must provide a consistent report generation interface from a single central console.	
80	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.	
81	The proposed system shall collect, analyze and summarize management data from LAN/WAN, MIB-II interfaces and various servers for performance management.	
82	The proposed system shall identify over-and under-utilized links and assist in maximizing the utilization of current resources	
83	The proposed system shall provide Performance of Network devices like CPU, memory & buffers etc., LAN and WAN interfaces and network segments.	
84	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.	
85	The proposed system shall provide easy to read representations of health, utilization, latency and availability.	
86	It shall provide Real time network monitoring and Measurement off-end-to-end Network performance & availability to define service levels and further improve upon them.	
87	The proposed solution should provide the following performance reports out-of-the-box:	
88	<b>Executive Summary report</b> that gives an overall view of a group of elements, showing volume and other important metrics for the technology being viewed.	
89	<b>Capacity Planning report</b> which provides a view of under-and-over-utilized elements.	
90	<b>Service Level report</b> that shows the elements with the worst availability and worst response time-the two leading metrics used to monitor SLAs.	
91	The proposed system must have a Cognos-based report authoring tool built-in which will enable complete customization flexibility of performance reports for network devices and monitored servers.	
92	The tool should provide a live trend diagram that continuously charts critical statistical performance variables as they are collected and displaying the resource utilization levels of various critical devices and links in the managed infrastructure.	
93	The tool should provide a live exceptions list displaying the various health and threshold exceptions that are occurring in the managed infrastructure.	
94	The tool should provide an integrated 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	
95	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.	

96	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 quickly:	
97	<b>At-A-Glance Reports</b> to present a single page report on vital device statistics like for routers could display:	
98	Backplane Utilization	
99	Buffer Create Failures	
100	Buffer Hits	
101	Buffer Misses	
102	Buffer Utilization	
103	Bus Drops	
104	CPU Utilization	
105	Fan Status	
106	Free Memory	
107	Memory Utilization	
108	Packets Out	
109	Power Supply Status	
110	Temperature Status	
111	Total Bytes	
112	Total Discards In & Out	
113	Total Faults In & Out	
114	Total Packets	
115	Total Queue Drops & Discards In & Out.	
116	<b>Trend Reports</b> 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 or capacity and identify long drawn problems	
117	<b>Top N Reports</b> 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%)	
118	<b>Service Level Reports</b> to analyze & display service level information for an enterprise, region, department or business process for e.g. a typical business unit service level report for finance department should indicate evaluation of the performance of all the systems, routers, LAN/WAN segments, and applications within that department	
119	<b>Health Reports</b> 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 make sense.	
120	The system must provide capability to measure & generate detailed performance reports for the following common TCP/IP applications:	
121	DHCP: Measure the round trip latency required to obtain an IP address.	
122	DNS: Measure the DNS lookup time including Latency and Packet Loss	
123	FTP : Measure the time it takes to connect and transfer a file including Latency and Packet Loss	
124	ICMP Ping : Measure round trip source to destination including Latency and Packet Loss	
125	HTTP: Measure the time it takes to serve up a web page including the following parameters:	
126	Latency	


  
 Page 44 of 62



127	Http DNS resolution	
128	Http TCP Connection Time	
129	Http download time	
130	HTTPS: Using SSL, Measure the time it takes to serve up a web page	
131	Latency and Packet Loss for:	
132	POP3	
133	SMTP	
134	TCP	
135	UDP Echo Test	
136	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.	
137	The tool should provide Latency (both one way and round trip times) report for critical devices and links	
138	The proposed system should use intelligent alarm de-duplication algorithms to learn the behaviour of the network infrastructure components over a period of time.	
139	<b>Flow-based Traffic Analysis, Reporting and Capacity Planning System:</b>	
140	NMS solution should have a tightly integrated traffic analysis module supporting all the standard flow analysis technologies like IPFIX, NetFlow, Jflow, Sflow etc.	
141	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:	
142	Rate	
143	Utilization	
144	Byte Count	
145	Flow Count	
146	Router/interface with automatic SNMP name resolution	
147	Protocol breakdown by host, link.	
148	BGP next hop address	
	<b>Helpdesk Management-System</b>	
1	The proposed solution shall provide a web based service support system to automate incident, problem, change, knowledge management, interactive support, self-service and advanced root cause analysis	
2	The proposed solution should have achieved PinkVERIFY 3.1 certification on ITIL v3 processes (a documentary proof of the same should be provided at the time of bidding).	
3	The proposed solution should have achieved certification on Gold Level ITIL Process Compliance for Incident, Problem, Change, Request Fulfilment, and Service Asset and Configuration Management by the OGC ISS (a documentary proof of the same should be provided at the time of bidding).	
4	The proposed solution shall support request management, problem management, configuration management and change order management.	
5	The proposed solution shall provide end-users the flexibility of logging, viewing, updating and closing service requests and incidents using a web-based interface.	
6	The proposed solution shall provide administrators (service desk analysts) the ability to use a fully-functional web-interface and should provide power-user tips for frequently used functions.	
7	The proposed helpdesk solution must have the ability to track work history of calls to facilitate troubleshooting.	

8	The proposed solution shall provide an identity management system that allows user/role management and integration with authentication systems such as LDAP/AD.	
9	The proposed solution shall provide the facility to register incidents via e-mail.	
10	The proposed solution shall provide appropriate standards based integration mechanisms (such as CLI/Web-services) that allow infrastructure management solutions to automatically register incidents.	
11	The proposed solution shall provide classification to differentiate the incident via multiple levels/tiers of categorization, priority levels, severity levels and impact levels.	
12	The proposed solution shall provide the ability to associate each incident with multiple activity logs entries via manual update or automated updates from other security or infrastructure management tools.	
13	The proposed solution shall provide the flexibility of automated incident assignment based on metrics such as analyst workload, category and location.	
14	The proposed solution shall support definitions of escalation policies for multiple escalation levels and notification to different personnel via window GUI/console with no or minimum programming.	
15	The proposed solution shall provide the flexibility of associating the escalation policy with different criteria like device/asset/system, category of incident, priority level, organization and contact.	
16	The proposed solution shall provide a web-based knowledge base that assists in finding, organizing, and publishing knowledge articles that aid in self-service & faster turn-around time.	
17	The proposed solution shall allow analysts to create knowledge articles based on resolved incidents/problems and shall also allow end-users to submit knowledge for consideration (after appropriate approvals).	
18	The proposed solution shall provide a web-based report authoring solution that provides role-based access to existing report content, creation of new reports and ad-hoc/scheduled reporting.	
19	The proposed solution shall provide an out-of-box reporting dashboard that indicates analytics about daily service support operations.	
20	The proposed solution shall provide status of registered calls to end-users over email and through web.	
21	The proposed solution shall support tracking of SLA (service level agreements) for call requests within the service desk through service types (that define response/resolution time)	
22	The proposed solution shall provide a fully functional CMDB (Configuration Management Database) as an integral part of the service desk and should be accessible from the same interface.	
23	The proposed solution shall support automated application configuration discovery and dependency mapping for target CIs (eg. Servers) and enrich the CMDB with this information.	
24	The proposed solution shall allow the IT team & Change Advisory Board to visualize CI relationships with a specified number of relationships on single window.	
25	The proposed solution shall provide a Change Order Schedule calendar to track scheduled changes	
26	The proposed solution shall support version control for defined Configuration Items.	
27	The proposed solution shall provide multiple CI families, classes and relationships out-of-box to reduce implementation time.	
28	The proposed solution shall provide ready content for foundation processes, procedures and work instructions for Request, Incident, Knowledge, Problem, Change and Configuration Management.	

29	The proposed solution shall support multi-tenancy to enable different tenants (departments/customers) to use the same physical instance of the service desk.	
30	The proposed solution shall provide a non-linear workflow with decision based branching, and the ability to perform parallel processing. The workflow system must also have a graphical workflow designer with drag & drop feature for workflow creation and updates.	
31	The proposed solution shall provide a distributed and scalable architecture that caters to growth in number of analysts, end-users and call volumes.	
32	The proposed solution shall provide bi-directional integration with the proposed infrastructure management solution (e.g. An event/alarm in the infrastructure management solution shall automatically create an incident in the service desk and the incident number shall be displayed against the alarm in the event console. If the alarm is cleared, the incident shall be closed automatically)	
33	Reporting: Report module and SLA Management module must be integrated to provide ease-of-reports configuration and execution.	
	<b>System Performance Management System</b>	
1	The proposed system performance monitoring solution should integrate with the proposed network performance monitoring tool for central performance monitoring of network and systems.	
2	The proposed server performance management system shall integrate network performance management systems and provide the unified performance state view in a single console. The current performance state of the entire network and server infrastructure shall be visible in an integrated console. Topology of both physical as well as virtual types of servers should be visible and monitorable from NMS console.	
3	The proposed tool must provide lightweight server agents to ensure availability and performance for target server nodes both physical as well as virtual and deliver scalable, real-time management of critical systems.	
4	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.	
5	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.	
6	The proposed tool should integrate with network performance management system and support operating system monitoring for various platforms including Windows, UNIX and Linux.	
7	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.	
8	The proposed tool must provide provision for performance scoping and trending to provide real-time as well as historical reporting, where specified.	
9	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.	
10	The proposed solution should support management for parameters including Processors, File Systems, Log Files, System Processes, memory etc.	
11	The proposed solution should provide automated management to detect, isolate, and resolve problems autonomously	
12	The proposed solution should provide self-monitoring wherein it will track critical status for CPU utilization, Memory capacity and File system space and other important data.	

13	The proposed tool should provide Process and NT Service Monitoring wherein if critical application processes or services fail, administrators are immediately alerted and processes and services are automatically re-started	
14	The proposed solution should provide quick at-a-glance reports on systems and applications, disk and file system statistics, hardware/software inventories and more. The tool should be able to identify CPU hogs, and detect memory-leaking processes and I/O bottlenecks before they bring down the server.	
15	The proposed tool should be able to provide Log File Monitoring which enables administrator to watch system logs and text log files by specifying messages to watch for. When matching messages gets logged, the proposed tool should notify administrators and enable to take action like sending an email.	
	<b>Application Performance Management</b>	
1	End to end Management of all proposed applications (including J2EE/.NET based) with continuous deep dive diagnostics.	
2	Determination of the root cause of performance issues whether inside the Java application in connected back-end systems or at the network layer.	
3	Automatic discovery and monitoring of the web application environment	
4	Ability to monitor applications with a dashboard.	
5	Ability to expose performance of individual SQL statements within problem transactions	
6	Monitoring of third-party applications without any source code change requirements.	
7	Proactive monitoring of all end user transactions; detecting failed transactions; gathering evidence necessary for problem diagnose.	
8	Storage of historical data is for problem diagnosis, trend analysis etc.	
9	Monitoring of application performance based on transaction type	
10	Ability to identify the potential cause of memory leaks.	
	<b>Desktop Management System: (For 500 client nodes from day one and scalable to n number of users)</b>	
1	• The proposed desktop management system should provide single integrated agent for asset management, remote software delivery and remote desktop control.	
2	<b>Asset Management System:</b>	
3	• The proposed Asset Management solution must 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.	
4	• The proposed Asset Management solution must have reporting capabilities; provide predefined reports and the possibility to create customized reports on data in the inventory database. Report results could be displayed as lists or graphs.	
5	• The proposed Asset Management solution must have the capability to export the reports to CSV, HTML and XML format.	
6	• The proposed Asset Management solution must provide the facility for user defined templates to collect custom information from desktops.	
7	• The proposed Asset Management solution must provide facility to recognize custom applications on desktops.	
8	• The proposed Asset Management solution must support administrators to register a new application to the detectable application list using certain identification criteria's (Like executable, Date/time stamp etc.). The new application must be detected automatically from next time the inventory is scanned.	

9	<ul style="list-style-type: none"> <li>The proposed Asset Management solution must provide facility for queries and automated policies to be set up and permit scheduling of collecting engines to pick up the data at defined intervals.</li> </ul>	
10	<ul style="list-style-type: none"> <li>The proposed Asset Management solution must be able to collect WBEM information.</li> </ul>	
11	<ul style="list-style-type: none"> <li>The proposed Asset Management solution must integrate with the helpdesk solution and allow ticket creation automatically on an event defined in asset management solution. It should also allow manual ticket creation also.</li> </ul>	
12	<b>Remote Software Deployment System:</b>	
13	<ul style="list-style-type: none"> <li>It should provide delivery, installation, and un-installation of software (ex. Patches of Anti-virus solution etc.) installed on end-user desktops by software delivery remotely through agents installed on them. It must allow pre- and post-installation steps to be specified if required &amp; support rollback in the event of failure in installing software to end-user desktops.</li> </ul>	
14	<ul style="list-style-type: none"> <li>The tool should have the capability to install applications based on interdependencies i.e. to be installed in a particular order.</li> </ul>	
15	<ul style="list-style-type: none"> <li>It should support deployment of MSI based packages.</li> <li>It should perform actual distribution of software remotely, not mere file transfer and manual installation at other end. Automated installation should be possible.</li> </ul>	
16	<ul style="list-style-type: none"> <li>It should include a Software packager for creating software packages to be delivered to end-user desktops which uses a snap-shot technology.</li> </ul>	
17	<ul style="list-style-type: none"> <li>It should support both push and pull software distribution modes. A catalogue/advertisement option of the existing software delivery packages must be provided for end-user to download and install software of his / her choice.</li> </ul>	
18	<ul style="list-style-type: none"> <li>Users must be allowed to cancel jobs if they are launched at an inconvenient time. Cancelled jobs must be allowed to be reactivated. Forcing packages onto the computer must also be possible.</li> </ul>	

**Appendix-"V"**

**30. Technical Specifications for 65" LCD Screen as console for Network Operation Control**

S/N	Specifications	Compliance
1.	LCD Screen: 65-Inch	
2.	Screen Resolution: 1920 x 1080	
3.	Contrast Ratio of 5000:1;	
4.	Aspect Ratio 16:9;	
5.	Speakers : Built-in	
6.	HDMI Port	
7.	Should be supplied with all accessories to integrate with NMS Server over Intranet for monitoring	

**Appendix-"W"**

**31. Technical Specification for Network Terminal**

S/N	Specifications	Compliance
1	Operating system Preinstalled: with media Genuine Windows Professional	
2	Genuine Windows-7 Professional with Media	
3	Processor 2 Intel® Core TM2 Duo Ultra Low Voltage (upto 1.2-GHz, 2-MB L2 cache)	
4	Chipset Mobile Intel GM 965	

5	Memory 2 GB total	
6	Hard Drive(s)at least 80GB	
7	DVD R–BUILTINOR EXTERNAL	
8	Display at least 10-inch diagonal or less Illumi-Lite,15WXGAUWVAwithDigitizer(1280×800),10-inch diagonal Illumi-Lite, WXGA UWVA with	
9	Graphics 8MobileIntelGMAX3100,upto384 MB of shared system memory	
10	Audio High Definition Audio, stereo speakers, stereo head phone/lineout, stereo microphone in, integrated dual-microphone array	
11	Expansion slots Express Card /54 slot or integrated Smart Card Reader, Secure Digital slot	
12	Ports and connectors 2 USB 2.0 ports, VGA, stereo microphone in, stereo headphone/lineout,1394a,power connector,RJ-11/modem, RJ-45/Ethernet, docking connector Ultra-Slim Expansion Base, secondary ultra-slim battery connector	
13	Input device Full-sized keyboard	
14	Manageability Intel® Centrino®Pro Processor Technology capable, Backup and Recovery Manager, Client Manager Software,	
15	Security Protect Tools, TPM Embedded Security Chip, Finger print Sensor	
16	Omnipass Software compatible	
17	Card Reader	
18	Power6-cell(44WHr)Lithium-Ionbattery,OneadditionalUltra-SlimBattery,65W AC Adapter	
19	Antivirus for one year	

**Appendix- "X"**

**32. Technical Specificationsfor 42U Rack and 15 U Rack**

**A. 42U (800 mmW x 1000 mm D) Floor Standing Server/Network Rack**

S/N	Features	Specifications
1.	Make and Model	
2.	Dimension Load bearing Capacity Depth of Rack Locking arrangement  Side Panels  Minimum Accessories:	19" rack Height 42U, Width 800mm, Depth 1000mm 500 Kg or more Approx  1000 mmD  Lockable Front Glass Door Lockable Rear MS Door (Perforated) Two Nos of Side Panels on Slam Latches - detachable  Racks to be fitted with adequate Fans
3.	(4 Nos of Fans be mounted on the Top for proper Cooling. Racks to be on Castors set of 4 with Front Brakes. Racks should have adequate Equipment Trays. It is suggested that minimum 2 Trays should be there. Racks can have one Key Board Tray. It should have adequate Hardware for installation of 19" mountable equipment in the Rack (it is suggested that at least one Hardware P/20 should be there) Earthing Kit- 1 No. Proper PDUs with Universal Sockets as per the features attached herewith.	

*(Handwritten signatures)*

4.	ACDB with 5/15amps as per the requirement with imported sockets
5.	KVM 16 Port USB (IP Based with managing Software) Rack mountable (1U) 16 Port KVM Switch with OSD, Cables and Accessories 16 Port USB KVM Switch which should be 19" Mountable 1 U Height will all the 16 Nos of KVM Cables to PC Cables (3 in 1) KVM Cables so that there is no confusion with regard to Quantity and Prices of the Cables: - (a) Keyboard/Video/Mouse (b) 1 No. Power Cable/Adaptor, 19" mountable Kit and (c) 1 No. of Daisy Chain Cable working up to 5mtrs from KVM console port to Server PC. The cable Combination for proper Rack mounting and management should be as under:- Total 16 Cables:- 12 Nos of 1.8 Mtr Cables and 4 Nos of 3 Mtrs Cables Should work with not only standard 3-key MS mouse, but also over 3 keys MS mouse or other fully MS compatible mouse
6.	17" LCD (a) 19" Rack mountable (1U) Keyboard, Mouse with 17" LCD Monitor and the Monitor should be 17".

### B. 15U Wall Mountable Rack

15U wall mount rack with front glass door with lock.

Rack accessories:

fans, 19" stationary shelf (1 no.), 5 point AC distribution box 5/15 Amps(1 no.), mounting  
hardware-pack of 10(3 nos.)

Should be supplied with Cable Manager and other necessary accessories.

### Appendix-"Y"

### **33. Technical Specifications for Database Encryption Hardware**

Feature	Specifications	Compliance
Performance	Should process more than 10000 encryptions per second	
	Should be scalable to hundreds of thousands of encryptions per second via clustering of multiples appliances	
Security Algorithms	3DES, Des, AES, RSA (signatures and encryption), RC4 SHA-1, HMACSHA-1	
Asymmetric Key sizes	512, 1024, 2048	
Symmetric key sizes	128, 168, 192, 256	
System Administration	Secure Web-based GUI, secure shell (SSH), and console	
Supported Databases	IBM DB2, Microsoft SQL Server, Oracle, and Teradata	
Form Factor	Form Factor: 1U, rack	
Network Management	SNMP (v1, v2, and v3), NTP, URL health check, signed secure logs, syslog, automatic log rotation, secure encrypted and integrity checked backups and upgrades, extensive statistic	
General	The solution should be supplied as completed system including Hardware, Software and connectors /licenses, if any involved.	

**34. Technical Specifications for Cables/Accessories for DC & DR**

S/N	Specifications	Compliance
1	The intelligent cabling solution offered must meet the following requirements:	
2	The intelligent solution should provide higher security to switch ports by avoiding changes directly on the switch ports and better patch cord maintenance. Changes in the patching are to be done in the Intelligent panel itself and no patching changes are to be carried out at the switch ports, cross connect configuration is mandatory.	
3	The intelligent solution should provide an option to minimize use of patch cords in the patching area i.e. on the intelligent patch panels.	
4	The Physical Layer Management solution should be strictly based on the PHYSICAL detection of patch cord connectivity ONLY.	
5	The system should be straight forward and report patching ONLY when the two ends of the same patch cords are inserted into the ports of the intelligent panels, without any specific configuration mode.	
6	The solution should provide the technician an easy method of patching with- out imposing any specific sequence rules/order for the patching, thus allowing the technician to carry patching work orders as in the case of a non-intelligent solution.	
7	The Intelligent Physical Layer Management Solution should have a LED guidance at panel port level. The solution should be such that to make a change in a rack the technician need not to visit other racks or displays for any information. The guidance should help in tracing the two ends of any patch cord, executing planned work orders and for remote management at each port level of the Jack Panel.	
8	The intelligent panels should have the necessary intelligent hardware. Retrofits are not an option. Also the panels should not require power supply directly thus making them active. The LEDs should get power from scanning devices only.	
9	The Intelligent Physical Layer Management solution should be scalable and the design should enable maximum usage of its components e.g. scanning devices, by sharing of same components over multiple racks when required.	
10	The solution should be simple, effective and as automated as possible requiring minimum human intervention. For e.g. for executing work orders the solution should depend on LED guidance only without need for reading instructions from any media/display at different rack.	
11	The solution should provide patching information based only on physical connectivity information and not thorough any other way.	
12	The solution should be web based and not require any clients to be installed on end devices. All features should be available through this web explorer only.	
13	All scanning devices monitoring the intelligent panels should be 1U only to allow maximum usage of rack space. Also they should have the capability to be shared among more racks.	
14	The scanning devices should automatically detect the panel type; the scanning devices are connected to, and should also automatically detect the connectivity between the scanning devices. This is necessary for automatic & error free real time detection & installation of hardware components in the software.	
15	The solution should offer flexibility to extend the panel scanning capability to distances more than 7 feet (one rack) in order to cover more than a single rack.	



16	Since all the upper & centre units of the rack (critical real estate space in rack) will be required to mount panels or switches to provide a hassle free environment for their control and installation, the scanning devices would be mounted either at the top or bottom of the rack. Hence it is important that the scanning devices should carry a design such that they require minimum interaction during any work order execution and do not force any change in the rack design to enable their functioning.	
17	The solution should be simple and efficient and should not require use of multiple media for providing or verifying of the same information or carrying out a work order.	
18	The solution should provide an option to technician to interact directly with the database information (e.g. for online view of the complete connectivity information) through additional devices e.g. handheld, without having any impact on the critical real estate space utilization or design of the rack proposed.	
19	The solution should provide an easy way for tracing panel port connectivity information even at the rack level without directly interacting with any panel port / software. This is important to provide information during network outage.	
20	The implementation of the intelligent solution should not hamper or should not be hampered by the progress in the other cabling, patching & active installation. The solution should be capable to be installed at any time during the network installation and testing.	
	The Intelligent Physical Layer Management Solution should have the capability to detect automatically and without any human intervention all patch cord connectivity information even in following cases:	
i	If the site is already patched and both the scanning devices & software is installed at a later stage.	
ii	If one or all scanning devices are not working and new patching needs to be done once the scanning devices are functional again.	
iii	If one of the patch cords is cut.	
21	It should have the ability to manage active (door locks, fans, etc.) and passive devices, like sensors, (doors, heat, dust, A/C).	
	<b>NMS Software For Cabling System</b>	
1	The Intelligent Physical Layer Management software should provide the following capabilities:	
2	Automatic Detection of IP Assets and Assignment – The software should automatically discover all IP devices in the network including; PCs, IP phones, printers, switches and other IP equipment and assign their locations, down to the exact room and cubicle, in real time.	
3	Device information - The software should provide information about the MAC id, IP and Host Name of the IP devices connected to the network.	
	Automatic tracing – the solution should not only detect but should also track the devices when they move from one location to another in real time.	
	Complete link information - The solution should automatically provide complete linkage information (from switch port up to the end device) in graphical format, providing full end-to-end visibility and automatic updates of new locations when moves occur.	
	Alerts on Connectivity changes – The solution should report any changes on patching information in real time through physical verification only and not through any other method.	
	Real time view of Communication Racks – The solution should provide information of the rack layout in graphical view and allow interaction with displayed information in real time (e.g. lighting an LED over an panel port remotely). This is extremely important for remote site management.	

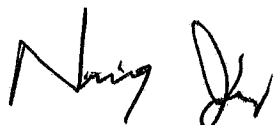


*Manoj J*

*M* *J*  
Page 53 of 62

	LED guidance based Scheduled Work Orders – The solution should have the capability to create and assign work orders to technicians. It should -	
1	Ensure the ability to create, assign and monitor the status of any work order to any technician.	
2	Warn of a mismatch between requested activity and real status through ongoing scanning activity and LED guidance.	
3	Automatically update the database upon completion of task.	
	Utilization Module – The solution should be capable to collect information of the activity at each switch port & identify unused switch ports. This is necessary to optimize the usage of switch ports	
	.Graphical Layout View - The solution should have the capability to import floor layout plans in dwg CAD, jpeg, bmp formats to show the geographical locations of each asset in the entire network down to each room, hall, cubicle and desk in the enterprise.	
	Enhanced Security – Should be able to identify between unauthorized and authorized changes on the network connectivity and send alerts accordingly.	
	Alerts – The solution should have in place the option to send alerts either through email, sms, pop-up messages at client end and pop-up messages to Dashboard.	
	Customized Reports – The solution should provide complete Fault Summary with customizable log files to generate reports for various requirement of the user. For e.g. the solution should -	
a	Provide printed reports and information	
b	Allow users to query selected data	
c	Display information in a tabular or graphic format	
d	Option to export information to external files and systems	
	Power down time - In case any changes are made to the network (patching) during a planned (power) down time, the solution should be able to register and report the changes if any during the power down time, once the system is up again, without any human intervention.	
	Integration to 3rd party software - The solution should provide a comprehensive open-ended solution e.g. an SDK (software development Kit) and not just the capability to send SNMP traps to integrate the solution with any 3rd party software or in-house software.	
	Database - The database should be using an open database to enable easy integration.	
	Intrusion detection - The solution should offer as a built in feature the possibility to report any unauthorized MAC outside the white list of MACs allowed on the site.	
	Switch blocking: The solution should be capable to block switch ports automatically on intrusion detection. This capability however should be selectable by the user depending on the critical nature of the location.	
	Device detection - The solution should allow automatic discovery of devices through a schedule as well as through SNMP port trap triggers.	
	Wireless devices - The solution should be capable to detect Wire Access Points (WAP). In the case where the WAP shows the information of the devices connected to it, the solution should provide information of the devices connected to the WAP also.	
	Real time power information - The solution should be ready to integrate to IP based power strips to get information of the power being consumed in the racks in real time and use this information for provisioning of servers inside any communication room.	

Handwritten signatures and initials, including a large signature on the left and several smaller initials or signatures to the right.

	Network provisioning – The solution should provide the capability to automatically check the possible movement of any device to a new location by verifying the network availability with any proposed setting, providing the patching information with options and creating a work order for the same. All this is to be achieved by a mere drag and drop operation.	
	Power and space provisioning – Based on the information of network provisioning, space available in the racks and the real time power being consumed, the solution should be able to automatically provision any new device in a datacentre and provide the required work order. All this is to be achieved by a mere drag and drop operation.	
	Multiple provisioning option– The solution should be capable to handle multiple provisioning operations to reduce the time of such operations drastically.	
	Secure / Critical Links - The software should provide capability to mark all the critical links as special and should be able to generate alerts or test the network connectivity status directly of such devices. Any changes on such links should be shown with special colours to immediately identify the changes made.	
	User Licenses - The solution should be provide with an unlimited user licenses. This is important to enable use by multiple users.	
	<b>Following tools may be required –</b>	
1	The solution should provide a Dash Board to get information from the database and represent it for use in various formats. This is important so that all information from the database can be viewed without the need to interact directly with the total solution. This tool is essential for reporting all activities to higher management.	
2	If required the solution should be ready to support use of system by multiple technician working in the same communication room / rack.	
3	The solution should provide a special tool to easily identify the racks in which the two ends of the patch cord are connected in case the two ends are in two different racks, again without the need of any special query to database or reading from any special device.	
	<b>Specification Intelligent UTP Patch Panels:</b>	
1	Compatible to Unshielded Twisted Pairs (UTP) cabling systems	
2	High performance panels that support Category 6A performance specifications up to 500 MHz	
3	Conform to ANSI/TIA/EIA-568-C.2, ISO/IEC 11801 2nd edition and CENELEC EN50173 for	
4	Category 6A/Class EA	
5	Special cap design for minimizing Alien Cross-Talk	
6	Simple labour-saving termination using standard 110 & Krone termination tools	
7	Backward compatible with Category 5e and Category 6 cabling standards	
8	Supports 48 ports, using 2U of rack space	
9	Compatible with 22-26 AWG Solid or stranded wire cables	
10	24 port 1U or 48 port 2U	
11	Option for reduced patch cord capability.	
12	High durability and reliability	
	<b>Environment</b>	
1	Temperature:-20° to 60°C	
2	Humidity: 0-90% non-condensing	
3	Compliance with International EMC Standards:	
4	The 48 line of patch panels is designed to comply with EN-55022, Class B (Europe) and FCC Part 15, Subpart J, Class A (USA)	

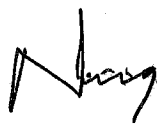



<b>Non – SMNP Scanning Devices:</b>	
1	Should be 1U device
2	Standards Safety UL 60950, EN 60950 -compliance EMC EN-55022, FCC Part 15 Class A, EN-55024
3	UP LINK - Standard RS-485, Full — Duplex, Connector Shielded RJ-45 socket, Data Rate Up to 115.2 Kbps
4	Interface Serial - Standard RS-232, Connector 9-pin D-type male, Data Rate Up to 115.2 Kbps, Protocol UART, Start bit 1, Stop bit 1, Non parity
5	Patch Panel Connections - Connectors 6 or 12 headers, 26-pin, 100mil spacing
6	Temperature 0 - 500C /32-1220
7	Humidity Up to 90% non-condensing
<b>SMNP scanning devices:</b>	
1	This scanning device includes an SNMP agent that allows the management software to receive all relevant data.
2	Should collect, save, and transmit connectivity data from the other non-smnp Scanners via and updates management software.
3	Should monitor up to four communication rooms.
4	The maximum length of a copper cable connecting the SNMP scanner to the other scanners
5	Should be 1,200m/4,000ft.
6	Each one of these DOWN LINK port on the SMNP scanning device represents a site.
7	Standards Safety - UL 60950, EN 60950, compliance EMC EN-55022, FCC Part 15 Class A, EN-55024
8	DOWN LINK 1 – 4 Ports, Standard RS-485, Full – Duplex, Connector Shielded RJ-45 socket, Data Rate Up to 115.2 Kbps
9	SERIAL Standard RS-232 Connector 9 pin D-type male, Data Rate Up to 115.2 Kbps, Protocol UART, Start bit 1, Stop bit 1, Non-parity,
10	100Base Tx RJ-45 socket, Ethernet IEEE 802.3,
11	100Base Tx/10Base T, 100/10 Mbps industry
12	standard for connection to local area network
13	1 U device
<b>Hand held controller device:</b>	
1	The controller device is connected to the Scanning device.
2	Using this the technician is guided through the process of connecting and disconnecting the cords to complete the links defined in the system.
3	By activating one of the three functions of the controller device, the technician is guided through different processes by the LEDs on the ports of the panels. The LED will either stay lit or blink depending on the activity being performed or required.
4	The controller device can be connected to any Scanning device within the Site / Patching Area.
5	Three options, Enabled, Disabled and Bypass are available for the controller. These options are selected in the Management Software application.
<b>Cords connect scanning devices to panels:</b>	
1	Should be flat bus cable type of scanner cords
2	Should be connected on one side to Panels and on the other side to scanning devices
3	Should be available in different lengths like 1m, 3m, 5m
4	Should be flat or round type

<b>1. CABLING FOR DATA SYSTEM</b>	
<b>1.1 SCOPE</b>	
This document defines the cabling system and subsystem components to include cable, termination hardware, supporting hardware, and miscellany required to furnish, and to install a complete cabling infrastructure supporting data and video. The intent of this section is to provide pertinent information to allow the vendor to bid the labour, supervision, tooling, materials, and miscellaneous mounting hardware and consumables to install a complete system. However, it is the responsibility of the vendor to propose any, and, all items required for a complete system whether or not it is identified in the specification, drawings and bill of materials attached to this specification. All the items must be used from an ISO 9001 and ISO 14001 certified manufacturer. The compliance statement for all the technical specification listed herewith must be provided on the OEM's letter head.	
<b>APPLICABLE DOCUMENTS:</b>	
The cabling system described in this specification is derived in part from the recommendations made in industry standard documents. The list of documents below (or the latest revisions) has bearing on the desired cabling infrastructure are incorporated into this specification by reference:	
1	This Technical Specification and Associated Drawings
2	ANSI/TIA/EIA 568-B Commercial Building Telecommunications Cabling Standard – March 2001
3	ANSI/EIA/TIA-569-A Commercial Building Standard for Telecommunications Pathways and Spaces - February, 1998
4	ANSI/EIA/TIA-606 Administration Standard for the Telecommunications Infrastructure of Commercial Buildings - February, 1993
5	ANSI/TIA/EIA-607 Commercial Building Grounding and Bonding Requirements for Telecommunications - August, 1994
6	ANSI/TIA-568-B.2-10 for Category 6A channel
<b>1.2 Cabling System and Component Specifications Solid Cable Cat 6A (10G) 4 pair UTP</b>	
1.2.	UTP Cabling System
1	
1.2.	Unshielded twisted pair cabling system, TIA / EIA 568-B.2-10 addendum Category 6A
1.1	Cabling system
	Networks Supported
	Support for Fast Ethernet and Gigabit Ethernet,10G, IEEE 802.3/5/12,Voice,ISDN, ATM 52 & 622 Mbps, Broadband, TP=PMD and ITU V.21 and X.11
	Warranty
	25-year Performance warranty; Warranty to cover Bandwidth of the specified and installed cabling system.
	Performance characteristics to be provided along with bid
	Attenuation, Pair-to-pair and PS NEXT, ELFEXT and PSELFEXT, Return Loss, ACR and PS ACR for 4connector channel
	Site Certification
	Site certification to be done by OEM certified installer for 25 years and certificate to be issued from OEM.
1.2.1	<b>Unshielded Twisted Pair, Category 6A, TIA / EIA 568-B.2-10 Solid Cable Cat 6A (10G) 4 pair UTP</b>
1	23 AWG Annealed bare solid copper, CAT-6A UTP Cable, Channel optimized to 800 Mhz
2	Meets EIA/TIA 568-C.2 Category 6A specifications, Use CM,CMR UL-Rated Plastic
3	Worst Case Cable Skew : 25 nsec/100 meters
4	Characteristic Impedence : 100±6 Ω@ 1-600 Mhz
5	Conductor Diameter 0.65 mm (nominal)
6	Insulation High Density polyethylene
7	Support for Fast Ethernet and Gigabit Ethernet,10G, IEEE 802.3/5/12,Voice,ISDN, ATM 52 & 622 Mbps, Broadband, TP=PMD and ITU V.21 and X.11
8	DC Resistance Max: 75 Ohms/1000m




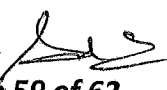




9	Sold Cable should be compliance to RoHS.	
10	Sheath Fire retardant PVC Compound (FRPVC) Flame Rating : 60 deg. C As per UL 1685 CM	
11	PAIRS Colour code: Blue / White-Blue, Orange / White-Orange Green / White-Green, Brown / White - Brown	
12	Outer Sheath PVC compound Thickness Diameter 1.45 mm (nominal) Outer diameter 9 mm (nominal)	
13	ELECTRICAL CHARACTERISTICS at 20° C Input Impedance (0.772-100 MHz) : 100 + 15 Ohms 125-250 MHz) : 100 +/- 22 Ohms	
14	Mutual Capacitance : 45pF/mtr	
15	Standard length: 305 Mtrs (1000 ft.)	
1.2.2	<b>UTP Jacks Type Unshielded Twisted Pair, Category 6A, TIA / EIA 568-B.2-10</b>	
1	Made from high impact, flame-retardant, UL- RATED 94v 0 thermoplastic ,ABS	
2	DC Resistance: 69 milli ohms.	
3	DC Resistance imbalance : 20 milli ohms.	
4	Insulating resistance 500 Mega ohms minimum.	
5	Current Rating : 1.5 A (max)	
6	Collapsible Angular Shuttered type jacks	
7	Support for Fast Ethernet and Gigabit Ethernet, IEEE 802.3/5/12, Voice, ISDN, 10G, ATM 155 & 622 Mbps, Broadband	
8	Spring Contact : 50u" gold over 100u" nickel	
9	Meets and exceeds ISO/IEC 11801:2002 Category 6 ,EIA/TIA 568-C.2 Category 6A component specifications	
10	The performance exceeds EIA/TIA 568-C.2 Category 6A component specifications	
11	The outlet is of IDC (insulation Displacement Contact) 180 deg punch type Cabling Consultant 9	
12	UL Listed to "ANSI/TIA/ EIA-568-B-2.10" specifications	
13	ROHS compliant	
1.2.3	<b>UTP Jack Panels Type 24 port, Unshielded Twisted Pair, Category 6A, TIA / EIA 568-C.2</b>	
1	Modular, PCB based and Keystone type Unshielded Twisted pair, category 6A, EIA/TIA 568-B.2-10	
2	The keystone modules are fire-retardant, moulded plastic modules UL94 VO rated, consisting of horizontal index strips for ease of re-termination.	
3	110 IDC Termination 180 degree Punch, allowing wires between 22 – 26 AWG sizes.	
4	Meets or Exceeds EIA/TIA – 568 – B.2-10 Category 6A connecting hardware specification.	
5	RJ45 (8P8C) T568A/T568B colour coding termination.	
6	Cable Guide way to guide the cable on the rear side	
7	1U size for 6/12/24 Ports and 2U for 48 Ports.	
8	UL Listed to "ANSI/TIA/ EIA-568-B-2.10" specifications	
9	Jack Panel should be RoHS Compliant.	
1.2.4	<b>Faceplates</b>	
1	Type	1Port, White surface box
2	Material	ABS / UL 94 V.0
3	No. of ports	One / two
4		High Impact Plastic Body ABS FR Grade 86 x 86 mm
5		Flush mountable or surface mountable with a back mount frame

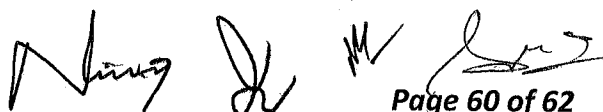
<b>1.2.5</b>	<b>Workstation / Equipment Cords Type Unshielded Twisted Pair, Category 6A, TIA / EIA 568-C.2</b>	
1	Patch cords shall be of multi strand copper cable	
2	With Matching coloured snag-less, elastomer polyolefin boot	
3	Terminals with gold contacts, 50 micron" gold over nickel	
4	Patch cord has a characteristic impedance of 100 +/- 3 Ohms	
5	Patch cord has extra long boot to maintain the bend radius.	
6	Assembled with short body RJ45 50u gold plate to minimized untwist pair length. ·	
7	Designed for high speed transmission ·	
8	Improved PS -NEXT, ELFEXT and Return Loss performance. ·	
9	Backward compatibility with all current Cat.5 products and applications. Cabling Consultant 10	
10	Material : ROHS compliant	
<b>1.4</b>	<b>Specification for Fibre</b>	
<b>1.4.1</b>	<b>Multimode Fibre optic Cable</b>	
1	Cable Type	6/12-core, Multimode, 10G Ethernet OM3, Unarmored, loose-tube, Gel Filled
2	Fibre type	50 / 125, Laser Grade, 250 micron primary coated buffers
3	No. of Core per Tube	4
4	No of Tube	6
5	No. of cores	24
6	Cable Construction	BELLCORE GR 20 / IEC 794-1
7	Attenuation	
8	@850nm	3.0 dB / KM
9	@1300nm	1.0 dB / KM
10	Bandwidth	
11	@850nm	1500 MHz-KM
12	@1300nm	500 MHz-KM
13	Network Support	
14	10 / 100 Ethernet	2000m
15	155 Mbps ATM	2000m
16	1000 Base SX	900m
17	1000 Base Lx	550m without Mode Conditioning launch patch cord.
18	Tensile rating	2670N
19	Maximum Crush resistance	4400N
20	Operating Temperature	-40 Degree C to +70 Degree C
21	Attenuation	
22	Wavelength (nm)	
23	Maximum Value (db/km)	
24	850	<=2.3
25	1300	<=0.6
26	Colour	Black
27	Inner jacket	High density polyethylene
28	Outer jacket	Halogen free fire retardant (HFFR) polyolefin.

29	Secondary Buffer Material	Gel filled Loose Tube.	
30	Min Bend	20 X Outer Diameter. Fibre Core macro-bending performance should be below 10 mm radius.	
31	Test (Must pass)	IEC794-1-E1 , IEC794-1-E2 , IEC794-1-E3 , IEC794-1-E4 , EIA-455-104 , IEC794-1-E7 , IEC794-1-E10 , IEC794-1-F1 , IEC794-1-F3 and IEC794-1-F5	
32	Marking	Identification marking at regular intervals of 1 meter	
33	Fiber Core	Raw fibre of corning. CORNING marking should be visible on the OFC	
34	Length of cable drum	standard factory length and can be supplied is max 4 Kms	
<b>1.4.</b>	<b>Fiber Optic Patch panels</b>		
<b>4</b>			
1	Fibre optic patch panel	19 inch, Rack mounted Fibre optic patch panel	
2	Height	1 U, 1.75 inches	
3	No. of fibres	6,12,24	
4	Dimensions	44 * 410 * 280 mm (H*W*D)	
5	Material	Complete Aluminium Alloy housing, fully powder coated	
6	Splice tray and cable spools to be included	Fully cushioned splice holder containing grooves for fixing splice protective sleeves	

#### Technical Specifications for Cables & Accessories at Remote Locations

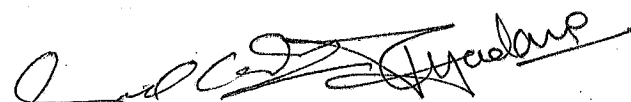
<b>A</b>	<b>UTP Copper Cables CAT 6 LSZH</b>		
1	23 AWG Annealed bare solid copper, CAT-6 UTP Cable, Channel optimized to 600 Mhz		
2	4 pair Cat 6 Low Smoke Zero Halogen ,UTP Cable is manufactured in accordance with the latest TIA/EIA 568-B.2-1 standards and exceeds the category 6 specifications		
3	Current Rating		
4	Characteristic Impedance		1.5 Amps
5	DC Resistance		100 ± 15 Ω
6	Contact Resistance		12 Ω / 100m
7	Propagation Delay		20 m Ω Max
8	Dielectric Strength		445 nS
9	Insulation Resistance		1000V AC
10	Pulling Strength		>500 M.
11	Operating Temperature		25 lds Max
12	Mutual Capacitance		- 20°C to +60 °C
13	Electrical Performance		5.6 nF Max / 100m
14	Sheath Material		As per EIA/TIA 568-B.2-1
15	Support for Fast Ethernet and Gigabit Ethernet IEEE 802.3/5/12, Voice, ISDN, ATM 155 & 622 Mbps and Broadband	UL 1685 – CM Rated – Fire redundant PVC UL 1666 – CMR rated UL 910 –CMP rated IEC 60332-3 - LSZH	



  
 Page 60 of 62





16	Cat 6 LSZH Cable must be UL Listed and Third Party verified by ETL to "ANSI/TIA/ EIA-568-B-2.1" specifications	
17	Cat 6 LSZH Cable must be RoHS Compliance.	
18	Zero Bit Error verified by ETL.	
19	PAIRS Colour code: Blue / White-Blue, Orange / White-Orange Green / White-Green, Brown / White - Brown	
20	Standard length: 305 Mtrs (1000 ft.)	
<b>B.i</b>	<b>Face Plate</b>	
1	Angular Bezel Module Face Plate	
2	With clear label(Identification)	
3	Made from high-impact, flame-retardant, UL- RATED 94v 0 thermoplastic - ABS	
<b>B.ii</b>	<b>Information Outlets (Jacks)</b>	
1	<b>Type</b>	<b>Unshielded Twisted Pair, Category 6, TIA / EIA 568-B.2</b>
2	Durability	
3	Modular Jack	750 mating cycles
4	Wire terminal	200 termination cycles
5	Accessories	Strain relief and bend-limiting boot for cable Integrated hinged dust cover using collapsible angular shuttered technology.
6	Approval	UL
7	Housing	Polyphenylene oxide, 94V-0 rated
8	Wiring blocks	Polycarbonate, 94V-0 rated
9	Jack contacts	Phosphorous bronze, plated with 1.27micro-meter thick gold
10	Approvals	UL , ETL and 3P
11	Performance Characteristics to be provided with bid	Attenuation, NEXT, PS NEXT, FEXT and Return Loss
12	Material	Spring Contact: 50m" goldover 100m" nickel
13	RoHS Compliance	ROHS compliant
<b>C</b>	<b>UTP Patch Cord</b>	
1	Conductor	24-26 AWG Multi stranded copper.
2	With Matching coloured snag-less, elastomer polyolefin boot	
3	Terminals with gold contacts, 50 micron" gold over nickel	
4	Patch cord has a characteristic impedance of 100 +/- 3 Ohms	
5	Patch cord has extra long boot to maintain the bend radius.	
6	Assembled with short body RJ45 50u gold plate to minimized untwist pair length.	
7	Designed for high speed transmission .	
8	Improved PS -NEXT, ELFEXT and Return Loss performance. .	
9	Back-ward-compatibility with all current Cat.5 products and applications.	
10	UL Listed and Third Party verified by ETL to "ANSI/TIA/ EIA-568-B-2.1" specifications	
11	Material	ROHS compliant

D	UTP Patch Panel	
1	Type	<b>24-port, Unshielded Twisted Pair, Category 6, TIA / EIA 568-B.2</b>
2	Ports	24
3	Port arrangement	Keystone type. Ports must be individually replaceable.
4	Category	Category 6
5	Circuit Identification Scheme	Icons on each of 24-ports
6	Port Identification	9mm or 12mm Labels on each of 24-ports (to be included in supply)
7	Height	1 U (1.75 inches)
8	Durability	
9	Modular Jack	750 mating cycles
10	Wire terminal (110 block)	200 termination cycles
11	Accessories	Strain relief and bend limiting boot for cable
12	Materials	ROHS compliant
13	Housing	Polyphenylene oxide, 94V-0 rated
14	Wiring blocks	Polycarbonate, 94V-0 rated, Spring Contact: Phosphor bronze 50m" gold
15	Jack contacts	Phosphorous bronze
16	Panel	Black, powder coated steel
17	Approvals	UL , ETL and 3P
18	Termination Pattern	TIA / EIA 568 A and B;
19	Performance Characteristics to be provided along with bid	Attenuation, NEXT, PS NEXT, FEXT and Return Loss


  
**(Subhash Chandra)**  
 Asstt. Dir., SSB


  
**(Pawan Kumar)**  
 Dy Comdt., BSF

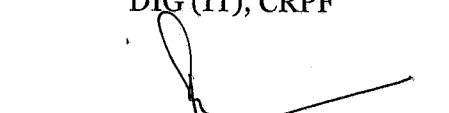
  
**(Ravindra Kumar)**  
 SC (Eqpt), NSG

  
**(Lt. Col. Vikas Prabhakar)**  
 Assam Rifle

  
**(Nishith Chandra)**  
 Comdt (IT), ITBPF

  
**(S. M. Hasnain)**  
 DIG (IT), CRPF

  
**(Virendra Agrawal)**  
 DIG (Eqpt), CRPF

  
**(R. K. Vishwakarma)**  
 Inspector General (Comn), CRPF

Approved / Not Approved

  
**(K. Vijay Kumar)**  
 Director General, CRPF