



**Request for Proposal (RFP) for Network Management support
services for Wide Area Network of the Bank**

Union Bank of India, Department of Information Technology
1/1A, Technology Center, Adi Shankaracharya Marg,
Opp. Powai Lake, Powai, Andheri East, Mumbai - 400072

DISCLAIMER

The information contained in this Request for Proposal (RFP) is provided to the Bidder(s) on the terms and conditions set out in this RFP document. The RFP document contains statements derived from information that is believed to be true and reliable at the date obtained but does not purport to provide all of the information that may be necessary or desirable to enable an intending contracting party to determine whether or not to enter into a contract or arrangement with Bank in relation to the provision of services.

The RFP document is not a recommendation, offer or invitation to enter into a contract, agreement or any other arrangement, in respect of the services. The provision of the services is subject to observance of selection process and appropriate documentation being agreed between the Bank and any successful Bidder as identified by the Bank, after completion of the selection process as detailed in this document. No contractual obligation whatsoever shall arise from the RFP process unless and until a formal contract is signed and executed by duly authorized officers of Union Bank of India with the Bidder. The purpose of this RFP is to provide the Bidder(s) with information to assist the formulation of their proposals. This RFP does not claim to contain all the information each Bidder may require. Each Bidder should conduct their own investigations and analysis and should check the accuracy, reliability and completeness of the information in this RFP and where necessary obtain independent advice. Union Bank of India makes no representation or warranty and shall incur no liability under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this RFP. Union Bank of India may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP.

GENERAL INSTRUCTIONS TO BIDDERS

All bidders must note that this being E-tender, bids received only through online on E-tendering portal <https://ubi.abcprocure.com> shall be considered as an offer. ***Any bid submitted in physical form will not be received or opened and shall be summarily rejected.***

Procedure for submission of E-tender by bidder:

Interested bidders who wish to participate should visit website <https://ubi.abcprocure.com> which is the ONLY website for bidding their offer. Further, the procedure is as follows:

1. Register your company in website <https://ubi.abcprocure.com> for obtaining a Login ID and Password.
2. Using the login ID, password and digital signature, login in to the tender portal to download the tender document. It is mandatory for the Bidders to have a valid Digital Signature Certificate - Signing and Encryption (Class - II or Class - III) issued by any of the valid Certifying Authority approved by Govt. of India as per IT Act, 2000. DSC on **Organization name** is required, if bidder want to participate on behalf of his/her Company.
3. Pay Earnest Money Deposit (i.e. EMD) through Demand Draft (i.e. DD)/Bank Guarantee (i.e. BG) and upload the scan copy in website.
4. Upload supporting documents by clicking "Mapped Documents". Then submit the tender. Take a print screen of "Bid successfully submitted" message for reference.
5. Primary Contact Numbers:- M:- 9081000427
 - a. Mr. Samjad khan - 079-68136868, M: 9265871720, samjad@auctiontiger.net
 - b. Jaymeet Rathod - 079-68136829, jaymeet.rathod@eptl.in
 - c. Vinayak Khambe - 079-68136835, vinayak.k@eptl.in
 - d. Nadeem Mansuri - 079-68136853, nadeem@eptl.in
 - e. Nandan Valera - 079-68136843, nandan.v@eptl.in
 - f. Hemangi Patel - 079-68136852, hemangi@eptl.in
 - g. Kanchan Kumari - 079-68136820, kanchan.k@eptl.in
 - h. Deepak Narekar - 079-68136863, deepak@eptl.in
 - i. Anshul Juneja - 079-68136840, anshul.juneja@eptl.in
 - j. Mehnaz Bano - 079-68136831, mehnaz@eptl.in
 - k. Sujith Nair - 079-68136857, sujith@eptl.in
 - l. Devang Patel:- 079-68136859, devang@eptl.in
6. Alternate Contact No.:- Ms. Shubhangi Banodiya:- 079-68136826/6824, M:9879996111, shubhangi@auctiontiger.net.
7. System requirement for online bid submission:
 - a. Computer / Laptop (Notebook) with internet connection of minimum 256 kbps speed.
 - b. Operating system - Windows XP Service pack -3 / VISTA/ Windows 7 or above.

Bidder must submit the offer before online closing date & time. The website will automatically stop accepting the offer after online closing date and time.

NOTE: Submission of any bid document through offline mode will not be accepted except Cost of RFP, Bid Security (EMD) and Pre-Contract Integrity Pact (on plain paper) signed by authorized signatory and should be submitted on or before last date & time of bid submission.

Abbreviations

The long form of some abbreviations commonly used in the document is given below:

Abbreviation	Description
3DES	Triple Data Encryption Standard
AAA	Authentication, Authorization and Accounting
ACD	Automatic Call Distribution
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
ASM	Any Source Multicast
AV	Anti-Virus
BCP	Business Continuity Planning
BFSI	Banking, Financial Services and Insurance
BG	Bank Guarantee
BGP	Border Gateway Protocol
BIA	Business Impact Analysis
BSNL	Bharat Sanchar Nigam Limited
CBM	Class-Based Marking
CBS	Core Banking Solutions
CBTP	Class-Based Traffic Policing
CBTS	Class-Based Traffic Shaping
CBWFQ	Class Based Weighted Fair Queuing
CBWRED	Class-Based Weighted early Detection
CDMA	Code Division Multiple Access
CHAP	Challenge Handshake Authentication Protocol
CIFS	Common Internet File System
CLI	Command Line
CNAME	Canonical Name
CoS	Class of Service
CPE	Customer Premises Equipment
cRTP	Compressed Real Time Transport Protocol
C-SOC	Cyber Security Operation Centre
CUG	Closed User Group
dACL	Discretionary Access Control List
DC	Data Center
DDI	DNS, DHCP & IP Address Management
DDOS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DID	Direct Inward Dialling
DKIM	Domain Keys Identified Mail
DMARC	Domain based Message Authentication, Reporting and Conformance
DNS	Domain Name System

DOT	Department of Telecom
DR Site	Disaster Recovery Site
DRAM	Dynamic Random Access Memory
DRC	Disaster Recovery Centre
DTMF	Dual Tone Multi Frequency
EAP-FAST	Extensible Authentication Protocol - Flexible Authentication via Secure Tunnelling
EAP-TLS	Extensible Authentication Protocol - Transport Layer Security
eBGP	External Border Gateway Protocol
ECMP	Equal Cost Multipath
EEE	Energy Efficient Ethernet
EMD	Earnest Money Deposit
EMS	Enterprise Management System
EPABX	Electronic Private Automatic Branch Exchange
ESN	Electronic Serial Number
EVDO	Evolution Data Only/Optimized
FCC	Federal Communication Commission
FIS	Fidelity National Information Services Inc.
FSS	Financial Software & Systems Pvt. Ltd
GRE	Generic Routing Encapsulation
GSS TSIG	Generic Security Service Transaction Signature Standard
GUI	Graphical User Interface
HDLC	High Level Data Link Control
HSPA	High Speed Packet Access
HSRP	Hot Standby Routing Protocol
HTTP	Hyper Text Transfer Protocol
iBGP	Interior Border Gateway Protocol
ICMP	Internet Control Message Protocol
IDRBT	The Institute for Development & Research in Banking Technology
IEC	International Electro-technical Commission
IEEE	Institute of Electrical & Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange
IPAM	Internet Protocol Address Management
IPSEC	Internet Protocol Security
ISATAP	Intra site Automatic Tunnel Addressing Protocol
ISO	International Organisation for Standards
ISP	Internet Service Provider
ITMS	Information Technology Managed Services
IVR	Interactive Voice Response
LACP	Link Aggregation Control Protocol
LAN	Local Area Network

LCR	Least Cost Routing
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode
LLDP-MED	Link layer discovery Protocol Media endpoint discovery
LLP	Limited Liability Partnership
LOI	Letter of Intent
LTE	Long Term Evolution
MDN	Mobile Directory Number
MIB	Management Information Base
MPLS	Multi Protocol Label Switching
MSID	Mobile Station ID
MSTP	Multiple Spanning Tree Protocol
MTNL	Mahanagar Telecom Nigam Limited
MTTR	Mean Time to Repair
MX	Mail Exchange
NAC	Network Access Control
NAPTR	Name Authority Pointer
NAT	Network Address Translation
NDA	Non-Disclosure Agreement
NDC	Near Data Center
NID	Network Interface Device
NMS	Network Management System
NOC	Network Operation Center
NPCI	National Payment Corporation of India
NPM	Network Performance Monitoring
NS	Network Simulator
NSF	Non Stop Forwarding
NSI	Network System Integrator
NSIC	National Small Industries Corporation
NTP	Network Time Protocol
OSPF	Open Shortest Path First
P&L	Profit and Loss
P2P	Peer to Peer
PAP	Password Authentication Protocol
PBG	Performance Bank Guarantee
PCM	Pseudo Code Modulation
PERT	Program Evaluation Review Technique
PKI	Public Key Infrastructure
PO	Purchase Order
PPP	Point to Point Protocol
PPPoE	Point to Point Protocol over Ethernet
PRI	Primary Rate Interface

PSB	Public Sector Bank
PSK	Pre Shared Key
PSTN	Public Switched Telephone Network
PSU	Public Sector Undertaking
QoS	Quality of Service
QSFP	Quad Small Form Factor Pluggable
RADIUS	Remote Authentication Dial in User Service
RBI	Reserve Bank of India
RED	Random Early Detection
RF	Radio Frequency
RFP	Request for Proposal
RIP	Routing Information Protocol
RoHS	Restriction of Hazardous Substances
RPVST	Rapid Per VLAN Spanning Tree
RRB	Regional Rural Bank
RSA	Rivest, Shamir and Adelman
RSVP	Resource Reservation Protocol
RTGS	Real Time Gross Settlement
RTP	Real Time Transport Protocol
SDN	Software Defined Network
SDWAN	Software Defined Wide Area Network
SFP	Small Form Factor Pluggable
SHA	Secure Hash Algorithm
SID	System Identification Number
SIM	Subscriber Identity Module
SIP	Session Initial protocol
SLA	Service Level Agreement
SMB	Server Message Block
SNMP	Simple Network Management Protocol
SPF	Sender Policy Framework
SRTP	Secure Real Time Transport Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
STP	Spanning Tree Protocol
SWIFT	Society for Worldwide Interbank Financial Telecommunications
TACACS+	Terminal Access Controller Access control System Plus
TCO	Total Cost of Ownership
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TEC	Telecommunication Engineering Centre
TLS	Transport Layer Security
TO	Technical Offer

ToS	Type of Service
TRAI	Telecom Regulatory Authority of India
UBI	Union Bank of India
UDLD	Unidirectional Link Detection
UDP	User Datagram Protocol
VCCI	Voluntary Control Council for Interference
VLAN	Virtual Local Area Network
VLSM	Variable Length Subnet Mask
VOIP	Voice Over Internet Protocol
VoQ	Virtual Output Queuing
VPN	Virtual Private Network
VRF	Virtual Route Forwarding
VRRP	Virtual Router Redundancy Protocol (VRRP)
VSAT	Very Small Aperture Terminal
WAN	Wide Area Network
WFQ	Weighted fair queuing
Wi-Max	Worldwide Interoperability for Microwave Access
WRED	Weighted Random Early Detection
XMPP	Extensible Messaging and Presence Protocol
ZTP	Zero Touch Provisioning

Bid Details:

RFP Ref. No. UBI/DIT/2019-20/WAN/01

Start Date & Time of issue of RFP/ Document Download	14.01.2020 at 11:00 Hours
Date and time of pre-bid meeting	21.01.2020 at 11:00 Hours (venue: 2 nd Floor at address mentioned for opening of bids)
Last date and time for submission of query	22.01.2020 by 17:00 Hours
Last date and time of Downloading of RFP	04.02.2020 by 15:00 Hours
Last date and time for submission Of Bidding Document	04.02.2020 by 16:00 Hours
Date and Time of Technical Bid Opening	04.02.2020 at 16:15 Hours
Place of opening of Bids	Union Bank of India, Department of Information Technology (5 th Floor), Technology Centre, Adi Shankaracharya Marg, Opp Powai Lake, Powai, Mumbai.
Address & Contact Numbers	As above Tel:(022) 25710507/528/527/236
Cost of RFP	Rs.10,000/- (Rupees Ten thousand only) in the form of Demand Draft in favor of Union Bank of India, Payable at Mumbai.
Security Deposit/Earnest Money Deposit (EMD)	Rs.1,50,00,000/- (Rupees One Crore Fifty lac Only) in the form of Demand Draft in favor of Union Bank of India, payable at Mumbai. EMD can also be paid in the form of Bank Guarantee (BG) of any scheduled commercial Bank other than Union Bank of India, Andhra Bank and Corporation Bank valid from the date of submission of RFP for a period of minimum 45 days beyond the final bid validity period.
Contact details	Interested Bidders are requested to send the email to: abhijit@unionbankofindia.com dnpeter@unionbankofindia.com madhan.r@unionbankofindia.com containing below mentioned information, so that in case of any clarification same may be issued: Name of company, contact person, Mailing address with Pin Code, Telephone No., Mobile No., email address etc.

Note: Bids once submitted will be treated as final and no further correspondence will be entertained on this. No bid will be modified after submission of bids. No bidder shall be allowed to withdraw the bid.

Table of Contents

1.	Introduction.....	12
2.	Integrity Pact (IP)	12
3.	Definition	12
4.	Objectives of the RFP	13
5.	Bank's Wide Area Network	13
6.	Invitation to Bidders	15
7.	Eligibility Criteria	15
8.	Broad Scope of Work.....	17
9.	Project Timelines (Delivery, Installation, Configuration and Integration)	51
10.	Transition Period	52
11.	Execution of Work	53
12.	Compliance with IS/Cyber Security Policy.....	53
13.	Cost & Currency.....	53
14.	Price Variation	54
15.	Acceptance of Offer.....	54
16.	Language of Bid	54
17.	Instructions for Bid Submission	54
18.	Award of Contract	63
19.	Price Composition.....	63
20.	Taxes and Duties.....	63
21.	Rejection of Bid.....	64
22.	Modification and Withdrawals of Bid	64
23.	Pre Bid Meeting.....	64
24.	RFP Response.....	65
25.	Payment Terms	65
26.	Order Cancellation/ Termination of Contract	66
27.	Contract Period.....	67
28.	Liquidated Damages (LD)	67
29.	Service Level Agreement and Penalties	68
30.	Authorized Signatory.....	73
31.	Limitation of Liability	74
32.	Confidentiality	74
33.	Indemnity	74
34.	Intellectual Property Rights.....	75
35.	Non-Transferable Offer	76
36.	Responsibility for Completeness.....	76
37.	Audit	76
38.	Force Majeure	77
39.	Exit Clause	77
40.	Termination of Contract	78
41.	RFP Ownership	79
42.	Proposal Ownership.....	79
43.	Patents Rights	79

44.	Conflict of Interest.....	79
45.	Disaster Recovery & Business Continuity Planning (BCP)	80
46.	Network audit	81
47.	Technological Up gradation.....	81
48.	End of Sale & End of Support	81
49.	Tender/RFP Cancellation.....	81
50.	Compliance with Laws	82
51.	Information Ownership	82
52.	Publicity	83
53.	Outsourcing Policy.....	83
54.	Arbitration	83
55.	Jurisdiction	83
56.	Submission of Bids.....	83
57.	Annexure A - Letter of Acceptance.....	84
58.	Annexure B - Bidder's Profile Format.....	86
59.	Annexure C - Eligibility Criteria.....	88
60.	Annexure D - Compliance to RFP Terms & Conditions.....	91
61.	Annexure E - Technical Compliance	93
62.	Annexure E (A) - Configuration of proposed solutions.....	185
63.	Annexure F - Unpriced Indicative Commercial Bid.....	187
64.	Annexure F (A) - Indicative Commercial Bid	198
65.	Annexure G - Declaration for Compliance	209
66.	Annexure H - Undertaking By Bidder	210
67.	Annexure I - Process for Evaluation of Bids.....	211
68.	Annexure J - Confidentiality / Non Disclosure Agreement.....	216
69.	Annexure K - Reference Site Details.....	222
70.	Annexure L - Business Rules for Reverse Auction	223
71.	Annexure L (A) - Compliance Statement - Reverse Auction	229
72.	Annexure L (B) - Letter of Authority for Participation in Reverse Auction	230
73.	Annexure L (C) - Undertaking of Process Compliance Statement for R A.....	231
74.	Annexure M - Pre Contract Integrity Pact.....	233
75.	Annexure N - Letter for Refund of EMD.....	239
76.	Annexure O - Bid Query Format.....	240
77.	Annexure P - Bank Guarantee for EMD	241
78.	Annexure Q - Format of Performance Bank Guarantee.....	243
79.	Annexure R - Know Your Employee (KYE) Clause	245
80.	Annexure S - Existing Infrastructure to be Managed by the selected NSI	246
81.	Annexure T - Resource Details of NSI	247
82.	Annexure U - Undertaking of Information Security	248
83.	Annexure V - List of Regional Offices	249
84.	Annexure W - Certificate of Local Content	250
85.	Annexure X - Standard Terms and Conditions for Outsourcing.....	251
86.	Annexure Y - Undertaking of Authenticity for Networking Hardware	264

Union Bank of India

1. Introduction

Union Bank of India (hereinafter referred to as BANK), is one of the leading Nationalized banks in India having a network of over 4400+ branches / offices and 6500+ ATMs spread across the country and expanding further rapidly. Bank has also presence in more than four countries.

Bank has implemented a Centralized Core Banking Solution covering all its branches and is extending Banking services to its customers through a number of delivery channels like ATM, e-banking, SMS banking, Mobile Banking, POS etc. Keeping in tune with changing times and to provide its customers more efficient and speedy service, the Bank has taken several initiatives in the field of computerization and implementation of various software/technologies.

2. Integrity Pact (IP)

Vendors/bidders/sellers, only those who commit themselves to Integrity Pact (IP) with the Bank, would be considered competent to participate in the bidding process. In other words, entering into this pact would be the preliminary qualification.

IP shall cover all phases of contract i.e. from the stage of Notice Inviting Tenders (NIT)/Request for Proposals (RFP) till the conclusion of the contract i.e. final payment or the duration of warrantee/guarantee. Format of IP is attached as [Annexure M](#) for strict compliance.

The following Independent External Monitors (IEMs) have been appointed by the Bank, who will review independently and objectively, whether and to what extent parties have complied with their obligation under the pact.

- a. Mr. B Ravichandran, IRS (C&CE) (Retd.),
E-mail- bravi1958@gmail.com
- b. Mr. Ashwani Kumar,
E-mail- ashwani_ashwani1@yahoo.co.in

3. Definition

- 3.1. 'Bank' means unless excluded by and repugnant context or the meaning thereof, shall mean 'Union Bank of India', described in more detail in clause 1 above and which has invited bids under this Request for Proposal and shall be deemed to include its successors and permitted assigns.
- 3.2. 'RFP' means this Request for Proposal prepared by Union Bank of India for Network Management support services for Wide Area Network of the Bank.
- 3.3. 'Bidder' means a vendor or NSI who is submitting the proposal in response to this RFP.
- 3.4. 'Contract' means the agreement signed by successful bidder and the Bank at the conclusion of bidding process, wherever required.
- 3.5. 'Proposal' means that Technical/Financial proposal including any documents submitted by the bidder as per the formats prescribed in the RFP.

- 3.6. 'Solution' means providing services for Network Management support services for Wide Area Network of the Bank.

4. Objectives of the RFP

- 4.1. This document has been prepared by Bank for selection of Network System Integrator (NSI) for supply, installation, maintenance and management of network equipments (i.e. router, switch, IP Phone, Modem, rack, NPM etc.) under rental model. Bank will avail network services under managed services to maintain the existing network and connect future branches for 5 years. Bank will retain its MPLS services availed from various service providers. The selected vendor will maintain the last mile line which connects the CPEs to PE router at MPLS PoP. The selected vendor will maintain the existing primary and secondary communication links and assist in commissioning primary and secondary links for new branches.
- 4.2. In addition to this, Bank also intends to have a Network Operation Center (NOC) service in a hybrid model to ensure smooth monitoring and management of network infrastructure. The NSI provider will monitor the infrastructure on 24*7*365 basis from its established NOC located in India and provide alerts to the Bank for any event/incidents. The on-site team of selected vendor stationed at the Bank's premises will be responsible for management and maintenance related activities. The bidder shall submit the list of such organization(s) and the roles and responsibilities as a part of the RFP bid.
- 4.3. The 'Request for Proposal' (RFP) document is now being issued requesting Network System Integrators to submit their responses to the Bank for supply, installation, commissioning and maintenance network equipments i.e. Router, switches, modems, IP Phones, Network Racks, etc under a managed service on monthly rental basis for DC, DRC, NDC, Central Office and branches/offices. For commercial evaluation, the Bank will adopt 'Reverse auction' process to finalize the vendor for the project. The procedure for the 'Reverse auction' is furnished in Annexure L.
- 4.4. Bank will not accept any deviations from the terms and conditions specified in the tender. Deviations could result in disqualification of the offer made by the vendor at the discretion of the Bank.

5. Bank's Wide Area Network

- 5.1. Wide Area Network (WAN) is an important component in the IT infrastructure landscape of every Bank. This provides branches/offices access to all centralized applications. The Bank has connected all its branches/offices through MPLS network.
- 5.2. Apart from having approximately 4400+ branch and office locations, The Bank has setup Data Centre at Powai, Mumbai and Disaster Recovery Centre (DRC) at Bengaluru. Also Bank has established its Near Site Data Centre (NDC) at Nariman Point, Mumbai. Powai office is having 8 floors and Nariman Point offices has 17 floors connected by Local Area Network. The network and network equipments at these locations are managed and maintained by the existing NSI.

- 5.3. Presently Bank have connected 4400+ branches and offices on Wide Area Network (WAN) primarily through layer 3 MPLS VPN with bandwidth capacity ranging from 2 Mbps to 20 Mbps. Primary connectivity in majority of branches are provided via BSNL MPLS. In order to ensure business continuity, Bank has also subscribed alternate link in the form of RF, VSAT and Wi-MAX. Currently all Bank sites are connected through Cisco equipment viz. routers, switches, IP phones, etc. BSNL provides primary MPLS services to the Bank. In addition to this, the Bank has M/s Bharti Airtel, M/s Vodafone Idea, M/s Tata Communication as alternate MPLS service providers. About 800 branches are connected through VSAT whereas 80 other branches have VSAT as the primary mode of connectivity. The Bank has also been continuously exploring, testing and implementing the latest network technologies (like 4G and WAN optimization) in the Bank's Wide Area Network.
- 5.4. The Data center, Near Site and the DR are interconnected with multiple MPLS as well as P2P links. Backhaul of MPLS links from service providers terminate at all three locations. The Bank has also deployed Internet Leased Lines from M/s TCL Communications. Further, the Bank has connectivity to the Reserve Bank of India, NPCI, IDRBT, third party vendors, SWIFT network, etc.
- 5.5. Presently, the network of the Bank is maintained by Network System Integrator (NSI) M/s. HCL Comnet Ltd under the "outsourced model".
- 5.6. The Bank has implemented site-to-site secure encrypted tunnel (GET VPN solution) from all branches/offices to the Data Centre, the NDC & the DR Site for securing financial applications data on the network. Dedicated router in High availability (HA) mode is installed at these sites to terminate the backhaul of the MPLS link providers.
- 5.7. The Bank has implemented Cisco Unified Communication (UC) system which provides Instant messaging, presence, audio and video conferencing facility. The facility is extended to all the branches/offices.
- 5.8. The Bank has implemented the Polycom Video Conference system. The MCU is installed at Data Center, Powai, Mumbai and 140 nos. of VC endpoints are installed in the administrative offices across country. The VC system is also integrated with UC systems.
- 5.9. The Bank has implemented Aruba ClearPass Network Access Control (NAC) across all branches/offices for centralize control of access of the network by end point system and posture validation. DHCP service is enabled on branch router for auto assignment of IP Address to network devices. Bank has also setup captive Cyber Security operation Center (C-SOC) wherein 24*7*365 monitoring of Bank's critical assets is being carried out by skilled resource. As part of C-SOC, security solution including but not limited to Perimeter Security, Endpoint security, User and Data Security, Deception, Vulnerability Management are being deployed and managed on ongoing basis.
- 5.10. The Indicative list of the major devices like routers and switches used by the Bank in current Network are given in [Annexure-S](#).

6. Invitation to Bidders

Bank invites proposal from the eligible entities for Network Management support services for Wide Area Network of the Bank.

No contractual obligation on behalf of the Bank whatsoever shall arise from the RFP process unless and until a formal contract is signed & executed by duly authorized officers of the Bank and the successful bidder. However, until a formal contract is prepared and executed, this offer together with Bank's written acceptance & notification of award shall constitute a binding contract with the successful bidder.

Bidders are expected to examine all instructions, forms, terms, specifications, and other information in the RFP document. Failure to furnish any information required by the RFP document or to submit a bid not substantially responsive to the RFP document in every respect will be at the Bidder's risk and shall result in the rejection of its bid. The procedure and terms & conditions for submission of bid are enumerated in this RFP.

All offers of the bidders shall be unconditional and once accepted whether with or without modifications by the Bank shall be binding between the Bank and such Bidder.

The Document may be obtained from the Bank at the communication address given below or can be downloaded from Bank's Website www.unionbankofindia.co.in or from government portal eprocure.gov.in or from Bank's e-Procurement Portal <https://ubi.abcprocure.com>.

7. Eligibility Criteria

Only those Bidders who fulfill the criteria are eligible to respond to the RFP. Document/s in support of eligibility criteria are required to be submitted along with the Technical Bid. Offers received from the bidders who do not fulfill any of the eligibility criteria are liable to be rejected.

- 7.1. The bidder has to submit Integrity Pact (IP) signed by authorized signatory as prescribed format mentioned in Annexure M on plain paper in advance (not prior to issuance of RFP) or at the time of bid submission. Bidder shall be liable for rejection in case of non-submission of the same.
- 7.2. The bidder should be a registered/existing company under Company Act 1956/2013 or PSU/Government Organization/ partnership firm / LLP and should be in existence for last 5 years from the date of RFP. Certificate of incorporation/certificate for commencement of business/other relevant documentary proof is to be submitted.
- 7.3. Bidder should have had a minimum annual turnover of Rs.300 Crore each during last three financial years i.e. 2016-17, 2017-18 & 2018-19. This must be the individual company turnover and not that of any group of companies. In case the audited financials for the year 2018-19 is not available, CA Certificate should be submitted. Copies of the audited balance sheet and P&L Statement of the company showing the same is to be submitted.

- 7.4. The Bidder should have operating Profit (as EBITDA i.e. Earnings, Before Interest, Tax, Depreciation & Amortization) in the last three financial years i.e. 2016-17, 2017-18 & 2018-19. In case the audited financials for the year 2018-19 is not available, CA Certificate should be submitted. Copies of the audited balance sheet and Profit/Loss statement of the company is to be submitted.
- 7.5. The OEMs of proposed SD-WAN, Switches, Routers & Unified Communication solution should have operating Profit (as EBITDA i.e. Earnings, Before Interest, Tax, Depreciation & Amortization) in the last three financial years i.e. 2016-17, 2017-18 & 2018-19. Copies of the audited balance sheet/Certificate of the company are to be submitted.
- 7.6. The bidder should have experience in setting up and maintaining a large wide area network based on MPLS/leased line in India (Minimum 1000 sites in one project) during last 5 years. Letter/PO from user organization is to be submitted.
- 7.7. The bidder should have a fully operational Network Operation Center (NOC) in India for at least 5 years and must be providing 24*7*365 support to at least two corporate having minimum 3000 primary links between them. It is also to be noted that NOC must be ISO 27001:2013 certified. Bidder should also have BCP for NOC in place. (Copy of certificate needs to be submitted.)
- 7.8. The bidder must have employed minimum 100 certified network engineers in their organization's payroll (NSI to submit the details of network engineers employed by them with names and qualifications as per [Annexure T](#)).
- 7.9. The bidder should have adequate support infrastructure with minimum 25 own or franchisee logistical centers across India out of which at least one support infrastructure should be necessarily located in Uttar Pradesh, Karnataka and Andhra Pradesh/Telangana each. (NSI to submit a list of own logistic centers along with full postal address, name of the center in-charge and their telephone numbers.)
- 7.10. Proposed SD-WAN Solution should have been implemented with minimum 250 CPEs in India in one organization. The said solution should be live with all SD-WAN components including but not limited to controller, Orchestrator, Analytics. (NSI/OEM needs to submit reference letter/Purchase Order/Sign-off from user organization.)
- 7.11. Proposed OEM's Switch as part of the RFP should have a minimum installation base of 1500 in one organization in India during last 5 years. (NSI/OEM needs to submit reference letter/Purchase Order/Sign-off from user organization).
- 7.12. Proposed Non-Video IP Phone as part of the RFP should have a minimum installation base of 1500 IP Phone in one Organization in India during the last 5 years. (NSI/OEM needs to submit reference letter/Purchase Order/Sign-off from user organization).
- 7.13. Proposed Network Performance Monitoring (NPM) Solution should have been deployed in two organizations in India. (NSI/OEM needs to submit reference letter/Purchase Order/Sign-off from user organization.)

- 7.14. Proposed DNS, DHCP & IP Address Management (DDI) Solution should have been deployed in two organizations in India. (NSI/OEM needs to submit reference letter/Purchase Order/Sign-off from user organization.)
- 7.15. Bidder should be either an Original Equipment Manufacturer (OEM) of devices/software solutions or authorized partner of OEM. In case the bidder is an Authorized partner of the OEM, Bidder needs to provide Manufacturer Authorization Form (MAF) from OEM stating that bidder is authorized partner of OEM and authorized to participate in this tender and in case the bidder is not able to perform obligations as per contract during the contract period, contracted services will be provided by OEM. OEM can quote directly or through authorized partners. However, both i.e. OEM & their authorized partner cannot participate in the RFP. In case, both (OEM & his authorized partner) participate, only bid of the OEM will be considered.
- 7.16. OEMs, whose hardware/software is proposed to be supplied to the Bank, must have presence in India and should be able to support the project in Mumbai & Bengaluru during contract period. Document Proof should be submitted.
- 7.17. The companies or firms, bidding for the above tender, should have not been black listed by any of Government Authority or Public Sector Undertaking (PSUs). The bidder shall give an undertaking (on their letter head) that they have not been black listed by any of the Govt. Authority or PSUs. In case, in the past, the name of their Company was black listed by any of the Govt. Authority or PSUs, the same must have been removed from the black list as on date of submission of the tender, otherwise the bid will not be considered. Undertaking on Company's letterhead as per [Annexure H](#) to be submitted by the bidder.

Note: The Bidder must comply with all the above-mentioned criteria. Non-compliance of any of the criteria will entail rejection of the offer summarily. The requirements mentioned above are mandatory. The cut-off date for the above criteria's will be the Date of submission of RFP.

Bidder should fulfill all the Eligibility criteria. Only those who fulfill all the eligibility criteria will qualify for further evaluation. Documents required to be submitted along with Technical bid.

Photocopies of relevant documents / certificates as mentioned above in support of the claims made. The Bank reserves the right to verify / evaluate the claims made by the Bidder independently and can accept or reject without any explanation to the Bidder. Reference Site Customer Name and Contact information to be provided to the Bank with whom discussion can be done.

8. Broad Scope of Work

The contract will be for a period of 5 years. Hardware to be provided for execution of project should be sized for 10000 branches by considering functional & technical requirements as per in-scope solutions. In case it is found that the hardware is not sized adequately or the hardware utilization goes beyond the threshold limit of 80%, the Bidder has to provide additional hardware at no additional cost to meet the performance parameters set by the Bank.

The Scope of work for providing Network Management Support Services for Wide Area Network includes but not limited to design, supply, configuration, implementation, customization, integrations, monitor, manage, backup, documentation, training, warranty support, post warranty maintenance support and any other activities if contracted related to or connected to the WAN and LAN Network Infrastructure, devices and technologies. Scope of work is given in three parts, viz.

- 1) Scope of work for Network Support Services
- 2) Scope of work for Network Devices
- 3) Scope of work for OEM

8.1. Scope of Work for Network Support Services

8.1.1. General Scope

- 8.1.1.1. Under the managed services model, Bank will not incur any capital expenditure for establishment of the network. All the CPEs or network devices of Server infrastructure supplied and deployed for connecting, managing and monitoring the branches by the selected NSI will be owned by the NSI. NSI will deploy the network equipments as per specified in this RFP document. Bank will make the payment to NSI for providing network services (equipments and link maintenance) on a periodical basis based on the network SLA.
- 8.1.1.2. The network to be managed, maintained and monitored by the Successful Bidder is consisting of entire Wide Area Network. Besides this, Successful Bidder has to manage the Local Area Network at Branches/offices/ATM, DC, DRS & other offices and has to integrate WAN network with the Local Area Network at each of the offices.
- 8.1.1.3. The selected vendor will replace the network equipment (i.e. Router, switches, modems, IP phones, Racks) of existing 4400 locations as per directions of Bank. The NSI have to replace the equipments before the expiring of contract date of existing vendor to avoid any downtime. Further, as part of continual growth, Bank keep on opening new branches every year. The selected NSI will connect the proposed branches/offices as and when it will be opened during the contract period. The selected NSI will be responsible for monitoring, management and maintenance of entire network for 5 years.
- 8.1.1.4. The selected NSI will connect the existing branches, which are connected through various modes including but not limited to MPLS, RF, VSAT, Wi-MAX, and 4G. The selected NSI will also be responsible to connect the additional/new branches proposed to be opened during the contract period.
- 8.1.1.5. The selected NSI is required to deliver all the required equipments meant for a branch i.e. Router, switch, IP Phone, rack, modem in a single shipment. Bank will not accept the partial delivery of the equipments. The partial delivery or installation will not be considered as installed. Payments for the site will commence after successful commissioning of solution at DIT and all the equipment are commissioned and installation report is signed off and configured on vendor's NOC in India.
- 8.1.1.6. The selected NSI is required to configure the commissioned network equipments and the Central Management servers and NOC portal for Management and monitoring/SLA

reporting. Bank will begin the rental payment for the equipments only after the deployment of the site on NOC portal.

- 8.1.1.7. The selected NSI is responsible for taking backup of all in-scope solution/device. The backup shall include but not limited to configuration backup, Log backup and same needs to be stored for contract period. Bidder shall also provide and maintain Backup solution including hardware software & licenses for taking Backup.
- 8.1.1.8. The NSI will be responsible for procuring and managing adequate & redundant MPLS/P2P connectivity of required bandwidth from the Bank's DC, DR to their NOC. In case it is observed that provided bandwidth is undersized, bidder has to upgrade that same without any additional cost to the Bank.
- 8.1.1.9. The selected NSI should monitor all the WAN network devices and communication links from the NOC and submit the reports as per NOC report details.
- 8.1.1.10. The selected NSI will also be responsible for monitoring, maintenance and management of Local Area Network (LAN) of Data Centre at Powai, Central Office at Nariman Point and DR Site at Bengaluru.
- 8.1.1.11. All the hardware and software deployed under this project by the NSI should be IPv4 and IPv6 enabled. Bank may decide the implementation of IPv6 at any stage during the contract period.
- 8.1.1.12. The NSI should prepare the design document for DC, NDC and DR for all existing and future applications in respect of the network and conduct the DR Drills as per the application requirement.
- 8.1.1.13. All the hardware and software provided to Bank by the NSI under this project should be licensed and legally obtained. All the hardware and other equipments supplied should be original, brand new and solution must be supplied with original and complete documentation, printed in English language only.
- 8.1.1.14. Depending on the requirement, Bank will place the delivery instructions or additional purchase orders from time to time during the contract period.
- 8.1.1.15. As the equipment during the contract will be in the book of NSI, all necessary licenses, up gradation and down gradations, OEM support, insurance etc. for CPEs will be arranged by the NSI without any cost to the Bank. Bank will only pay the charges towards the usage of equipment and services based on SLAs. Bank will subscribe and pay for the network bandwidth to Telecom Service Providers where NSI should co-ordinate.
- 8.1.1.16. Presently Bank has connected all branches/offices through L3 VPN MPLS network and backup of MPLS link is RF/4G/Wi-MAX/VSAT. Bank has also subscribed secondary MPLS link from Other Telecom Service provider for maintaining BCP. In case Bank make any change in links, ISPs, Mode of connectivity, the selected NSI has to make, manage, deploy the configuration.
- 8.1.1.17. In case of Non-SDWAN branch, selected NSI has to test the backup links once in a month and need to submit the report with status of backup links.
- 8.1.1.18. Selected NSI should develop a Standard Operating Procedure (SOP) for day to day operation for management and monitoring of in-scope devices. SOP shall cover step by step illustrative guide with required screenshot for carrying out any operation.

- 8.1.1.19. Selected NSI is responsible for reporting and logging of network incidents through the use of appropriate automated ticketing tools. NSI should Track and monitor the closure of these incidents and escalation of these incidents to appropriate ISP/teams/ individuals in the Bank.
- 8.1.1.20. Maintenance and upkeep of the network equipment deployed under this project by the NSI shall be the responsibility of the NSI. The Bank will provide necessary UPS power for the equipment to be deployed by the NSI. Bank shall have no responsibility for any damage to the equipment on account of voltage fluctuation etc.
- 8.1.1.21. In case of equipments provided to bank under this project declared “Out of support” by OEM, NSI will deploy the similar or next available higher version of the equipment during the contract period without any additional cost to the Bank up to the remaining period of the contract. Payment & period of the contract and residual value for that equipment will be followed as a continuity of the earlier equipment which is replaced because of ‘Out of Support’.
- 8.1.1.22. The equipments proposed should not have been declared ‘Out of Sale’ at time of delivery. In case of equipments provided to bank under this project are declared “Out of sale” by OEM during the contract period, NSI will deploy the similar or next available higher version of the equipment during the contract period without any additional cost to the Bank for new branches/offices.
- 8.1.1.23. NSI is responsible for preparing, maintaining and updating network documents/diagrams/inventory as per the Bank's requirement. The documents/ diagrams should be updated with proper version controls. Tool/application with adequate license needs to be provided by NSI for creation and maintaining network diagram.
- 8.1.1.24. The contract will be fixed for a period of 5 years. Bank reserves the right to extend the contract period for further 2 years on the same terms and conditions. However, Bank may negotiate the cost.
- 8.1.1.25. The NSI is required to work in tandem with other vendors with whom the Bank is having an agreement for installation/support/implementation /management of existing/proposed banking applications/other activities outsourced like Security Management/Patch Management/AV management etc. which have dependency on Bank's Network infrastructure.
- 8.1.1.26. Bank may, at the end of contract period of 5 years, desire to retain all the installed equipment including its license at the branches/offices on its book value or Rs.1/- whichever is lower. Vendor should agree to this arrangement.
- 8.1.1.27. On behalf of Bank, Bidder shall be responsible for testing new and/or emerging technology such as 5G/LTE/NFV (Network Function Virtualization), etc in the networking field. Based on the outcome of test result, bidder shall appraise Bank on adoption of same.
- 8.1.2. Connecting DC, NDC and DRC**
- 8.1.2.1. The selected NSI should deploy network equipment such as routers, modems, switches, IP phones etc. as per specifications mentioned in RFP.

8.1.2.2. Availability of LAN network of the DC, NDC and DRC are very critical for Bank operation. The selected NSI will manage and monitor the LAN network of DC, NDC and DRC and ensure the high availability of the network at these centers.

8.1.2.3. Bank has procured the Juniper QFX, Cisco Nexus Core switches and other critical equipments installed at DC, NDC and DRC. The selected NSI should manage the network equipment installed at these centers and owned by Bank. Complete list of these devices is provided in [Annexure-S](#).

8.1.3. Connecting the branches / offices to MPLS/Point-to-point leased lines

8.1.3.1. The selected NSI should deploy network equipment such as routers, modems, switches, IP phones etc. as per specifications mentioned in RFP.

8.1.3.2. The selected NSI should implement and maintain the Bank's network topology, the media (such as MPLS, 4G, optic fiber, Broadband etc.) and bandwidth of primary and backup links, as per the network equipment specifications and the IP addressing scheme.

8.1.3.3. The Bank will issue the delivery instruction for supply of network equipments to connect the new branches. The selected NSI should deliver the network equipment to commission the links within 6 weeks from the date of delivery instruction. If the NSI fails to deliver, install, commission the links within the stipulated time schedule or on extended date as may be communicated by the Bank, it will be treated as breach of contract.

8.1.3.4. NSI should maintain database of all the links of the Bank's WAN as per the parameters decided by Bank. NSI will also be responsible to collect the details of each existing link and new link provided by different service providers and add the details to central database. Bank at its discretion, may add/modify said parameters and NSI has to update its database accordingly without any additional cost to Bank.

8.1.4. Selected NSI should ensure at least once a year visit of their field engineers to all Bank Branch/offices to carry out site maintenance activity. As part of site maintenance, field engineer will physically validate deployed network infrastructure, ensure proper dressing and cleaning on deployed network rack and appliance.

8.1.5. IP Address Scheme

8.1.5.1. The NSI is responsible for maintaining and managing IP address and VLAN schema for Bank across all locations.

8.1.5.2. The NSI should design the IP addressing scheme for the new branches/offices proposed to be connected in the RFP in line with the existing IP schema and implement the same at each WAN location after obtaining approval from the Bank.

8.1.5.3. If it is felt necessary that the IP design needs to be changed at a later date, the NSI should design the new IP scheme based on Bank's requirements and implement the same on the network. VLANs are planned at Central Office and Data center Powai. The Vendor shall coordinate with the vendors of LAN, PCs, servers and other equipments and with the help of them migrate old IP addresses to the new scheme. The Vendor shall submit a comprehensive document for the IP address scheme including implementation details for connecting all the branches/offices/ATMs/other locations of the Bank. The

above IP address design, implementation, migration and documentation shall be offered without any extra cost to the Bank.

8.1.5.4. Presently Bank is using IPv4 IP address across the network. If it is felt necessary that the IP design needs to be migrated to IPv6 at later date, the vendor should design the new IPv6 scheme based on Bank's requirements and implement the same on the network without any additional cost to the Bank. Initially both IPv4 and IP v6 will continue simultaneously. The Vendor should submit a comprehensive document for the IPv6 address scheme including implementation details for connecting all the branches/offices/ATMs/other locations of the Bank. The IPv6 address design, implementation, migration and documentation shall be offered without any extra cost to the Bank.

8.1.5.5. The selected NSI will coordinate with MPLS service providers and other third party (TP) vendors for migration of the IP Addresses from IPv4 to IPv6.

8.1.6. Configuration of the devices

8.1.6.1. The NSI shall prepare the basic configuration template for all devices i.e. router, switch, etc. as per the Bank's IT security policy and implement the same across the network to maintain the uniformity of the configuration.

8.1.6.2. The NSI should implement security policy, QoS policy and traffic reengineering policy that will be decided by the Bank. Bank may change policies as per the requirement of the Bank from time to time. The vendor shall coordinate with the service provider for its implementation both at customer-premises-end router and service-provider-edge router.

8.1.6.3. The NSI will be responsible for hardening of OS and other applications that comes under network infrastructure under this project as per the Bank's IT security policy. Bank conducts the audit of the IT systems by Internal and External auditors on yearly basis. Vendor will be responsible for complying with all the audit observations in all respect including but not limited to OS, application, database, etc. for systems provided by the NSI under this project.

8.1.6.4. Bank's technical team will decide from time to time the parameters to audit, which will be provided by the bidder. Based on the requirement, Technical committee will also suggest the implementation of technical aspect such as implementation of security zone, IP Address plan etc. and selected NSI has to implement the committee recommendations.

8.1.7. Network functionalities / modalities

8.1.7.1. Bank shall have the option to integrate any third-party network using any standard network equipments such as routers, modems, switches etc., from any other system integrator / network integrator for its network in future. The NSI will coordinate with such system / network integrator for proper integration. If felt necessary, the Bank, may call upon the selected vendors to maintain and service such third party networks under the framework of the itemized prices agreed under this tender.

8.1.7.2. Bank reserves the right to make changes to the list of locations and any change in the list of location notified by the bank shall be binding on the NSI. The Bank further reserves the right to advise the Vendor to postpone the connectivity schedule including

delivery of hardware, etc., in respect of some of the locations based on Bank's requirements.

- 8.1.7.3. Because of the business requirement, Bank may shift branches/office premises to new locations. All the network equipments including the links need to be shifted to the new premises. The NSI will uninstall the equipments, duly pack them and will transport the equipments to the new location and will reinstall the equipment at the new location. Equipment transportation cost through courier will be reimbursed. Similarly, the NSI will coordinate in shifting/surrendering the links both at old and new locations. Bank will pay the agreed shifting charges to the vendor. Vendor has to carry out link shifting / equipment shifting within 4 weeks from the date of purchase order / work order.
- 8.1.7.4. Based on the requirements, Bank may seek increase/decrease of bandwidth for certain locations. The NSI has to deploy suitable equipment for the same and coordinate with the telecom service provider for commissioning the required bandwidth. Bank will pay the link commissioning charges if the local loop is required to be upgraded. In case of change of equipments to any other category, the Bank will pay the itemized cost for the newly deployed equipment from the date of deployment. Old equipment will be taken back by the vendor at his own cost.
- 8.1.7.5. The Bank reserves the right to place the order in a phased manner in one or multiple lots depending upon availability of connectivity, site readiness etc.
- 8.1.7.6. The Bank may seek delivery of some of the equipments/services quoted, depending upon the requirements envisaged from time to time and will pay the itemized agreed cost to the vendor.
- 8.1.7.7. The NSI, during the contract period, will apply, on behalf of the Bank, for Leased lines/RF/3G/4G/MPLS ports with Basic service Providers. It will be the responsibility of the NSI to co-ordinate with the Basic service Providers and other Government Organizations in obtaining the leased line/RF / 4G / MPLS port connections for all branches / offices across the country. Further, NSI will coordinate with the telecom service provider including submission of line applications, collecting demand notes and submitting the payment drafts to the service providers by obtaining the same from Bank.
- 8.1.7.8. During the period of the Contract, the Bank reserves the right to add other networks to the Banks network.
- 8.1.7.9. Bank reserves the right to Increase /decrease the quantities/types/Bandwidth /designs as mentioned in this RFP.
- 8.1.7.10. The NSI should configure end-to-end traffic engineering (end to end means CE to CE).
- 8.1.7.11. The NSI should Monitor and manage all links for strict compliance with SLA through their NOC.
- 8.1.7.12. The NSI will meet the defined SLAs for uptime of the network and NSI should ensure lower turnaround time in the event of equipment failure.
- 8.1.7.13. The NSI is required to implement End-to-End Router based IPSec encryption (IPSEC/AES) architecture for all existing and new / proposed locations and to DC, NDC and DRC so as to encrypt the data flow based on the requirement of the applications deployed.

- 8.1.7.14. The NSI has to integrate the VPN networks with the LAN segment of the Bank's locations. The NSI has to ensure and enable end-to-end encryption to provide security in the communications.
- 8.1.7.15. The NSI should submit Network Monitoring reports for Link availability and for SLA compliance to obtain payments. Bank might also countercheck the reports generated by its own EMS.
- 8.1.7.16. The selected NSI will charge the Bank on per location (branch/office) basis. Bank has categorized locations with respect to the requirement of equipments and their sizing. The payment will be made location-wise based on the actual number of equipments/lines/links and their uptime that are deployed.
- 8.1.7.17. The selected NSI shall update the software/OS/Patch of network devices as and when required without any additional cost to the Bank.
- 8.1.7.18. The NSI should enable the network for functioning of all the client-server, web-based applications deployed/to be deployed by the Bank, Voice and Video simultaneously. The network should be enabled for functioning of videoconferencing on IP etc.
- 8.1.7.19. The NSI should carryout traffic prioritization at CPE routers in coordination with service providers for Voice, Video and various applications depending on the Bank's requirement.
- 8.1.7.20. The NSI should enable centralized user authentication system for all network equipments.
- 8.1.7.21. The NSI should connect the network to their NOC with suitable redundancy for monitoring and providing various NOC reports such as device/link uptime, link utilization, call/ticket monitoring, SLA Reporting etc., in order to monitor the SLAs at their cost.
- 8.1.7.22. The NSI should coordinate with BSNL/MTNL and other Basic Service Provider for obtaining connectivity, for the locations depending on the Bandwidth requirement.
- 8.1.7.23. The NSI should ensure placement of resident engineers at strategic locations as defined in this document. The Bank has required the resident engineers as per its past experience. In case of more engineers are required at critical locations i.e. DC, NDC and Metros for maintenance of the network, NSI have to place the engineer as per cost identified through this RFP.
- 8.1.7.24. The NSI should carryout maintenance of LAN manageable switches at Bank's Central Office situated in Nariman point, DC at Powai and DR at Bengaluru.
- 8.1.7.25. The NSI should coordinate with third party NSIs for commissioning and maintenance of third party links including routers at third party locations.
- 8.1.7.26. An uptime on a monthly basis for each site shall be provided by the NSI. However, payment will be made on quarterly basis in arrears.
- 8.1.7.27. Maintenance and upkeep of the network equipment provided by NSI shall be the responsibility of the NSI. The Bank will provide necessary UPS power for the equipment to be deployed by the bidder. Bank shall have no responsibility for any damage to the equipment on account of voltage fluctuation, earthing, natural calamities, etc. NSI shall take adequate insurance cover for the equipment provided at the site against theft, damage etc., at its own cost.

- 8.1.7.28. The NSI shall maintain the connectivity at each location on 24*7 basis. Bidder also has to monitor the sites pro-actively through their NOC so as to prevent the link failure. Bidder should take the necessary action to restore the link in case of down time without waiting for down call from Bank.
- 8.1.7.29. The NSI will also take the responsibility of liaising with the Government Departments for obtaining the necessary regulatory approvals, if any. However, the Bank will issue letters that are required and sign such applications as are necessary.
- 8.1.7.30. The NSI has to make his own arrangements to fulfill all delivery formalities like payment of road/entry tax, etc., and should not involve Bank in these activities. Bank will not accept any liability on account of non-payment of taxes etc. by the NSI.
- 8.1.7.31. The NSI will provide escalation procedures and the names of the officials to whom the calls can be escalated for project implementation and network sustenance.
- 8.1.7.32. The NSI shall submit a detailed PERT (Project Evaluation and Review Technique) or Gantt chart, location-wise, within 15 days from the date of receiving the PO/LOI. The NSI shall submit weekly report on the progress of the project and also the status as on the scheduled date and actual date of each activity detailing any deviation from baseline PERT chart to the Bank.

8.1.8. Maintenance and monitoring of network

- 8.1.8.1. The NSI shall do all such configuration as access list, firewall features that are required on the routers or other equipments under their maintenance.
- 8.1.8.2. The NSI shall maintain the network equipments inventory and configuration details.
- 8.1.8.3. The NSI will be responsible for ensuring the quality of service required by each of the applications running on the network. This activity includes application wise investigation of bandwidth usage, network latency, and identification of congestion points, troubleshooting and capacity planning.
- 8.1.8.4. In case, the network latency/jitter/packet loss is more than expected, it shall be the duty of the NSI to investigate the network to find out the cause and rectify the same for achieving the optimal network operation.
- 8.1.8.5. The NSI will be responsible for monitoring of Bank's WAN infrastructure and regular checking of network health. Some of the major activities include but not limited to:
 - 8.1.8.5.1. Daily Networks Health Checklist of all Network Equipment's at data center, DR Site, Near Line Site, Branch Office shall include Interface status/errors, equipment uptime, CPU / memory utilization, Logs, power status, Module status for Core Switch, diagnostic result.
 - 8.1.8.5.2. Finding out status of all links from DC, DR, Office, and branches. If any link is down, the bidder shall initiate steps to resolve the same.
 - 8.1.8.5.3. Capacity/Bandwidth usage monitoring. Need to capture Min/Max/Avg utilization on Daily/Weekly/Monthly basis of all links.
 - 8.1.8.5.4. Monitor port status on network devices.
 - 8.1.8.5.5. Network cabling status and verify connectivity in DC and DR. Co-ordination with respective teams /vendors.

- 8.1.8.5.6. The NSI using his in-house expertise will be responsible for conducting network audits on yearly basic to review the implementation and ongoing operation in regards to protocol usage statistics, Communication Matrix, Bandwidth hoggers. Bidder will evaluate such parameters against industry best practices and provide suggestion to bank as part of official report.
- 8.1.8.5.7. Tracking location-wise WAN bandwidth.
- 8.1.8.5.8. Bandwidth analysis for all applications of the Bank for Link wise (Inbound, Out Bound), Application wise (pre-defined applications), IP wise (Source In, Out and Destination In, Out).
- 8.1.8.5.9. Bandwidth utilization analysis for all applications like Core Banking/Tax Payment (ETDS) /AV updations and Patch updations (when implemented) used by the Bank on WAN and suggest bandwidth sizing of these applications and recommend improvements.
- 8.1.8.6. The NSI shall be a single point of contact to all branches/offices for any problem related to connectivity and IP issues. It would have to analyze the WAN and LAN issues and if related to network or networking equipments would have to initiate steps to resolve the same within the stipulated time. which includes but not limited to:
- 8.1.8.6.1. Identification and troubleshooting of any network problem faced by the Bank within the defined time frame. Co-ordinate with various service providers for early resolution of links, including escalation and co-ordination with the Service Provider for resolution of the problem.
- 8.1.8.6.2. Testing the links for various link errors.
- 8.1.8.6.3. Identification of Configuration/hardware problem of all Network devices of Data Centre, DR Site, NDC, Branches, Zonal Offices, and resolve the same. This would include escalation and coordination with the supplier for resolution of the problem, if required.
- 8.1.8.6.4. The selected NSI should be able to analyze the problems identified in the network, perform a root cause analysis for the problem and they should troubleshoot network issues, locate network breaches, etc. among captured network packets. The successful bidder shall also analyze whether the application slowness is on account of abnormality of Network parameters (High Latency, Bandwidth utilization, CPU utilization of Network devices) and take necessary steps to resolve the slowness issue immediately.
- 8.1.8.6.5. The successful NSI should use network monitoring tool through which all the core network devices and branch network devices are integrated for monitoring purpose.
- 8.1.8.6.6. Responding to network complaints of application team and resolving them within given timeframe.
- 8.1.8.6.7. Provide a web-based dashboard to key personnel regarding health of important/critical links specified by the Bank. Alarms/alerts to be made on WAN link down status. Details to be provided through the portal shall be agreed mutually.
- 8.1.8.7. The NSI will also have the responsibility of maintaining all networking resources and equipment which includes but not limited to:
- 8.1.8.7.1. Maintaining updated records/documents of all the change request orders, network diagram, bandwidth details and hardware/port details.

- 8.1.8.7.2. Maintain up to date inventory of all WAN network hardware assets including information like locations, configuration details, serial number, asset code, warranty and AMC details. Bidder may, initially co-ordinate with the Bank to set up a base data.
- 8.1.8.7.3. Track installation of WAN equipment including routers, switches, modems and any other WAN equipment.
- 8.1.8.7.4. The NSI shall manage configuration of IP protocol on the Router & Switches and perform periodic password changes on the all network devices.
- 8.1.8.7.5. The NSI has to compile the inventory of IP addresses mapped to the Serial Number of the Router, Location and the Branch/Office.
- 8.1.8.7.6. The NSI will also be responsible of closing all Vulnerability Assessment, Audit finding in given timeframe.
- 8.1.8.7.7. The NSI should log calls with the respective supplier of the Networking Equipment for Hardware issues and co-ordinate with the members in the escalation matrix of the supplier.
- 8.1.8.7.8. The NSI is responsible for collecting information (bandwidth capacity, IP details, vendor, location etc.) about existing links in the Wide Area Network of the Bank and adding the information to Central Database.

8.1.9. Technical implementation and coordination committee

- 8.1.9.1. Bank will form a technical implementation and co-ordination committee comprising of Bank officials and a representative from the finally selected NSI's company. This committee is empowered to oversee the entire project implementation and maintenance for the contract period. The decisions taken by the committee will be final and binding on the finally selected NSI. During the first year of contract, the committee will meet once in a month to review the progress and to take necessary steps/decisions for performance improvement. Further, post completion of one year of contract period, the committee will be meeting on quarterly basis. The scope of the committee includes the following.
- 8.1.9.2. Taking decisions on network designs
- 8.1.9.3. Making necessary policies/ changes as part of change management
- 8.1.9.4. Examining the level of SLA compliance achieved and taking steps for improvement.
- 8.1.9.5. Attending to dispute resolution
- 8.1.9.6. Suggesting extra reports based on SLA requirement
- 8.1.9.7. Review the prices every year to determine the downward revision, if any due to reduction in taxes, duties, levies etc.
- 8.1.9.8. Alternative mode of connectivity for critical branches/offices
- 8.1.9.9. Transition process planning
- 8.1.9.10. Matrix for Health monitoring of the network

8.1.10. Maintenance of Third-party links

The Bank has engaged various companies like Diebold, FSS, FIS, NPCI, RBI, IDRBT, SWIFT, etc. for providing various delivery channel services like ATMs, Credit Cards, SWIFT, etc. For this purpose, network links have been established connecting Bank's Data Center to various third-party offices with network links. The selected NSI is

required to maintain these links and deploy suitable network equipments as per Bank requirement.

8.1.11. Supporting network at field level

- 8.1.11.1. The Successful Bidder shall provide technical expertise at the site to resolve any type of network problem e.g. Service Provider's exchange/ POP problem, local lead problem, power problem etc. for smooth operation of the bank applications.
- 8.1.11.2. Support should be available during business hours on all working days and during odd hours and holidays on exigency basis for all sites. At DC, DR support shall be provided on (24X7) on all days including holidays.
- 8.1.11.3. In the event of any problem at any location the support shall be made available immediately irrespective of the locations working on Wired/Wireless connectivity including the links from any service providers.
- 8.1.11.4. To resolve the problem successful bidder shall liaise with all concerned service providers and extend technical and other support to resolve the issue.
- 8.1.11.5. The successful NSI shall be responsible for escalating the unresolved problems by field engineers to his higher authorities and get it rectified within stipulated time period and ensure uptime as defined in this bid document (Successful bidder is to provide the call escalation matrix to every location).
- 8.1.11.6. The successful NSI shall arrange manpower as specified at Resource Deployment Plan of the document at various locations for day-to-day smooth functioning of network.
- 8.1.11.7. If a branch is getting decommissioned, the selected bidder will be responsible for coordinating with the service provider for link termination, handing over the requisite equipment's to bank officials with detailed report.

8.1.12. Managing & Supporting Network at Regional level

- 8.1.12.1. One qualified network engineer to be stationed at Regional Offices across India (List enclosed in [Annexure V](#)) having working experience of 1 year or more in similar network. In case bank opens any new Regional office, skilled engineer needs to be stationed at those places as per itemized agreed cost.
- 8.1.12.2. These engineers are required to resolve problems in the network/link problems of the branches coming under the Regional offices and to co-ordinate with their field engineers to resolve the network and for day-to-day smooth operation. The engineers shall function as help desk functionary and shall be the single point contact for all the issues pertain to network. The engineers to resolve the problems pertain to network equipment deployed across the network falling under Region. The engineers are to coordinate with NOC helpdesk and get the configuration etc. issues pertain to new / existing network equipment.
- 8.1.12.3. Handle all the down call alerts of the branches coming under the Regional offices, in liaison with bidder's NOC team, raised in the NMS tool and shall log tickets with respective service providers of NW devices, WAN links (MPLS, LL, VSAT etc) and follow-up with the service provider till successful resolution of the reported issue.

- 8.1.12.4. The engineers are also required to coordinate with local ISP exchange to resolve issues pertaining to their link.
- 8.1.12.5. The engineers are also required to provide field support and resolve the issues of the network /link problems to maintain the uptime of the branches.
- 8.1.12.6. The engineers are required to submit the report on day-to-day basis on the status of the links of the branches to the RCC/ZCC in charge.
- 8.1.12.7. Liaise with bidder's NOC - L1 team, L2 Team and L3 team and with all link service providers and all network device service providers for commissioning, shifting, upgradation and surrendering of links (any service provider) of the branches coming under the regional offices attached to the zonal office.
- 8.1.12.8. Obtain feasibility report for BSNL/MTNL and other links service providers for bank locations as and when required in liaison with bidder's regional offices and respective local service provider's team.
- 8.1.12.9. Report on daily link down incidents in NMS/ITSM tool at on daily basis as per format agreed by Bank to the respective zonal offices along with details of steps taken for resolution of the same.

8.1.13. Managing & Supporting Network at Data Centre, Powai and DR Site-Bangalore

- 8.1.13.1. The onsite engineers deployed at DC and DR needs take care of management, monitoring, troubleshooting & Integration of all (existing and new) network devices, WAN links (any type), internet links and also the LAN connectivity on 24 X 7 basis. The bidder should depute necessary resources to ensure that 24X7 on-site support is provided at Data Centre and DRS locations.
- 8.1.13.2. DC-DR onsite engineers will be in charge on the network aspect for any DR drills conducted by the Bank in coordination with Bank's CBS/ application team as and when required even on Bank holidays without any condition or any additional cost to Bank.
- 8.1.13.3. Whenever any issue observed at DC and DR the onsite engineer should inform, escalate and coordinate with appropriate Vendor/Service provider for resolution within the defined time frame as per project scope/ SLA.
- 8.1.13.4. Daily Networks Health checkups of all Network Equipment at Data Centre, DR should be taken regularly. The checkups should include status on Interface errors, reliability, equipment uptime, CPU/memory/Bandwidth utilization, Port Status, Logs, Power/Modules/other hardware components status etc and report the same to Bank.
- 8.1.13.5. The onsite engineers should provide services for any troubleshooting activities of the datacenter network issues along with the NOC team.
- 8.1.13.6. Coordinate with all the network service providers (BSNL, Airtel, TATA, Vodafone Idea, Sify, Reliance etc) for maintaining the uptime of all the links at datacenter and DR location.
- 8.1.13.7. In addition to this, The NSI should nominate a Program/Implementation Manager immediately on acceptance of the order, who shall be the single point of contact for the implementation project at Mumbai. The Program/Implementation manager nominated by the NSI should have prior experience in implementing similar-sized WAN with types of connectivity proposed by the Bank. Similarly, the NSI should nominate a representative at other locations who will be the contact person for that location.

- 8.1.13.8. The project manager shall be responsible for all the network related activities in the Wide Area Network of the Bank. Some of the key responsibility areas are:
- 8.1.13.8.1. Liaise with bidder's NOC - L1 team, L2 Team and L3 team, engineers at Regional Offices, with all link service providers (BSNL, Airtel, TATA, MTNL, Vodafone Idea etc) and all network device service providers for commissioning, shifting, upgradation and surrendering of links (any service provider) and for configuration, management and maintenance of network devices across all locations of the Bank respectively.
 - 8.1.13.8.2. Have access to the dashboard/ tools and need to fetch necessary MIS reports whenever required.
 - 8.1.13.8.3. Coordinate with the engineers stationed at zonal/regional offices and other locations for any escalation calls.
 - 8.1.13.8.4. Be in charge on the network aspect for any drills conducted by Bank in coordination with DC-DR Network team.
 - 8.1.13.8.5. Obtain feasibility report for MPLS/ILL/Leased Line links for bank locations as and when required in liaison with bidder's regional offices and respective local ISP team and coordination.
 - 8.1.13.8.6. Liaising for early commissioning / shifting / surrendering/ upgradation/ conversion of links.
 - 8.1.13.8.7. Liaising for cable laying and port/channel allocation, internal cabling inside the Bank's premises up to the network equipment.
 - 8.1.13.8.8. keep record of all the fault tickets logged with various service providers related to NW devices, WAN links (LL, MPLS, VSAT etc.) based on NMS tool, also based on bidder's regional help desk team reported issues and report the same to Bank whenever required. This activity is in the basic scope of NOC team however the on-site engineer shall liaison with bidder's NOC team for same.
 - 8.1.13.8.9. Report on daily link down incidents as per format defined in Bank along with details of steps taken for resolution of the same. This activity is in the basic scope of NOC team however the on-site engineer shall liaison with bidder's NOC team for same.

8.1.14. Managing & Supporting Network at NDC, Mumbai

Network Engineer placed at NDC, Mumbai shall:

- 8.1.14.1. Liaise with bidders NOC - L1 team, L2 Team and L3 team and with all link service providers and all network device service providers pertaining to NDC network for commissioning, shifting, upgradation and surrendering of links and for configuration, management and maintenance of network devices respectively.
- 8.1.14.2. Manage, integrate and troubleshoot the existing as well as future LAN infrastructure at NDC (Including nearby offices i.e. Ernest House and World Trade Center office) including routers, core switches, manageable switches, unmanageable switches and any other network equipment.
- 8.1.14.3. Selected NSI should provide services for any trouble shooting activities of the NDC network issues along with the NOC team.

8.1.15. Logging of critical devices

- 8.1.15.1. The NSI have to maintain the system logs of critical network devices installed at DC, NDC, DRC and critical locations for a period of 5 years. The logs should online/onsite for three months thereafter logs can be stored on tapes and submitted to Bank.
- 8.1.15.2. The NSI have to maintain the log of SD-WAN solution and AAA server for 5 years. Logs should be online for 3 months thereafter logs can be stored on tapes and submitted to Bank.
- 8.1.15.3. The periodicity for the retention of the log will be reviewed by the Bank on yearly basis and same has to be implemented by NSI.
- 8.1.15.4. NSI will design and implement all simple scripts that may be needed to analyze logs and produce reports as needed by Technical and co-ordination committee.

8.1.16. Operations

- 8.1.16.1. Based on the requirement successful bidder has to integrate any new network to the Banks existing network smoothly, which may be obtained from existing bandwidth provider or any new bandwidth provider as per the decision of the bank. Successful bidders may advice bank in the selection of media.
- 8.1.16.2. Successful NSI should install & configure network equipment for integration of new application, additional network etc., should support for smooth operation of its entire network, or any other location desired by the bank, conduct user training at the location specified by the bank and provide consultation, management and monitoring for other network related problems of any applications.
- 8.1.16.3. Successful NSI should conduct BIA (Business Impact Analysis) of the bank's network & security architecture and prepare Disaster Recovery plan (for network including links, equipment) including step-by-step procedure of the network recovery, time taken for each operation and dependencies.
- 8.1.16.4. The NSI shall be assisting the Bank with respect to the network design for new requirements/ revamping the existing architecture as per the best practices and implementing the same. The Network Specialist/Network Engineer to be available onsite during such deployments as and when required by the Bank.
- 8.1.16.5. The successful NSI is responsible to ensure that the NOC solutions and operations (including DR NOC) comply with the Bank's information security policies and industry leading standards (such as mentioned elsewhere in this Tender) and applicable laws and regulations.
- 8.1.16.6. The successful NSI should do necessary configuration changes in the network devices to mitigate the vulnerabilities of the devices. The bidder shall provide support to the Bank/security team in doing the vulnerability assessment of the devices on a regular basis.
- 8.1.16.7. In addition, the NSI is responsible for impact assessment and modification of NOC operations at no extra cost, on account of any changes to applicable information security policies/ procedures / standards/ regulations
- 8.1.16.8. As per industry practices, selected NSI should submit and regularly update following indicative list of documents for all in-scope solutions and operation activities:

- 8.1.16.8.1. High Level Design Document (HLD)
- 8.1.16.8.2. Low Level Design Document (LLD)
- 8.1.16.8.3. Standard Operating Procedure (SOP) for all operation activities
- 8.1.16.8.4. Network Diagram for DC, DR, NDC and other application as per requirement of Bank
- 8.1.16.8.5. Admin Guide for various in-scope solutions
- 8.1.16.8.6. Any other document as required by Bank

8.1.17. Continual Improvement

- 8.1.17.1. The selected NSI is required to make necessary modifications and improve the network monitoring, device configurations, traffic management, load balancing, bandwidth utilization, etc. in cost effective manner.
- 8.1.17.2. All activities related to modifications shall be planned well in advance and necessary permissions shall be taken from the team to perform such activities, through Change Management process.
- 8.1.17.3. This modification should be on a regular basis and the successful bidder will be held responsible if any issue occurs during any modification activities. It is expected from the successful bidder to co-ordinate with the bank team to improve processes related to network management. The selected bidder will have to improve this internal process if required to improve the network performance.
- 8.1.17.4. NSI shall work towards improving the policies configured on an on-going basis to reduce the occurrence of false positives & false negatives.
- 8.1.17.5. Periodic audits should be carried out on-site, by the OEM every year to ensure the quality of implementation and operations. On need basis health checkup exercise shall also be conducted.
- 8.1.17.6. Bidder shall curtail the closure time for incidents and events, also ensure the periodic check-up reviews for the same.

8.1.18. Providing Reports/MIS related to network

- 8.1.18.1. The vendor should provide Bank, the details of portal for calls logging which should be comprised of Auto Call Logging feature.
- 8.1.18.2. NSI will provide access to IT Service Management tool to Bank for Incident/Problem Management, Network Inventory Management (Links as well as equipments), Reporting and Dashboard.
- 8.1.18.3. Following are some of the reports that are to be submitted to Bank:
 - 8.1.18.3.1. Daily, Weekly
 - Daily/Weekly Incident Report
 - Isolated branches
 - Affected branches
 - Threshold violation report
 - 8.1.18.3.2. Monthly
 - Link wise availability report

- Link-wise Bandwidth Utilization report with suggestions for bandwidth upgrade/ downgrade based on the report.
- WAN Progress report to be provided for primary and secondary links Region wise, zone wise, link wise, new links added, links surrendered etc.
- Service Provider wise availability report
- Branch isolation reports
- SD WAN operating reports from respective SD WAN manager
- Change reports and change compliance
- Incident response and resolution SLA reporting
- Link commissioning/de-commissioning, upgrade/de-grade report& SLA reporting

8.1.18.3.3. Quarterly

- All monthly reports with trend analysis
- Quarterly SLA report
- WAN equipment/Network Assets inventory Report including Model, OS Version, DRAM, Flash RAM and Interface card details with other hardware available in the equipment.
- Link inventory including location, ISP. Bandwidth, Link Carried Medium, Peak utilization, Average utilization, etc.
- Review application rankings & policies in SD WAN orchestrator

8.1.18.3.4. Any other reports on network status/monitoring etc. as required by Bank in due course.

8.1.19. Problem Management

8.1.19.1. The bidder has to open problem tickets for at least following type of incidents impacting the Bank, perform Root Cause Analysis (RCA) and implement the resolution as per agreed change management process.

8.1.19.1.1. Identify incidents in DC which have caused an impact on the Bank's operations.

8.1.19.1.2. Identify branches that were isolated for more than 5 times in a month.

8.1.19.1.3. Identify individual links that were impacted more than 7 times in a month.

8.1.20. Dashboards

8.1.20.1. As part of Deliverables, bidder must provide integrated dashboard covering all appliances for viewing real-time incidents / events, alerts, status of actions taken etc. The dashboard should be an easy-to-use Web User Interface with search function, create reports, as well as access cases and applications, with just a few clicks. The vendor should implement an integrated online dashboard for services provided to the Bank.

8.1.20.2. The dashboard should be web based online portal available over desktop, Mobile, Tablet and iPad. This should have the automated facility of sending e-mails and SMSs. This tool should be accessible on Laptop and Mobile devices through VPN.

8.1.20.3. The NSI shall provide different dashboard and screens for different roles, provide online secured portal (web-based dashboard) for viewing real-time incidents / events, alerts, status of actions taken etc.

8.1.20.3.1. Top Management (Company View).

- 8.1.20.3.2. Network In-charge (complete and detailed dashboard of Network posture of the organization set-up being monitored through this NOC).
- 8.1.20.3.3. Network Administrator (for devices / equipment for which he/she is administrator).
- 8.1.20.3.4. Auditor (Internal Auditors, IT Auditor, ISO Certification Auditor or any other authorized official of the organization).

8.2. Scope of Work for Network Devices

- 8.2.1. Bidder/NSI should deploy & manage below mentioned Network tools in Bank's premises as part of managed network infrastructure to Bank. NSI shall perform the following tasks as part of deployment:

Phase		Activities	Deliverables
Phase I	Planning	<ul style="list-style-type: none"> • Conduct Kick-off meeting • Identify project point(s) of contact • Identify Bank resources required to assist in deployment, policy walkthrough, testing, and installation. • Identify business requirements • Identify technical requirements • Project Planning • Plan the schedule 	Project Plan and Gap Analysis
Phase II	Design	<ul style="list-style-type: none"> • Develop and/or review and validate solution design/architecture documents which will include: <ul style="list-style-type: none"> ✓ Solution overview and conceptual design ✓ Detailed design and connectivity parameters • Create a User Acceptance Test Document • OEMs of disparate solutions should be involved in this phase. Specifically, all the OEMs should certify and endorse the final design document. 	<ul style="list-style-type: none"> • Design & Architecture Document • Prerequisite Document • User Acceptance Test Plan
Phase III	Installation and Configuration	<ul style="list-style-type: none"> • Deploy solutions • Complete initial configuration • Completed Integration with required ITSM tool • Documentation of installation and configuration • OEMs should be involved and certify the correct configuration of their equipment 	<ul style="list-style-type: none"> • Successful deployment solution • Installation and Configuration Document • Gap Assessment

Phase IV	Optimize	<ul style="list-style-type: none"> • Fine-tuning of solution • Monitor and resolve issues • Provide an information knowledge-transfer workshop 	<ul style="list-style-type: none"> • Tuning policies. • Policies override SOP • Transfer of Information session
Phase V	Deployment Validation	<ul style="list-style-type: none"> • This phase will comprise of deployment validation to be conducted by OEMs. 	<ul style="list-style-type: none"> • Validation Report by OEM
Phase VI	Monitoring, Management & Sustenance	<ul style="list-style-type: none"> • Post- deployment (after sign-off) bidder will manage & monitor proposed solution • Facilitation & operation for all change management, upgradation, updates, etc during contract period. • OEMs should perform an annual audit of the system certify proper configuration and performance. 	<ul style="list-style-type: none"> • Reports and Dashboards as per defined SLAs • Go Live Operations

8.2.2. Software Defined- Wide Area Network (SD-WAN)

- 8.2.2.1. Bank intends to implement managed SDWAN Technology/Solution services with SDWAN Network devices for Bank branches/offices across PAN India. The solution should have operational simplicity and ease, application aware networking, robust and secure infrastructure and reduce TCO (Total Cost of Ownership) of WAN Infrastructure.
- 8.2.2.2. The proposed SD-WAN solution should be able to create dynamic VPN Tunnels in between Edge devices and the DC and DR so that the various applications of Bank can use the channel to offer services to the beneficiaries of Bank and also for the day to day office tasks.
- 8.2.2.3. The Service provider will have to supply, Install, test and commission, manage and monitor the SDWAN network devices at approximately 4500 initial locations at Bank branches across country with network devices as per the delivery schedule mentioned in this RFP document.
- 8.2.2.4. The number of locations may increase over the time. The solution/technology services will be required to be further extended to increased number of Bank offices across country with the same rates and terms and conditions in phased manner.
- 8.2.2.5. In all the office locations of Bank, SDWAN vendor has to provide SDWAN devices to provide a secure, stable, redundant connectivity over the multiple shared or dedicated internet, MPLS and/or other links/connectivity.
- 8.2.2.6. The bidder will have to provide managed end-to-end SDWAN services to Bank as a part of deliverables at Bank branch/offices across India. The charges should be inclusive of monitoring, troubleshooting and maintaining them.
- 8.2.2.7. At all the Bank Branches/offices, Bank has provided any combination of two or more Internet/MPLS/3G/4G/VSAT/Wi-MAX connections from different service providers. The

SDWAN device and switches provided at Bank offices should have the capacity to handle the data traffic while enabling the entire required feature including but not limited to VPN, Firewall and IPS.

8.2.2.8. It is to be noted that there should be one single centralized management console for SD-WAN solution irrespective of number of controllers, orchestrator, analytics, or any other Head end devices installed to match Bank's scalability requirement. Further in case NSI is proposing 3rd party product such as Firewall, IPS as part of SD-WAN offering, same should be able to manage using same centralized console with offering all required features including but not limited to Zero Touch Provisioning, Centralized updates, Patch and configuration management.

8.2.2.9. In case bank opt to implement Full Mash/partial mash topology, all the communication between branches should be through encrypted IPSec Tunnels. It is also to be noted that all such tunnel should be formed dynamically without any kind manual intervention/configuration.

8.2.3. Networking Switches

In order to provide LAN side connectivity to all branches/offices, Bank intends to implement Network Switches at all its offices/branches. Detailed Sizing and other technical specifications of required switches are mentioned in this document. It is to be noted that all these network switches should have centralized management and monitoring. Bidder is also responsible for provide required infrastructure and tool/application to manages all switches centrally from DC and DR Site. The centralized management and monitoring of switches include but not limited to following:

- Asset Management
- Configuration Management
- OS and Patch Management
- Compliance Management
- Health Monitoring
- Backup Management

8.2.4. Networking Routers

In order to have flexibility of connecting with traditional WAN network at DC, DR, Bank intends to implement traditional L3 Network routers at centralized locations i.e. DC, NDC and DR site. Detailed technical specifications are mentioned in Annexure - E.

8.2.5. Unified Communications - IP Telephony

Bank seeks to implement hosted IP Telephony system. This system will replace the current, locally installed, IPT system and must be capable of meeting Bank's future needs. It is the intent of this Request for Proposal that the NSI shall provide a complete solution for all aspects the project. The vendor shall provide all design, planning, system architecture, installation, network analysis, training and post installation support for the project. As part of scope, Bidder is expected to provide required infrastructure, application to host VOIP at central location at DC and DR. Bidder shall also responsible for providing both video and Non-Video (Colored) IP Phone across India as per requirement of Bank. In addition to this, Bank also intends to have soft Phone clients for

certain endpoints. Exact count and specification are mention in detail later in this RFP. The project requires the design, implementation, and support of a hosted VOIP telephone system. Bank seeks a solution that includes Unified Messaging and integrates with existing network infrastructure. All existing telephones should be replaced with proposed IP phones that provide the required features. The NSI will be expected to work directly with Bank to ensure compatibility, call quality, and reliability.

8.2.6. Network Performance Monitoring (NPM)

- 8.2.6.1. Bank is planning to implement network performance management solution in order to monitor and ensure optimal performance levels of a Bank's network. Solution should provide the visibility and insights to accelerate, transform, and innovate networks and services for a flawless, agile, and cost-effective application delivery.
- 8.2.6.2. Network performance management needs to collect and provide performance metrics from across the network at a granular level. To keep up with this rapid pace of growth and innovation at Bank, IT Ops teams need a holistic approach to real-time application management based on end-to-end visibility across all service delivery interdependencies - whether physical or virtual, on-premises and off-premises, private and public clouds.
- 8.2.6.3. Network performance monitoring solution should help in identifying performance bottlenecks, whereas network performance management should ensure that problems are mitigated, and the network is restored back to the required performance level. The Solution should deliver valuable macro-level insights into the status and performance of enterprise-wide services, application components, individual hosts or groups of clients or servers. This expands the IT architect's understanding of service consumption patterns, application component dependencies, and overall user experience to better support resource optimization and capacity planning. In addition to internal metrics, network performance management should also be able to analyze, maintain and manage performance from end user perspective.
- 8.2.6.4. The NSI is responsible for Supply, Installation, Integration, Maintenance & Operation of the offered NPM System.
- 8.2.6.5. The NSI shall be responsible to document reports that need to be generated for fault, performance and analysis of the network performance as per the bank's requirement.
- 8.2.6.6. The NSI shall be responsible to supply necessary documents such as Installation Guide, Administration Guide, Manuals and Data Sheet etc.
- 8.2.6.7. The offered Network Performance Management solution should support at least the following. The detailed technical specifications are mentioned in this RFP document. All the proposed Components for NPM should be from single vendor. Solution should have following:
 - 8.2.6.7.1. Solutions should have capability for network and application visibility, monitoring, analytics, reporting, and troubleshooting. Should be scalable based on wire data increases the integrity, fidelity, and quality of analysis.
 - 8.2.6.7.2. Provides insight into the performance of all infrastructure and application components involved in service delivery.
 - 8.2.6.7.3. Supports Unified Communications & Collaboration service features including call setup / teardown and call quality analysis.

- 8.2.6.7.4. Dashboard, Service and Traffic Monitors with contextual Session Analysis and Packet Analysis drill downs.
- 8.2.6.7.5. Real-time proactive alerting notifies of problems before they become service impacting, user affecting events. Customizable reporting module provides day- to-day business and operational reports which can be scheduled for daily, weekly and monthly delivery.
- 8.2.6.7.6. Scalable, enterprise-class architecture supports large scale geographically distributed deployments in physical, virtualized, hybrid, or cloud-based environments with single pane of glass.
- 8.2.6.7.7. The offered NPM solution should be scalable, secure, robust, advanced, state of art, flexible, easy to deploy, reliable, built in redundancy and should support distributed architecture along with 3rd party integrations.

8.2.7. Modems

Since Bank has most of its primary MPLS link from BSNL which is on traditional mode connectivity i.e. G.703/V.35. In order to manage links through SD-WAN, Bank intends to convert all such traditional connectivity into Ethernet by deploying appropriate modem. Detailed technical specifications for all required modem and converter devices are mentioned in [Annexure-E](#).

Selected NSI shall be responsible for assessing each site and provide required/suitable modem accordingly.

In order to protect investment, Bidder will do the feasibility study of all available BSNL and MTNL link and wherever feasible, must provide Ethernet modem so that same modem can be used for up-gradation of link above 2 Mbps.

8.2.8. Racks

In order to host network equipments including Routers, switches, modems, etc in branch locations, NSI will be responsible for supplying, implementing, mounting 9U Network racks at all branch/office locations. All the rack should have inbuilt surge protector to ensure adequate surge/spike protection for implemented devices. Required specifications are mentioned in Annexure-E.

8.2.9. DNS, DHCP & IP Address Management Solution (DDI Solution)

Bank intends to have DNS, DHCP & IP Address Solution (DDI) to scale IT infrastructure with clear visibility. Currently Bank's Internal DNS are running on multiple DNS server. Further IP addresses are being managed through Excel sheet. Bank has hosted DHCP on Branch end routers and thus all three DDI stack is today running non-integrated environment which pose challenge in operations & scale. Bank intend to have all three components (DNS, DHCP & IP Address Management) to be deployed and centrally for ease of operation.

Proposed DDI Solution can run all modules together on single appliance or can propose multiple appliances (which complement each other) based on proposed architecture to support defined scale. DDI Solution needs to be deployed at DC & DR as built in redundancy. Each site should be capable of handling 100% load while either site failure.

8.2.10. Backup solution

Bidder is required to take backup of all solutions and device configurations provided under this tender as per the bank backup policy (daily, weekly, monthly). Bidder needs to provide the backup solution comprising of hardware, software and tape library required for taking the backup of the various solutions. Bank will only provide the required no. of tapes for taking the backup. Bidder also needs to restore the data from tape on quarterly basis.

8.3. Scope of Work for OEM

- 8.3.1. The OEM/OEMs should be committed to the success of the project during actual implementation by being involved in implementation of the project till its completion as per phases given in clause 8.2.1 of the RFP. The OEMs should be involved in throughout all phases during implementing proposed solution by the bidder as per the scope of work defined in RFP.
- 8.3.2. NSI shall ensure that the product OEM is involved in the implementation of the project till its completion. The OEMs through their on-site professional services will ensure that their products are being implemented as per industry best practices. OEMs have to give the certificate to the Bank post implementation, confirming the implementation of their products with best industry practices and the standards. Bidder should have back-to-back support with OEM during the total contract period for necessary support. Bidder would submit a letter by OEM issued to bidder in this regard.
- 8.3.3. In addition to this, if in any case, bidder fails to implement/successfully implement the solution, the OEM has to take complete ownership and implement the solution without any additional cost to the Bank.
- 8.3.4. A letter from the product OEM confirming the following has to be submitted in the technical bid.
 - 8.3.4.1. They will be involved in the implementation of the project till its completion as per scope given in the RFP as described in Table mentioned in Scope of Work for Network Devices.
 - 8.3.4.2. In case NSI fails to implement the solution, OEM will ensure implementation of the same without any additional cost to the Bank.
- 8.3.5. The OEMs also have to give the certificate to the Bank post implementation, confirming the implementation of their products with best industry practices and the standards and no zero-day threats or malware in the installed device or appliance.
- 8.3.6. A letter from bidder confirming the following has to be submitted as part of technical bid:
 - 8.3.6.1. The NSI should have necessary agreement with the OEM for all the required support during the implementation as well as for entire contract period.
 - 8.3.6.2. The NSI should have necessary agreement with the OEM for all the required support during the implementation as well as for entire contract period. Bidder shall furnish teaming agreement with OEM for the above scope of work and submit the same as part

of the bid. This teaming agreement should include but not limited to the ownership of the activities, timelines and resources associated to the activities.

8.3.7. The following are the expectations with respect to OEM involvement during the contract period, however the bank reserves the right to change the scope:

- 8.3.7.1. Review of Business Requirements Specification (BRS) document, taking into account all quantitative and qualitative aspects related to configuration of the solution from an industry leading practices perspective and in tune with regulatory guidelines.
- 8.3.7.2. Review of solution architecture to assess the extent to which the same will support business requirements and review gaps and provide customizations that may be needed.
- 8.3.7.3. Review of information requirements and supporting processes with respect to completeness and quality.
- 8.3.7.4. Review of functional configuration by duly benchmarking against defined scope and business requirements.
- 8.3.7.5. Review of test strategy, scenarios and test cases developed for supporting the configuration for conducting UAT of the solution configured.
- 8.3.7.6. Review of UAT environment, plans, mapping of test cases and functional requirement specification and tracking mechanism for resolution of issues.
- 8.3.7.7. Review transition plan and approach.
- 8.3.7.8. Sign off by Bidder and OEM for Go live of respective component.
- 8.3.7.9. For above scope of work, OEM shall produce following deliverables in the course of implementation:
 - BRS review report with recommendations for resolution of any gaps
 - Review Report on solution architecture and information requirements with recommendations for resolution of gaps
 - Report on functional configuration check done containing the observations on UAT test strategy, cases and scenarios, UAT plan, etc
- 8.3.7.10. The NSI should further provide the deliverables and sign off for each of the deliverables at various stages of migration, Upgradation, customization and implementation.
- 8.3.7.11. Further, the bidder should arrange for sign-off by OEM for each of the critical stages of migration, Upgradation, customization and implementation.
- 8.3.7.12. OEMs shall provide on-site resources support through their professional services at each central location for their respective solutions during the implementation phase for:
 - Validation of solution design and architecture
 - Continuous monitoring of implementation at each location.
 - Provide SME support to working teams.
 - Ensure customization is in line with bank's requirements.
 - OEM sign off would be necessary after implementation of its products.
 - Yearly audit of the solutions implemented by the OEM.

8.4. Additional Scope of Work

8.4.1. Implementation & Integration

- 8.4.1.1. NSI will be responsible for designing and implementation of the specified solutions and necessary hardware required by Bank and as per the scope and technical specification of the solutions which are detailed in Annexure-E.

- 8.4.1.2. The NSI is responsible to ensure that the all solutions and operations comply with bank's information security policies and industry leading standards (such as ISO 27001, ISO 22301, PCIDSS, etc.) and any applicable laws and regulations.
- 8.4.1.3. In addition, the bidder is responsible for impact assessment and modification of NOC operations at no extra cost, on account of any changes to applicable information security policies/ procedures / standards/ regulations.
- 8.4.1.4. The support for all the solutions proposed should be provided for minimum 5 years post go live of all components in the solution.
- 8.4.1.5. In case end of life/end of support for any proposed solution including software, hardware, license and appliance is declared by OEM within contract period, Bidder shall provide upgraded version of the products without any additional cost to the Bank.
- 8.4.1.6. Bidder/ System integrator is responsible for developing and implementing the security configuration hardening of all the devices and software that are procured for WAN Expansion and Network Operation Center. Also, they have to periodically review the guidelines and configure as and when required.
- 8.4.1.7. Develop Escalation Matrix in order to handle Incidents efficiently.
- 8.4.1.8. Provide necessary documentation for the operation, integration, customization, and training of each of the solutions in scope.

8.4.2. Reporting

The bidder should provide periodic reports to the Bank as per the following requirements:

- Daily Reports: Critical reports should be submitted per day.
- Weekly Reports: Any particular day of week as decided by Bank
- Monthly Reports: 1st week of each month.
- Quarterly Reports: 1st Week of each quarter
- In addition to this Bank may ask for any custom report at any given point of time.

Selected bidder is expected to detail every report which it will provide to the Bank related to the services and activities performed.

Any delay in reporting will attract penalties as mentioned in SLA.

8.4.3. System Integration Testing (SIT) and User Acceptance Testing (UAT)

- 8.4.3.1. There will be a User Acceptance Test by the Bank for the tools deployed and NOC operations wherever applicable.
- 8.4.3.2. The Bank shall commence the User Acceptance Testing as and when each products and services are made ready by the Bidder and a formal confirmation that the system is ready for UAT is submitted to the bank. The results thereafter will be jointly analyzed by all concerned parties including OEMs.
- 8.4.3.3. UAT will cover acceptance testing of all the product/services, integration with NOC tools and dashboard (primarily ITSM) and integration of NOC with all targeted devices and systems.
- 8.4.3.4. Complete acceptance has to adhere to the stipulated time lines.
- 8.4.3.5. The solution will not be accepted as complete if any facility /service as required is not available or not up to the standards projected by the Bidder in their response and the requirement of this RFP.

- 8.4.3.6. The Bank will accept the solution on satisfactory completion of the above inspection. The contract tenure for the Solution will commence after acceptance of the solution by the Bank.
- 8.4.3.7. In case of discrepancy in facilities and services provided, the Bank reserves the right to cancel the entire contract.

8.5. Benchmarking

The bidder will demonstrate the benchmarking tests to confirm compliance with the stated performance parameters.

8.6. Workflow Automation

Selected Bidder will define the work flow automation so that applications are integrated and manual intervention is minimal.

8.7. Monitoring

It is expected that monitoring shall be carried out from Network Operation Center (NOC) hosted as premises of NSI. The NSI shall be responsible for providing adequate resource count for the operations of the NOC. In addition to having shared pool of resources at NOC, NSI shall also be providing dedicated SPOC (Single Point of Contact) and escalation matrix at NOC. The NSI is expected to monitor NOC related activities and events for Bank's network infrastructure on 24x7x365 basis and suggest/ take appropriate action on an on-going basis.

8.8. Amalgamation

- 8.8.1. Bank is in process of being amalgamated with Corporation Bank and Andhra Bank. Bank is in the process of finalizing IT Consultant for merging of various products and projects and Successful bidder has to work with the IT Consultant identified by Bank in the amalgamation process. Accordingly, post-merger, existing branches of those Bank shall be added into Bank's network. The migration of these branches in Bank's network shall be carried out in planned and phased manner. The NSI shall be responsible to design new network architecture including but not limited to designing new IP Schema, connectivity diagram, High level and low-level design, plan network routing. Post-merger, The NSI shall also be responsible integrating existing network infrastructure of the amalgamated entity as per discretion of Bank.
- 8.8.2. It is to be noted that post-merger these banks will integrate with their traditional switch and router which might not be SD-WAN ready. Keeping the same in mind, NSI has to propose SD-WAN architecture in a way that Non-SD-WAN branches (branches having tradition router) can also connect to Bank's central location in secure manner (secure IPSec tunnel or equivalent). It is also to be noted that post-merger, Bank will have network equipment from different make/model from different OEMs. So NSI has to make sure that solution such as Centralized network switch management, DDI, NPM are vendor agnostic and does not have dependency over any particular OEM, Make, Model.
- 8.8.3. It is expected that Bank shall have approximately 10,000+ branch/offices across India after completion of merger. In order to serve all these locations, NSI has to make sure that all deployment should be scalable to accommodate Bank's future requirement, if any.

- 8.8.4. It is also to be noted that Bank shall have right to place additional order (partial and full) for any in-scope solution for any location in India during the contract period at the same rate discovered through this RFP. Bank shall also have the right to add any number of additional links for monitoring and management through NSI Network Operation Center (NOC). Bank shall also have the right to ask for additional facility management resources at any new and/or existing location as per itemized agreed cost.
- 8.8.5. Post-merger, the NSI have to replace the Bank's acquired network equipments before the expiring of contract date of existing vendor to avoid any downtime. Payment will begin after the expiry of present contract.
- 8.8.6. During and post-merger/integration NSI has to co-ordinate with NSIs of merging Bank for successful integration and running of network operation.

8.9. Solution Acceptance

The Bank/appointed consultant in coordination with the bidder shall conduct an Acceptance test wherein the bidder has to demonstrate the implementation of the solution as per the requirement of the bank. The bidder shall have to submit detailed reports of the test outcomes to the bank.

8.10. SLA Compliance

The bidder shall ensure compliance with SLAs as defined in the RFP.

8.11. Business Continuity

The NSI is responsible for defining a DR/ BCP plan for the NOC operations and also to ensure that periodic tests are conducted as per the testing calendar agreed with the bank.

8.12. Team Composition

The WAN operations team shall be divided into three teams. The first team shall include the dedicated team that includes the Program manager, Network specialist and Network engineers. This team shall be dedicated to the Bank's WAN & LAN operations. This team will be stationed on-site at Bank's Data Center, NDC & DR Site.

The second team shall include support engineers at stationed at each Regional Office locations. This team shall provide support for telecom (liaising with Basic service provider for procurement and maintenance of links) and network equipment in their respective regions.

The third team will be pooled resources at NSI's NOC Premises. They shall be responsible for 24X7X365 monitoring of Bank's WAN and LAN infrastructure, incident and ticket management. Apart from having pooled resource at its NOC premises, Bidder is required to assign Single point of contact (SPOC) dedicatedly working for Bank project at their premises.

The dedicated team proposed by the Bank for the period of five years is as follows:

Sr. No.	Description	No. of Resource
1	Project Manager (in Mumbai)	1
2	Network Specialist (in Mumbai) This will include: <ul style="list-style-type: none"> SD-WAN Specialist Proposed Network Switch and Router Specialist Specialist on Bank's existing LAN network infrastructure OEM solutions (Detailed in Annexure -S) All other in-scope solutions including Centralized network management, DDI, NPM, AAA server, Policy Management. 	6
3	Network Engineers at DC -in shifts - 12 Engineers two manage 24X7X365 operation DR Site Bengaluru - 2 Engineer to manage 08:00AM-08:00PM operations NDC - 2 Engineer 08:00AM-08:00PM operations	16
4	Network cum Telecom Member at Regional Offices - 1 Telecom Member in one shift of 8 hrs.	63
5	1 Qualified DDI Operation Resource at DC	1
6	1 Qualified Network Performance Monitoring Resource	1
7	Unified Communications Resource - 2 Engineer to manage 08:00AM-08:00PM operations	2
Grand Total		90

8.13. Roles & Responsibilities

Service Groups	Responsibility Areas	Deliverables
Project Manager	Overall responsibility for the entire project including - Network Implementation Network Monitoring & Maintenance Inventory Management Spares management SLA Management	<ul style="list-style-type: none"> Timely project execution Team management Overall monitoring and management of network Spare and logistics management SLA reporting Meeting scheduling with Telecom Service Provider Reviews
Network Specialist	Responsible for all the technical aspect of project implementation and running of the entire network. Network troubleshooting Network Changes - vetting Changes in existing routers IP Address and VLAN	<ul style="list-style-type: none"> Vetting any alteration to the network Centralized Management of In-Scope solution including but not limited to SD-WAN Controller, Switch manager, Existing Router & Switches configuration Assigning access level to Network / Telecom Member

	Maintenance	<ul style="list-style-type: none"> • IP address maintenance • Trouble shooting and debugging of problems, if any • Upgradation of existing routers • Changes in existing routers
Network Engineers	Day-to-day maintenance & Troubleshooting of all network equipments, links etc.	<ul style="list-style-type: none"> • Network equipment installation at the locations where Network Engineers are based • Manage Network equipment configuration • Network equipment access controls • Trouble shooting and debugging of problems, if any • Upgradation of Network equipment • Changes in Network equipment
Network Telecom Engineers cum	Liaison for new leased lines Liaison for new MPLS Liaison with Private Basic Service Providers Basic Network troubleshooting for Branches under Zone	<ul style="list-style-type: none"> • Commissioning of new leased lines / MPLS links • Day to day maintenance • Shifting and realigning of leased/MPLS circuits • Upgrading of leased/MPLS circuits • Surrendering of circuits, if any • Billing related liaison • Any other matter to be taken up with Basic Service Provider
DDI Operation Resource	Day to Day Maintenance and management related proposed DDI Solution	<ul style="list-style-type: none"> • Maintenance and Management of Hardware and Application infrastructure for DDI • Troubleshooting any issue related to DDI • Call logging with OEM for rectifying any issue
Network Performance Monitoring Resource	Day to Day Maintenance and management related to Proposed NPM Solution	<ul style="list-style-type: none"> • Maintenance and Management of Hardware and Application infrastructure for NPM • Troubleshooting any issue related to NPM • Call logging with OEM for rectifying any issue
Unified Communications Resource	Day to Day Maintenance and management related to Unified Communication IP Telephony	<ul style="list-style-type: none"> • Maintenance and Management of Hardware and Application infrastructure for UC • Troubleshooting any issue related to UC • Coordinate with local Network pool of ISP for delivery, installations, replacement of IP Phones • Call logging with OEM for rectifying any issue

8.14. Service Windows

Mutually agreed roaster for Engineer shifts will be designed post awarding the contract. However, it is to be noted that Onsite support at Data Center and offsite support from NSI NOC must be in 24X7X365 basis. In addition to this, in case of exigency of for any other requirement, Bank may call Project Manager, Network specialist, Help desk cum telecom engineer on holidays as well as on non-business hours.

8.15. Other terms and Conditions

- 8.15.1. Based on requirement, Bank may ask for additional facility management resources for any new/existing site as per cost discovered. Bank at its discretion also reserves right to reduce number of required resources for any/all locations. In such case payment will be made at actual.
- 8.15.2. Bank reserves the right to conduct interviews of the proposed On-site team members.
- 8.15.3. In case of exigencies or as and when Bank requires, Network Engineers and Network Specialist should be available on Sundays and Holidays as well.
- 8.15.4. In case of absence of any of the resource person, standby manpower may be provided by the vendor. If Bank is not satisfied with the performance of the standby personnel, Bank may not accept such standby manpower and in such cases, charges on actual basis of manpower support will be deducted from the vendor subject to adherence of SLA conditions. The above details are only indicative figures and may undergo change as per the requirement of the Bank from time to time.

8.16. Educational Qualification for Onsite Engineer

8.16.1. Project Manager

- Should be Graduate with minimum 7 years of experience in the field of Networking and managing in-scope solutions.
-
- Should have experience in Installation, Configuration, Administration and Troubleshooting of network and/or security equipment with minimum 2 large scale project leading experience with minimum of 100 active nodes.
- Should have relevant certification related to project implementation such as PMP.

8.16.2. Network Specialist

- Should be a graduate with minimum 5 years of experience in the field of Networking.
- Should have at least 1-year experience on proposed solution.
- Engineer should also have any valid certificate of expert level for in the field of networking
- It is to be noted that at least 2 of the deputed engineers must be certified (With hands-on experience) on proposed SD-WAN Solution.

8.16.3. Network Engineer

- Should be a graduate with minimum 3 years of experience in the field of Networking and managing in-scope solutions.
- The resource must also have a valid certification for CCNA and/or any other relevant Technical Certification in networking
- It is to be noted that at least 1 of the deputed engineers must be certified (With hands-on experience) on proposed Network Performance Monitoring Solution.
- It is to be noted that at least 1 of the deputed engineers must be certified (With hands-on experience) on proposed Network DDI Solution.

8.16.4. Network cum Telecom Engineers

- Should be a graduate with minimum 1 years of experience in the field of networking.
- Should have CCNA or any other relevant Technical Certification in networking

8.16.5. Unified Communications Resource

- Should be a graduate with minimum 2 years of experience in the field of Unified Communication IP Telephony.
- Should have at least one-year experience on propose solution.

8.16.6. DDI Operation Resource

- Should be a graduate with adequate admin level certificate on proposed DDI Solution.
- Should have at least one-year experience on propose solution.

8.16.7. Network Performance Monitoring Resource

- Should be a graduate with adequate admin level certificate on proposed NPM Solution.
- Should have at least one-year experience on propose solution.

Above mentioned Project Personnel must have undergone Know your Employee process thoroughly and bidder has to submit undertaking as per [Annexure-R](#). It will be bidder's responsibility to get the NDA signed by such resources and submit to the Bank.

8.17. Training

The selected bidder will be responsible for training the Bank's employees as and when required in the areas of implementation, operations, management, monitoring, error handling, system administration etc. The training will be given both pre-implementation and post-implementation for proposed solution.

Pre-Implementation: Training will be provided to the bank personnel team on the product architecture, functionality and the design for each solution under the scope of this RFP.

Post Implementation: Training will be provided to the bank personnel team on operations, monitoring, policy configuration for all in-scope solutions, routine operations, management, monitoring, etc.

In addition to this the NSI will also be responsible for providing minimum 3 days training on networking (Once in 2 year) to Bank official at 5 different Bank locations as communicated by Bank. The Bidder shall train the Bank's personnel for basics of networking, operation, policy management, Troubleshooting and familiarization of

features and functionalities, policy configuration, alert monitoring. The final agenda of training will be mutually agreed.

The bidder is required to provide all trainees with detailed training material for each solution as per the scope of work of the bank. This training material should cover installation, operation, integration, maintenance, troubleshooting and other necessary areas for each solution.

All out of pocket expenses related to training shall be borne by the selected bidder. The bidder may utilize the OEM resources in case the bidder does not have adequately experienced resources for providing training. It is to be noted that all expenses related to trainer (logistic or other) shall be borne by the bidder. Rest all requirement such as training room, printout, etc shall be taken care by the Bank.

The Bidder/OEM will be responsible to install the required (in any) applications/systems, training server at DC and also ensure connectivity to the training server, for the purpose of training at the training Centers. There will be no cost payable by the Bank for the application, database and operating system software installation at such training sites.

8.18. Hardware Quality Assurance

In case any equipment has a hardware failure during contract period for more than three occasions in a period of less than three months or six times in a period of less than twelve months, it shall be replaced by equivalent or higher-level new equipment by the Bidder at no additional cost to the Bank.

For any delay in making available the replacement and repaired equipment for inspection, delivery of equipment or for commissioning of the systems or for acceptance tests / checks on per site basis, Bank reserves the right to charge a penalty and the Bidder agrees that the rate of penalty would be as per section related to Service Level Agreement of this document.

8.19. Obligation of Bidder

During the contract period, selected NSI will ensure that all supplied hardware and Software are under adequate Maintenance & Support services. Bidder shall be responsible for the following:

- 8.19.1. The NSI shall render both on-site and off-site maintenance and support services to the Bank. The Bidder shall provide troubleshooting / customer support mechanism. The Software Maintenance and Support Services shall be provided by the Bidder from the Bank's premises.
- 8.19.2. NSI shall assign personnel of appropriate qualifications and experience to perform the services in order to fulfill its obligations.
- 8.19.3. NSI shall designate one of its personnel as the Project Manager, to interact with the Designated Customer Support Contact from the Bank for the purposes of getting approvals, progress report, discussing and resolving issues, arranging meetings, etc.
- 8.19.4. NSI shall exercise requisite control and supervision over its personnel in the course of rendering the services and make best efforts to ensure that the services are rendered in a continuous and uninterrupted manner.

- 8.19.5.1. Though NSI has the right to withdraw its personnel, Bidder will replace the persons with other personnel having appropriate experience and skills at no extra cost to the Bank.
- 8.19.5.2. In the event that any person engaged/deputed/deployed for rendering services, is, either-
- 8.19.5.2.1. No longer available by reason of resignation or termination or the like; or,
 - 8.19.5.2.2. Unable to render satisfactory services; or,
 - 8.19.5.2.3. Not acceptable to the Bank by reason of any misconduct or non-performance on the part of such person, then Bidder will use all reasonable endeavors to replace such individual(s) promptly by other sufficiently skilled, qualified, and experienced person(s) at no extra cost to the Bank. Bidder will in the discharge of its obligations use all reasonable endeavors to minimize changes in personnel.
- 8.19.5.3. NSI will respect the confidentiality of all information given to it by the Bank and will not divulge such information to any third party or other units without the consent of the Bank.
- 8.19.5.4. NSI should impart knowledge to the authorized employees of the Bank, additional technical and/or user training in respect of any corrected licensed software provided, if required by the Bank.
- 8.19.5.5. The NSI should promptly install/implement the corrected licensed software and/or maintenance releases provided at the Designated Location(s) of the Bank at no additional cost or fees or expenses.
- 8.19.5.6. The NSI should undertake regular preventive maintenance of the licensed software.
- 8.19.5.7. All bug fixations / modifications / enhancements relating to the licensed software shall be done by the Bidder in a time bound manner as per the SLA. The Bidder shall adopt a common, smooth, timely and effective and satisfactory bug/enhancement handling mechanism. The Bidder agrees that the errors resulting from the licensed software shall not be attributed to alleged misuse, improper use, alteration or damage by users. The Bidder shall compensate the Bank such financial loss suffered by the Bank if the Bidder fails to fix bugs, provide the modifications / enhancements / customization as required by the Bank as per the terms and conditions of this tender and to meet the services level agreements as will be entered into by the Bidder with the Bank.

8.20. Completeness of Project

The project will be deemed as completed only after project scope and requirements are met in full and the all in-scope solution meets all technical specifications and delivers all the functional requirements, as per the terms of RFP.

The project will be deemed incomplete when the mutually agreed acceptance and completion criteria are incomplete or not met or not fulfilled. The Bank reserves the sole right to accept or reject the acceptance of any product / service in the event the agreed acceptance and completion criteria are not met by the Bidder.

8.20.1. Project Review:

The progress in the project implementation will be closely monitored and reviewed periodically by the Bank.

8.20.2. Escalation Matrix

The bank as well as the NSI will decide an escalation matrix to resolve any issues that may crop up during implementation of the project. Both the bank and Bidder including the consortium members shall inform the names of the persons and their telephone numbers for the escalation matrix to be effective.

8.21. Buy Back of Old IP Telephony Server

Bank will place order with option of buyback of existing Unified Communication (UC) equipments including Server and IP Telephone “as is where is basis”. Bidder should produce the relevant document as proof for having collected old hardware/equipment and peripherals, against which only the payment will be released. The condition for buy back is “as is where is basis” and bidder has to collect it from respective locations. A line of confirmation should be submitted to this effect. The bidder should include the cost of buy back old VC equipments “as is where is basis” in TCO. It is the responsibility of bidder to collect old hardware and peripherals from respective offices of the bank on their own expenditure. Bank will not bear any dismantling/transportation charges or any other expenses incurred while collecting the old UC equipments. Existing Unified Communication equipments including Server and IP Phones are approximately 10 years old. Details of buyback UC equipments are mentioned in Indicative Bill of Material in [Annexure F\(A\)](#).

8.22. General Scope for Onsite Resources

- 8.22.1. L1 Bidder should deploy one onsite resource during the contract period with adequate skill set and experience for monitoring and management of the proposed solution during office hours. However, in case of need or emergent situation it must be extended on Sundays/Holidays also. The deputed resources should manage and maintain networking/software as per the agreement. Bank reserves the right to claim change in resource based on the performance of the resources.
- 8.22.2. The technical resources should be competent to handle/ Integrate/ Implement/ Test/manage with the tools/Application/networking. Onsite resource is expected to perform testing, support, monitoring, implementation, Trouble Shooting, reporting, RCA reports, coordination with banks team/s, Audit compliance, any other statutory compliance, Patch Installation, fixes, analytics, fraud risk/rule management & monitoring, day to day MIS reports, Regulatory reports, conducting DR Drill, backup/restore. These activities are illustrative and the details will be shared with successful bidder. Bank reserves the right to claim change in resource based on the performance of the resources.
- 8.22.3. Detailed process documentation, SOP (Standard operating procedure) and management of solution should be created and submitted before project signoff.

- 8.22.4. Selected bidder is expected to deploy academically good, technically sound and competent personnel to ensure smooth operations at bank's site. The deputed personnel will be employed by the selected bidder on their payrolls/contracts without having any employment right with the bank. Moreover, deployed personnel will not have any right whatsoever to lodge claim of any nature directly or indirectly with the bank and it would be responsibility of selected bidder to address such issues without involving the bank. The deputed persons have to maintain the utmost secrecy & confidentiality of the bank's data including process performed at the Bank premises. At any time, if it comes to the notice of the bank that data has been compromised/ disclosed/ misused/ misappropriated then bank would take suitable action as deemed fit and selected vendor would be required to compensate the bank to the fullest extent of loss incurred by the bank. Bidder is expected to adhere to Bank's request for removal of any personnel, if bank notices any negligence/gross misconduct/violation of trade secret/disclosure of bank's data to third party and any decision of the bank in this regard would be final and binding upon the selected vendor.
- 8.22.5. Bidder has to agree and provide undertaking not to disclose any Bank information and will maintain confidentiality of Bank information as per policy of the Bank and will sign "Non-Disclosure Agreement" document provided in [Annexure - J](#).
- 8.22.6. The Bidder also has to agree and submit an undertaking that during the subsistence of this agreement it will not employ any personnel/individual below the Minimum Wages fixed by appropriate Government on this behalf from time to time, as per the provision of Minimum Wages Act 1948.

8.23. Placement of Order

Bank at its discretion will place separate or combined purchase order for all in-scope solution. Bank at its discretion may decide not to avail/purchase any or all services/solution/software/licenses. Banks decision in this regard will be final.

The Bank reserves the right to alter the number of locations specified in the tender, and to delete/substitute items from the ones specified in tender. Bank may also place order for various services which are only part of this RFP in addition to the quantities mentioned in this tender at the same rate terms and conditions including the cost agreed upon.

Bank reserves the right to place additional order with the selected Vendor during the validity of the contract, for any in-scope solution/Application also at the contracted rates and terms and conditions.

Bank also has the right not to avail/partially avail service mentioned in the RFP. In such case all payment will be made at actual.

9. Project Timelines (Delivery, Installation, Configuration and Integration)

Bank shall provide the address and contact details for delivery of required hardware/software items while placing the order.

All the software and hardware components at DC, DR must be delivered & installed **within 10 weeks** of issue of the purchase order to the successful Bidder.

All the software and hardware components at Zonal/Regional Offices, Branches and any other location must be delivered and installed **within 20 weeks** of issue of the confirm purchase order to the successful Bidder.

In case of any new order is given in future for new/existing site, delivery of all required components/equipments must be made **within 6 weeks** of placing the orders.

The Installation will be deemed as incomplete if any component of the hardware is not delivered or is delivered but not installed and / or not operational or not acceptable to the Bank after acceptance testing/ examination. In such an event, the supply and installation will be termed as incomplete and system(s) will not be accepted and the warranty period will not commence. The installation will be accepted only after complete commissioning of hardware and sign-off from Bank.

The Bank will not arrange for any Road Permit / Sales Tax or any other clearance for delivery of hardware to different locations and the Vendor is required to make the arrangements for delivery of hardware to the locations as per the list of locations /items provided from time to time by the Bank.

Commissioning of the hardware will be deemed as complete only when the same is accepted by the Bank in accordance with the Terms and Conditions of this Tender.

Partial or incomplete or damaged delivery of materials will not be considered as delivered of all the ordered materials. Date of delivery shall be treated as date of last material delivered to the ordered locations if materials are not damaged. In case materials are delivered with damage, Date of delivery shall be treated as date of replacement of damaged material with new one. Delivery payment shall be paid against completion of delivery of all the ordered materials without any damage and proof of delivery duly certified by Bank's Officials, along with delivery payment claim letter.

10. Transition Period

It is the responsibility of the successful bidder to take the transition from current Network Integrator within 1 month from award of contract /Purchase order.

The successful bidder has to present the detailed process for completing the transition to the Bank. At every stage, a signoff needs to be taken from the bank.

The successful bidder shall inform contact details of SPOC identified for as implementation manager within 2 weeks of receipt of order.

Post discussion with Bank's team, the successful bidder will have to share the profile of its support staff and technical personnel at each Regional office, DC, DR-Bengaluru, and Head office within 2 weeks from date of receipt of order.

The successful bidder has to submit a daily status report to the Regional Offices/Zonal offices and DIT regarding number of branches whose transition has been completed.

Once the successful bidder has updated the Bank about the completion of the transition of a branch, from that point onwards the whole responsibility of that branch (maintaining SLA, uptimes) is with the successful bidder.

The successful bidder shall conduct study of Bank's existing network (including IP scheme, router and switches configurations, routing protocols etc.,) and design the architecture for proposed network.

Network Design document and configuration document of all Bank applications in the network has to be submitted separately.

The successful bidder has to submit detailed report to bank containing but not limited to network equipment's requirement (like managed switches, etc.), bandwidth requirement, LAN design alteration etc.

Disaster Recovery plan (for network including links, equipment) should be prepared with step-by-step procedure of the network recovery, time taken for each operation and dependencies.

Project Manager is responsible/Single Point of Contact for all technical and non-technical/commercial activities within the scope of this order/ contract.

11. Execution of Work

- 11.1. The contract will be fixed for a period of 5 years.
- 11.2. The bidder shall be responsible in the event of security incidents due to improper configuration of in-scope devices.
- 11.3. Escalation Matrix shall be worked out at the time of placing orders from both sides.
- 11.4. Final selected bidder shall guarantee that all the software and aligned components used to service to bank are licensed and legal.

12. Compliance with IS/Cyber Security Policy

The Vendor shall have to comply with Bank's IT & IS Security policy in key concern areas relevant to the RFP, details of which will be shared with the selected Bidders. Some of the key areas are as under:

- 12.1. Responsibilities for data and application privacy and confidentiality
- 12.2. Responsibilities on system and software access control and administration
- 12.3. Custodial responsibilities for data, software, hardware and other assets of the Bank being managed by or assigned to the Vendor
- 12.4. Physical Security of the facilities
- 12.5. Physical and logical separation from other customers of the Vendor
- 12.6. Incident response and reporting procedures
- 12.7. Password Policy of the Bank
- 12.8. Data Encryption/Protection requirements of the Bank.
- 12.9. In general, confidentiality, integrity and availability must be ensured.

13. Cost & Currency

The offer must be made in Indian Rupees only as per [Annexure F\(A\)](#) - Indicative Commercial bid.

14. Price Variation

Prices payable to the successful bidder as stated in the contract shall be firm and not subject to any changes at any circumstances during the contract period.

15. Acceptance of Offer

- 15.1. The Bank reserves its right to reject any or all the offers without assigning any reason thereof whatsoever.
- 15.2. The Bank will not be obliged to meet and have discussions with any Bidder and/ or to entertain any representations in this regard.
- 15.3. The bids received and accepted will be evaluated by the Bank to ascertain the best and lowest bid in the interest of the Bank. However, the Bank does not bind itself to accept the lowest or any Bid and reserves the right to reject any or all bids at any point of time prior to the order without assigning any reasons whatsoever. The Bank reserves the right to re-tender the RFP with or without modifications.
- 15.4. The Bidder including those, whose tender is not accepted shall not be entitled to claim any costs, charges, damages and expenses of and incidental to or incurred by him through or in connection with his submission of tenders, even though the Bank may elect to modify/withdraw the tender.
- 15.5. The selected bidders shall submit the acceptance of the order within 7 days from the date of receipt of the order. No conditional or qualified acceptance shall be permitted.
- 15.6. Bank reserves its right to consider at its sole discretion the late acceptance of the order by selected Bidder.
- 15.7. Contract period is of 5 years from the date of post go-live of SD-WAN Solution with 4500 branches/offices or 6 months from date of 1st Installation, whichever is earlier. However, location wise rental payment will commence from the date of completion of all equipments installed at Branch/office. Bidder need to submit the duly signed copy of installation report.

16. Language of Bid

The language of the bid response and any communication with the Bank must be in written English only. Supporting documents provided with the RFP response can be in another language so long as it is accompanied by an attested translation in English, in which case, for purpose of evaluation of the bids, the English translation will govern.

17. Instructions for Bid Submission

17.1. Cost of RFP

- 17.1.1. RFP document can be purchased against payment of Rs.10,000/- (non-refundable) in the form of a demand draft issued by a scheduled commercial bank favoring Union

Bank of India payable at Mumbai. In case of bidders registered with The National Small Industries Corporation Limited (NSIC)/MSME, they are eligible for waiver of RFP document cost. However, they need to provide valid MSME/NSIC Certificate clearly mentioning that they are registered with NSIC/MSME under single point registration scheme.

17.1.2. RFP document can also be downloaded from the Bank's website www.unionbankofindia.co.in or from Government tender portal www.eprocure.gov.in or from E-procurement site ubi.abcpocure.com.

17.1.3. In the event of non-payment of the fee of Rs.10,000/- towards the RFP form, the offer will be rejected.

17.1.4. All costs and expenses (whether in terms of time or material or money) incurred by the Recipient/ Bidder in any way associated with the development, preparation and submission of responses, including but not limited to attendance at meetings, discussions, demonstrations, etc. and providing any additional information required by the Bank, will be borne entirely and exclusively by the Bidder.

17.2. Bid Security/ EMD (Refundable)

17.2.1. The bidder should deposit bid security of Rs.1,50,00,000/- (Rupees One Crore fifty lac Only) in the form of a demand draft favoring Union Bank of India, payable at Mumbai or Bank Guarantee issued from Scheduled Commercial Bank other than Union Bank of India, Andhra Bank and Corporation bank. Bank Guarantee should be valid from the date of submission of RFP for a period of minimum 45 days beyond the final bid validity period. IFSC Code for issuance of EMD is UBIN0556688.

17.2.2. In case of bidders registered with NSIC/MSME, they are eligible for waiver of EMD. However, they need to provide valid NSIC/MSME Certificate clearly mentioning that they are registered with NSIC under single point registration scheme. Other terms & conditions relating to Bid security is as under:

17.2.2.1. No interest will be payable on the Bid Security amount.

17.2.2.2. Unsuccessful Bidders' Bid security will be returned after completion of tender process. Unsuccessful Bidders should submit the Letter for Refund of EMD/Bid Security for returning of the bid security amount as per [Annexure N](#).

17.2.3. Bid Security will be forfeited in the following cases:

17.2.3.1. If a bidder withdraws its bid during the period of bid validity; or

17.2.3.2. If a Bidder makes any statement or encloses any form which turns out to be false / incorrect at any time prior to signing of Contract.

17.2.3.3. In case of any technical issues during reverse auction, if Bank decides to re-conduct reverse auction and any of the shortlisted bidder does not participate in the re-reverse auction at least by way of log in.

17.2.3.4. In case of a successful Bidder, if the Bidder fails:

17.2.3.4.1. To execute Contract within the stipulated time or

17.2.3.4.2. To furnish Performance Bank Guarantee as mentioned in Performance Bank Guarantee herein.

17.2.3.4.3. If the bidder refuses to accept the corrections of errors calculated in accordance with the terms of RFP.

17.2.4. The successful Bidders Bid security will be discharged upon signing the Contract Agreement and against submission of performance bank guarantee (other than Union Bank of India, Andhra Bank and Corporation Bank).

17.3. Performance Bank Guarantee (PBG)

The successful bidder shall provide a Performance Bank Guarantee for a value equivalent to 10% of yearly payout valid for one year within 30 days from the date of receipt of purchase order or signing of the contract whichever is earlier in the format as provided in [Annexure Q](#) with a claim period of 60 days and such other extended period as the Bank may decide for due performance of the project obligations. It is the responsibility of bidder to renew the Performance Bank Guarantee every year for a value equivalent to 10% of yearly payout. The PBG should be of that of scheduled Commercial Bank, other than Union Bank of India, Andhra Bank and Corporation Bank.

In the event of non-performance of obligation or failure to meet terms of this tender the Bank shall be entitled to invoke the performance guarantee without notice or right of demur to the successful bidder. Any amount pending for payment due to non-achieving of milestone/s set under the agreement or any other reason solely attributable to the successful bidder should be included in the remaining amount of the contract value.

The Bank reserves the right to recover any dues payable by the selected bidders from any amount outstanding to the credit of the selected bidders, including the pending bills and/or invoking Performance Guarantee, if any, under this contract.

If the Performance bank guarantee is not submitted within the stipulated time, the Bank reserves the right to cancel the order / contract and the earnest money deposit taken from the successful bidder, will be forfeited.

17.4. Period of validity of Bids

Bids should remain valid for the period of at least 180 days from the last date for submission of bid prescribed by the Bank. In case the last date of submission of bids is extended, the Bidder shall ensure that validity of bid is reckoned from modified date for submission. Further extension of the validity of the bid will be decided by the bank in case of need. The price quoted in Final Commercial Offer will be valid for at least 180 days from the date of offer.

17.5. Amendment of Bidding Documents

Prior to the last date for bid-submission, the Bank may, for any reason, whether at its own initiative or in response to clarification(s) sought from the prospective Bidders, modify the RFP contents/ covenants by amendment. Clarification /amendment, if any, will be notified on Bank's website. No individual communication would be made in this respect. In order to provide, Bidders, reasonable time to take the amendment into account for preparing their bid, the Bank may, at its discretion, extend the last date of submission of bids.

17.6. Authorization to Bid

The proposal/ bid being submitted would be binding on the Bidder. As such, it is necessary that authorized personnel, acceptable to bank, of the firm or organization sign the bid documents. The designated personnel should be authorized by a senior official of the organization having authority.

- 17.6.1. All pages of the bid shall be initialed by the person or persons signing the bid.
- 17.6.2. Bid form shall be signed in full & official seal affixed.
- 17.6.3. Any inter-lineation, erasure or overwriting shall be valid only if they are initialed by the person or persons signing the Bid.
- 17.6.4. All such initials shall be supported by a rubber stamp impression of the Bidder's firm.
- 17.6.5. The proposal must be accompanied with an undertaking letter duly signed by the designated personnel providing a bid commitment. The letter should also indicate the complete name and designation of the designated personnel.

17.7. Two part Bid

The Bid should be submitted online at the e-Procurement site <https://ubi.abcpurchase.com> by the Bidder. It should comprise the following components:

- 17.7.1. Technical bid - Part I: "Technical Bid for Network Management support services for Wide Area Network of the Bank".
- 17.7.2. Commercial bid - Part II: "Indicative Commercial Bid for Network Management support services for Wide Area Network of the Bank".
- 17.7.3. Any bid document not conforming to any one of the above terms will be rejected.
- 17.7.4. In the first stage, Cost of RFP, EMD/Bid Security, Integrity Pact (IP) signed by authorized signatory submitted by bidder will be reviewed and if it is as per prescribed format then only TECHNICAL BID will be opened and evaluated. Bidders satisfying the technical requirements as determined by the Bank and accepting the terms and conditions of this document shall be short-listed for commercial evaluation.
- 17.7.5. In the second stage, the INDICATIVE COMMERCIAL BID of only those bidders, whose technical bids are qualified and shortlisted, will be opened.
- 17.7.6. After evaluation of indicative commercial bids, the L1 bidder will be selected using Reverse Auction process. Reverse Auction Rules are given in [Annexure L](#)
- 17.7.7. The indicative commercial bid will be used for deciding the start bid price for reverse auction. After completion of the reverse auction, selected bidder should submit the price break-up as per the [Annexure F\(A\)](#).

17.8. Technical Offer

- 17.8.1. The Technical Bid - Part I should be complete in all respects and contain all information asked for in this document. It should not contain any price information.
- 17.8.2. The Technical Bid - Part I must be submitted online.
- 17.8.3. The following three original documents are to be submitted to the bank physically on or before last date & time of bid submission:
 - 17.8.3.1. Cost of RFP of Rs. 10,000/- (Rupees Ten thousand only) in the form of demand draft issued by scheduled commercial bank favouring Union Bank of India, Payable at Mumbai.
 - 17.8.3.2. Bid security of Rs.1,50,00,000/- (Rupees One Crore fifty lac only) in the form of a demand draft issued by a Scheduled commercial bank favoring Union Bank of India, payable at Mumbai or Bank Guarantee from commercial Bank other than Union Bank of India, Andhra Bank and Corporation Bank.
 - 17.8.3.3. Integrity Pact (IP) as provided in [Annexure M](#) is to be submitted physically. It should be on plain paper duly signed by authorized signatories.
- 17.8.4. The following documents are to be submitted online at the e-procurement site <https://ubi.abcpocure.com>:
 - 17.8.4.1. In case of bidders registered with NSIC/MSME, who are eligible for waiver of EMD, they need to provide valid NSIC/MSME Certificate clearly mentioning that they are registered with NSIC under single point registration scheme.
 - 17.8.4.2. [Annexure A](#) - Letter of Acceptance
 - 17.8.4.3. [Annexure B](#) - Bidder's Profile Format
 - 17.8.4.4. [Annexure C](#) - Eligibility Criteria
 - 17.8.4.5. [Annexure D](#) - Compliance to RFP Terms & Conditions
 - 17.8.4.6. [Annexure E](#) - Technical Compliance
 - 17.8.4.7. [Annexure E\(A\)](#) - Configuration of Proposed Solution
 - 17.8.4.8. [Annexure F](#) - Unpriced Indicative Commercial Bid
 - 17.8.4.9. [Annexure G](#) - Declaration for Compliance
 - 17.8.4.10. [Annexure H](#) - Undertaking by Bidder
 - 17.8.4.11. [Annexure J](#) - Confidentiality / Non-Disclosure Agreement
 - 17.8.4.12. [Annexure K](#) - Reference Site Details
 - 17.8.4.13. [Annexure L](#) - Business Rules for Reverse Auction
 - 17.8.4.14. [Annexure L\(A\)](#) - Compliance Statement for Reverse Auction
 - 17.8.4.15. [Annexure L\(B\)](#) - Letter of Authority for Participation in Reverse Auction
 - 17.8.4.16. [Annexure L\(C\)](#) - Undertaking of Process Compliance for RA
 - 17.8.4.17. [Annexure R](#) - Know Your Employee (KYE) Clause
 - 17.8.4.18. [Annexure U](#) - Undertaking of Information Security
 - 17.8.4.19. [Annexure X](#) - Standard Terms and Conditions for Outsourcing
 - 17.8.4.20. [Annexure Y](#) - Undertaking of Authenticity of Networking Hardware

- 17.8.4.21. The Bid should be signed by the authorized signatory of the bidder. A power of attorney to that effect shall be submitted by the bidders and should be uploaded online on portal along with technical bid.
- 17.8.4.22. Photocopies of relevant documents / certificates as proof in support of various information submitted online in aforesaid annexure and other claims made by the bidder.
- 17.8.4.23. All the annexure should be submitted online in letter head of bidder duly signed with seal of the company. Photocopies of relevant documents / certificates as proof in support of various information submitted in aforesaid annexure and other claims made by the vendor.
- 17.8.4.24. Detailed Architecture/Design of the proposed solution with various features/functions of the system/sub-system including fail-over methodology/strategy at both Primary & DR Site.
- 17.8.4.25. Documents and brochures pertaining to product that will be deployed in the proposed solution.
- 17.8.4.26. Signed & Sealed copy of all the pages of RFP and corrigendum if any, to be submitted online along with the technical bid.
- 17.8.4.27. The bidder should ensure that all the annexure are submitted as prescribed by the Bank. In case it is not in the prescribed format, it is liable to be rejected.
- 17.8.5. The Bank reserves the right to resort to re-tendering without providing any reason whatsoever. The Bank shall not incur any liability on account of such rejection.
- 17.8.6. The Bank further reserves the right to reject any or all offers based on its own evaluation of the offers received, or on the basis of stability, capabilities, track records, reputation among users and other similar features of a bidder.
- 17.8.7. The Bank reserves the right to disqualify the bidder/(s) if bidder/(s) have not completed/performed any project successfully/satisfactorily in Union Bank of India in stipulated time i.e. supply, Installation, Implementation etc.
- 17.8.8. The Bank reserves the right to modify any terms, conditions or specifications of RFP before date of submission of bids. Bidder has to submit bid documents as per the changes/modifications while submitting the bid. Notification of amendments/corrigendum will be made available on the Bank's website www.unionbankofindia.co.in, Government tender portal as well as e-procurement portal and will be binding on all bidders and no separate communication will be issued. In order to allow prospective bidders reasonable time in which to take the amendment into account in preparing their bids, the Bank, at its discretion, may extend the deadline for a reasonable period as decided by the Bank for the submission of bids. No post bid clarification of the bidder shall be entertained.

17.9. Indicative Commercial Offer

The commercial offer must not contradict the Technical offer in any way and should include the cost of all the items offered. The suggested directive for Commercial offer is as follows:

17.9.1. The Indicative Commercial Offer (Part II) should be submitted online at the e-Procurement site as per [Annexure F\(A\)](#) by way of entering the values in the format provided at the site. This must contain all price information.

17.9.2. The vendors should not offer any options or any conditional offers to the Bank while giving the price information. The offer should strictly be in conformity with the items as specified by the Bank. No additions or deletions to the Annexure are allowed. Any deviations may lead to disqualification of the bid.

17.10. RFP Clarifications

Queries / clarifications will not be entertained over the phone. All queries and clarifications must be sought by email to abhijit@unionbankofindia.com, dnpeter@unionbankofindia.com and madhan.r@unionbankofindia.com with subject “Request for Proposal (RFP) for Network Management support services for Wide Area Network of the Bank” as per [Annexure O](#).

The Bidder is requested to collate and submit queries together to seek clarifications / responses from Bank. The Bidder should ensure that all the queries and clarifications are communicated in email on or before the date given in the schedule of events of this RFP document. Bidders are requested to visit Bank’s website for clarifications and other communications.

Any modification of the RFP, which may become necessary as a result of the queries, shall be made available by the Bank exclusively through the issue of Corrigendum on Bank’s website www.unionbankofindia.co.in, government tender portal www.eprocure.gov.in or at e-procurement portal ubi.abcpocure.com.

17.11. Technical Bid Evaluation

17.11.1 During the period of evaluation, bidders may be asked to provide more details and explanations about information provided in the proposals. Bidders should respond to such requests within the time frame indicated in the letter/e-mail seeking explanation, if the bidder does not comply or respond by the date, their bid will be liable to be rejected. If any part of the technical specification offered by the bidder is different from the specifications sought in our RFP, the bidder has to substantiate the same in detail the reason of their quoting a different specification than what is sought for, like higher version or non-availability of the specifications quoted by us, invariably to process the technical offer and it should be compatible to our application.

17.11.2 Setting of evaluation criteria for selection purposes shall be entirely at the discretion of the Bank. The decision of the bank in this regard shall be final and no correspondence shall be entertained in this regard.

17.11.3 The Bank may, at its discretion, waive any minor informality, nonconformity, or irregularity in a bid which does not constitute a material deviation and financial impact, provided such waiver does not prejudice or affect the relative ranking of any bidder. Wherever necessary, observations on such 'minor' issues (as mentioned above) Bank may be conveyed to the bidder, asking them to respond by a specified date also mentioning therein that, if the bidder does not respond by the specified date, their bid will be liable to be rejected.

17.11.4 On the basis of technical evaluation, the Bank shall take a decision for short listing of the bidders for Commercial Evaluation. If the technical evaluation is not found to be satisfactory, further evaluation will not be done. No separate information will be sent to the disqualified bidders. Any decision of the Bank in this regard shall be final, conclusive and binding on the bidder.

17.11.5 Complete technical Evaluation Process is provided as per [Annexure I](#) to this RFP.

17.12. Commercial Bid Evaluation

17.12.1. For finalization of the most competitive offer, the Bank will conduct 'Reverse auction'. The detailed procedure and Business rules for the Reverse auction is given as per [Annexure-L](#) and are also available on Bank's web site.

17.12.2. The technically qualified bidders will participate in the Reverse auction process that will be conducted by an Auction company authorized by the Bank. Specific rules for this particular event viz. date and time, start price, bid decrement value, duration of event etc. shall be informed by the Auction Company to the participating bidders before the event. The bidders should furnish indicative prices for the project in their Indicative Commercial Bid to facilitate finalizing the start bid for 'Reverse auction' under E-Procurement process.

17.12.3. The lowest Indicative commercial offers (total cost) may be taken as the starting bid of the Reverse Auction and not for deciding the L-1 status. Bidders should note that the indicative commercial bid is considered for the purpose of conducting Reverse auction process only. The L-1 bidder will be decided only later, on finalization of prices through Reverse auction.

17.12.4. The L-1 bidder emerging at the end of the Reverse Auction process shall be required to submit the break-up of his Final price (last bid price) again in [Annexure-F \(A\)](#). Failure or refusal to offer the services/goods at the price committed through Reverse Auction shall result in forfeit of the EMD to Bank, which please be noted.

17.12.5. The final decision on the bidder will be taken by Union Bank of India. Union Bank reserves the right to reject any or all proposals. Similarly, it reserves the right not to include any bidder in the final short-list.

17.12.6. Applicability of Preference to Make in India, Order 2017 (PPP-MII Order)

17.12.6.1. Guidelines on Public Procurement (Preference to Make in India), Order 2017 (PPP-MII Order) and revised vide GOI, Ministry of Commerce and Industry,

Department of Industrial Policy and Promotion letter No. P-45021/2/2017(BE-II) dated May 28, 2018 will be applicable for this RFP and allotment will be done in terms of said Order as under:

- a. Among all qualified bids, the lowest bid (as quoted in reverse auction) will be termed as L1. If L1 is from a local supplier, the contract will be awarded to L1.
- b. If L1 is not from a local supplier, the lowest bidder among the local suppliers will be invited to match the L1 price subject to local supplier's quoted price falling within the margin of purchase preference, and the contract shall be awarded to such local supplier subject to matching the L1 price.
- c. In case such lowest eligible local supplier fails to match the L1 price, the local supplier with the next higher bid within the margin of purchase preference shall be invited to match the L1 price and so on and contract shall be awarded accordingly. In case none of the local suppliers within the margin of purchase preference matches the L1 price, then the contract will be awarded to the L1 bidder.

17.12.6.2. Definitions

- a. "Local content" means the amount of value added in India which shall be the total value of the item procured (excluding net domestic indirect taxes) minus the value of imported content in the item (including all customs duties) as a proportion of the total value, in percent.
- b. "Local supplier" means a supplier or service provider whose product or service offered for procurement meets the minimum 50% local content.
- c. "Margin of purchase preference" means the maximum extent to which the price quoted by a local supplier may be above the L1 for the purpose of purchase preference. The margin of purchase preference shall be 20%.

17.12.6.3. Verification of local content

- a. The local supplier at the time of submission of bid shall be required to provide a certificate as per [Annexure W](#) from the statutory auditor or cost auditor of the company (in the case of companies) or from a practicing cost accountant or practicing chartered accountant (in respect of suppliers other than companies) giving the percentage of local content.

17.12.7. The Bank shall follow all the guidelines/notifications for public procurement.

17.13. Rules for Re-Reverse Auction

- 17.13.1. Bank may consider the option of a Re-reverse Auction in following circumstances:
- 17.13.2. During the process of reverse auctions, if there is either no bids from logged in bidders or only one bidder puts up bid/s, Bank may decide a re-reverse auction by taking fresh Indicative prices from all qualified bidders in sealed cover only, to amend the start price for Re-reverse auction.
- 17.13.3. In case the start price for the Reverse Auction event is decided by Bank and there are no bids or only one bid/s by a single bidder in the Reverse Auction, Bank may

decide Re-reverse Auction while further amending the start price.

17.13.4. Reverse auction will be valid only if two or more bidders are participating in the reverse auction event.

17.13.5. In all the above circumstances, the functional head of the department may take a decision on re-reverse auction.

17.14. Bank's Right to Accept or Reject any Bid or all Bids

Bank shall be under no obligation to accept the lowest price bid or any other offer received in response to this Tender notice and shall be entitled to reject any or all offers including those received late or incomplete offers without assigning any reason whatsoever. The Bank reserves the right to make any changes in the terms and conditions of purchase. The Bank will not be obliged to meet and have discussions with any Bidder, and / or to listen to any representations unless there is change in the terms and conditions of purchase.

18. Award of Contract

On completion of evaluation of commercial bids through reverse auction, Bank will determine the L1 bidder and contract will be awarded to lowest bidder after reverse auction process as per [Annexure L](#).

19. Price Composition

19.1 TCO is for 5 years. The Bidders should quote prices strictly as per the price composition stated in indicative commercial bid failing which the offers are likely to be rejected.

19.2 The indicative commercial bid should be quoted in the indicative commercial bid format attached as [Annexure F \(A\)](#) to this bid.

19.3 The prices should be firm and not dependent on any variable factors and expressed in Indian Rupees.

19.4 The Total cost should be inclusive of all other charges but exclusive of GST (CGST/SGST/IGST) which will be paid at actual at the time of invoicing.

19.5 Bidder has to show the bifurcation/details of GST (CGST/SGST/IGST) in every invoice.

19.6 Bank will not pay any Labor charges, incidental chargers, transportation and miscellaneous expenditure separately. All such costs, if any, should be absorbed in the TCO.

20. Taxes and Duties

The Bidder shall solely be responsible for all payments (including any statutory payments) to its employees and shall ensure that at no time shall its employees, personnel or agents hold themselves out as employees or agents of the Bank, nor seek to be treated as employees of the Bank for any purpose, including claims of entitlement to fringe benefits provided by the Bank, or for any kind of income or benefits. The Bidder alone shall file all applicable tax returns for all of its personnel assigned hereunder in a manner consistent with its status as an independent contractor of services; and the Bidder will make all required payments and deposits of taxes in a timely manner.

Payment of all taxes i.e. GST (CGST/SGST /IGST) will be made at actual, on production of suitable evidence of payment by the Bidder.

The Bidder shall be liable to pay all applicable corporate taxes and income tax that shall be levied according to the laws and regulations applicable from time to time in India.

Wherever the laws and regulations require deduction of such taxes at the source of payment, Bank shall effect such deductions from the payment due to the Bidder. The remittance of amounts so deducted and issuance of certificate for such deductions shall be made by Bank as per the laws and regulations in force. Nothing in the Contract shall relieve the Bidder from his responsibility to pay any tax that may be levied in India on income and profits made by the Bidder in respect of this Contract.

21. Rejection of Bid

The Bid is liable to be rejected if:

- 21.1 The document does not bear signature of authorized person in each page and duly stamp.
- 21.2 It is received through Fax/E-mail/dropped in tender box.
- 21.3 It is received after expiry of the due date and time stipulated for Bid submission.
- 21.4 Incomplete Bids, including non-submission or non-furnishing of requisite documents / Conditional Bids / Bids not conforming to the terms and conditions stipulated in this Request for proposal (RFP) are liable for rejection by the Bank.
- 21.5 It is evasive or contains incorrect information.
- 21.6 Any form of canvassing / lobbying /influence/ query regarding short listing, status etc. will be a disqualification.
- 21.7 Bidder should comply with all the points mentioned in the scope of work. Noncompliance of any point will lead to rejection of the bid.
- 21.8 Non-submission of bid security/EMD/Integrity Pact (IP).

22. Modification and Withdrawals of Bid

No bid can be modified by the bidder subsequent to the closing date and time for submission of bids. In the event of withdrawal of the bid by bidders, the EMD will not be refunded by the Bank.

23. Pre-Bid Meeting

For the purpose of clarifications of doubts of the bidders on issues related to the RFP, Bank will hold a pre-bid meeting on the date & time as indicated in the RFP. It may be noted that no query of any bidder shall be entertained / received after the mentioned date. Queries raised by the prospective bidders and the Bank's response will be available at Bank's web site. Only authorized representative of bidder (maximum two) will be allowed to attend the Pre-bid meeting. A letter from authorized signatory of the organization should be submitted for the same at the time of pre-bid meeting.

Non- attendance at the Pre-bid Meeting will not be a cause for disqualification of a bidder.

Any modification of the RFP, which may become necessary as a result of the Pre- bid Meeting, shall be made by the Bank exclusively through the issue of an Addendum/Corrigendum on Bank's website www.unionbankofindia.co.in, government tender portal www.eprocure.gov.in and e-Procurement site <https://ubi.abcprocure.com>.

24. RFP Response

All submissions will become the property of Bank. Recipients shall be deemed to license, and grant all rights to, Bank to reproduce the whole or any portion of their submission for the purpose of evaluation, to disclose the contents of the submission to other Recipients who have registered a submission and to disclose and/or use the contents of the submission as the basis for any resulting RFP process, notwithstanding any copyright or other intellectual property right that may subsist in the submission or Banking documents.

Bid properly documented should be uploaded on e-Procurement site ubi.abcprocure.com within stipulated date & time mentioned in the RFP.

25. Payment Terms

The Bidder must accept the payment terms proposed by the Bank as proposed in this Section.

- 25.1. Bank will release payment for hardware and software rental charge, facility management charge and Link Management charge quarterly on a per-site basis based on the achievement of SLAs. It is reiterated that the network performance and uptime of the network as specified under SLA clause will be assessed on monthly basis and the payment will be made quarterly. The vendor should submit the site-wise equipment details along with the uptime achieved to enable the Bank to pay quarterly charges.
- 25.2. The rental charges will be paid based on site category (site category is as per actual deployment of equipments in that location).
- 25.3. The charges per location will begin from the date of completion of installation of all equipments and termination of the links. The NSI should submit the installation and commissioning certificate signed by the Bank's official certifying successful completion of installation and commissioning for the payment.
- 25.4. One time charges (such as upgradation, shifting, commissioning, etc) will be paid on per site basis after successful completion of activity and testing as per the itemized charges under the head - Link commissioning and shifting, at the end of each quarter.
- 25.5. TDS on payments will be deducted as applicable.
- 25.6. No advance payment against purchase order.
- 25.7. Bidder has to show the bifurcation/details of GST (CGST/SGST/IGST) in every invoice.

25.8. Procedure for claiming payments

- 25.2.1. NSI should raise invoices after deducting the applicable penalties i.e. SLA, extended, etc.
- 25.2.2. The Bidder's requests for payment shall be made to the Bank in writing accompanied by Original Invoice detailing the systems, software delivered, installed and accepted by the bank.

25.2.3. The payment after deducting applicable TDS will be released by the Bank. All payments will be made only by electronic transfer of funds either by NEFT or RTGS. The Bidder therefore has to furnish the bank account number to where the funds have to be transferred for effecting payments.

25.9. General Conditions:

- 25.9.1. There shall be no escalation in the prices once the prices are fixed and agreed by the Bank and the Bidder.
- 25.9.2. No advance payment will be made prior to the start of the implementation.
- 25.9.3. All applicable taxes and duties will be deducted at source as per applicable laws.
- 25.9.4. Any penalties / liquidated damages imposed on the bidder for non-performance will be deducted from the payment as deemed necessary.

26. Order Cancellation/ Termination of Contract

- 26.1. The Bank reserves its right to cancel the Purchase Order at any time by assigning appropriate reasons and recover expenditure incurred by the Bank in addition to recovery of liquidated damages in terms of the contract, in the event of one or more of the following conditions:
 - 26.1.1. Delay in commencement of the project beyond two weeks after the assignment order or beyond the date given by the bank in the purchase order.
 - 26.1.2. Serious discrepancies noted in the inspection.
 - 26.1.3. Breaches in the terms and conditions of the Order.
- 26.2. The Bank reserves the right to cancel /terminate the contract placed on the selected bidder and recover expenditure incurred by the Bank on the following circumstances:
 - 26.2.1. Non-submission of acceptance of order within 7 days of order
 - 26.2.2. Non-submission of Performance Bank Guarantee as per terms of RFP.
 - 26.2.3. Excessive delay in execution of order placed by the Bank.
 - 26.2.4. The selected bidder commits a breach of any of the terms and conditions of the bid.
 - 26.2.5. The bidder goes in to liquidation voluntarily or otherwise.
 - 26.2.6. Misconduct of the bidder or any of its staff/employees or representatives which affects execution of the contract/loss of reputation/financial risk to bank.
 - 26.2.7. Any third party claim against bank, loss/damage to bank arising due to bidder/bidder's omissions, errors.
 - 26.2.8. Non-execution of agreement/s within the time stipulated by bank
- 26.3. Bank shall serve the notice of termination to the bidder at least 30 days prior, of its intention to terminate services.
- 26.4. After the award of the contract, if the selected bidders do not perform satisfactorily or delays execution of the contract, the Bank reserves the right to get the balance contract executed by another service provider of its choice by giving one months' notice for the same. In this event, the selected bidder is bound to make good the additional expenditure, which the Bank may have to incur to carry out, for the execution of the balance of the order/contract. Such additional expenditure shall be incurred by the bank within

reasonable limits & at comparable price prevailing in the market. This clause is also applicable, if for any reason, the contract is cancelled.

- 26.5. The Bank reserves the right to recover any dues payable by the selected bidder from any amount outstanding to the credit of the selected bidder, including the pending bills and security deposit, if any, under this contract.
- 26.6. In addition to the cancellation of purchase order, the Bank reserves its right to invoke the Bank Guarantee or foreclose the Security Deposit given by the bidder towards non-performance/non-compliance of the terms and conditions of the contract, to appropriate towards damages.

27. Contract Period

- 27.1. Contract period is of 5 years from the date of post go-live of SD-WAN Solution with 4500 branches/offices or 6 months from date of 1st Installation, whichever is earlier.
- 27.2. Bidder is required to provide the services for the contract period of 5 years.
- 27.3. Post completion of the contract/ or in the event of early termination, the bidder is expected to provide support for transition of the services to the nominated members of the bank (or) to a third party nominated by the bank.
- 27.4. All solution supplied on OPEX model should be under comprehensive warranty/ AMC support directly or through their OEM authorized representatives at all locations for bank. OEM of each solution shall provide the same in writing.
- 27.5. If any support is required after the contract with respect to logs, the system integrator has to provide the same.
- 27.6. Bidder shall provide transition support, which amongst other shall include provision of logs, rules, technical architecture of solution as deployed, detailed description of the processes, etc. as part of the transition to subsequent NSI or bank on completion or on termination of contract. The support should be for a period of 6 months.
- 27.7. The performance of the bidder will be reviewed on yearly basis to ascertain bidder's capability during the period.
- 27.8. If found unsatisfactory, the contract may be terminated by giving 6 months' notice period at any point of time. However, during the notice period, the bidder is expected to deliver the same level of services as prescribed in the RFP and same payment terms will be applicable.

28. Liquidated Damages (LD)

If Successful bidders fail to deliver any or all software/Hardware or commence any or all of the Service(s) specified in the RFP/Contract / Agreement i.e. 20 weeks for initial order and 6 weeks for future new/existing branch/office, would attract liquidated damages. Bank Shall without prejudice to its other rights and remedies under and in accordance with the RFP/Contract / Agreement, levy Liquidated Damages (LD) from payments, which are due to the Successful bidder. For calculation of LD:

28.1. Delay in delivery of hardware

If the deliverables are not submitted as per the implementation schedule and project phasing or extensions in writing as may be given by Bank, the Bidder shall be liable to pay 0.5% per week of the invoice value (exclusive of Taxes) location/office address wise with a cap of 5% of the Hardware price.

28.2. Delay in implementation of solution

In case bidder fails to install, configure & Implement any solution in given timeline, the Bidder shall be liable to pay 0.5% per week of the invoice value (exclusive of Taxes) location/office address wise with a maximum cap of 5%.

28.3. The contract price for calculation of LD is TCO.

28.4. The overall LD during implementation will be to a maximum of 10% of the total cost of the project.

28.5. The Bank reserves its right to recover these amounts by any mode such as adjusting from any payments to be made by the Bank to the company.

28.6. Part of week will be treated as a week for this purpose.

28.7. However, the Bank may, at its discretion, waive the liquidated damages in case the delay cannot be attributed to the Bidder.

28.8. Bank will deduct the amount of liquidated damages from the payment due of the same project from the Successful bidder. Bank may also withhold the amount to be recovered from the payment due from other projects held by the same bidder.

28.9. Any such recovery or liquidated damages shall not in any way relieve the Successful bidder from any of its obligations to complete the works / service(s) or from any other obligations and liabilities under the Contract/Agreement/ Purchase Order.

29. Service Level Agreement and Penalties

29.1 The Bank notifies the successful Bidder that its Bid has been accepted, the Bidder shall enter into a Service Level Agreement (SLA) with the Bank, containing all the Terms and Conditions of this RFP, including confidentiality, non-disclosure and penalty clauses, and any other clause relevant to the services offered.

29.2 The Bidder need to execute a Service Level Agreement/Contract with the Bank covering all terms and conditions of this tender. Bidder need to strictly adhere to Service Level Agreements (SLA). Services delivered by bidder should comply with the SLA mentioned below. The Bank shall without prejudice to its other rights and remedies under and in accordance with the terms of the RFP levy penalty from payments due to the Bidder. SLA will be reviewed on a quarterly basis. SLA violation will attract penalties.

29.3 Inability of the Bidder either to provide the requirements as per scope or to meet the timelines as specified would attract penalty.

29.4 Service Levels will include Availability measurements and Performance parameters.

29.5 The Vendor shall provide Availability Report on a monthly basis and a review shall be conducted based on this report. A monthly report shall be provided to the Bank on the 5th of the succeeding month containing the summary of all incidents reported and associated Bidder performance measurement for that period. Bidder shall use an appropriate tool for the purpose of such reporting.

29.6 Performance measurements would be assessed through audits or reports, as appropriate to be provided by the Bidder e.g. utilization reports, response time measurements reports, etc. The tools to perform the audit will need to be provided by the Bidder. Audits will normally be done on regular basis or as required by the Bank and will be performed by Bank or Bank appointed third party agencies.

29.7 System availability is defined as:

$$\{(\text{Scheduled operation time} - \text{system downtime}) / (\text{scheduled operation time}) * 100\}$$

Where:

29.7.1. "Scheduled operation time" is the scheduled operating hours of the System for the month. All planned downtime on the system would be deducted from the total operation time for the month to give the scheduled operation time.

29.7.2. "System downtime" subject to the SLA, is accumulated time during which the System is not available to the Bank's users or customers due to in-scope system or infrastructure failure, and measured from the time Bank and/or its customers log a call with the Bidder help desk of the failure or the failure is known to the Bidder from the availability measurement tools to the time when the System is returned to proper operation.

29.7.3. Service Levels should be complied with irrespective of the customizations that the applications would undergo during the tenure of the Contract.

29.8 Penalties for not meeting uptime

29.8.1. Components hosted in DC and DR such as servers, Call manager, Concentrator/Head End Devices, Network controller must have high uptime and for any unscheduled downtime Penalties will be calculated as mentioned below:

S.N.	Service Area	Expected Service Level	Penalty
1.	Set of Devices (Hardware/Software) component failure leading to the complete disruption of the objective performed by the said devices. (Both DC and DR down at the same time)		10% of monthly rental of effected solution on each occasion 100% of monthly rental of effected solution charges if problem not resolved within 48 Hours.
2.	Solution Uptime. (Individual systems at DC / DR) Uptime % calculated on	99.95% and above	NA
		98.00% and above but below 99.95%	5% of monthly cost of affected solution
		95.00% and above but below	10% of monthly cost of

monthly basis for each solution.	98.00%	affected solution
	80.00% and above but below 95.00%	30% of monthly cost of affected solution
	70.00% and above but below 80.00%	50% of monthly cost of affected solution
	Less than 70%	100% of monthly cost of affected solution

29.8.2. In case any branch/office is down for more than 24 hours due to failure of hardware (Router, Switch, Modem), Penalty of Rs.1,000/- per day per site shall be deducted in addition to SLA mentioned above.

29.9 Link Maintenance and Monitoring

The table below specifies the end-to-end link uptime matrix along with mean time to respond (MTTR)

No	Office	City	Uptime	MTTR (HH:MM)
1	DC, DRC& NDC	Metro	99.999%	00:00
2	Other Links	All	99.50%	02:00

The round trip delay of the network at any point to any point during the business hours (8 A.M to 8 P.M) should be less than 100 msec (average obtained by the ping command over 1000 samples) and packet drop should be less than 0.1% in any one minute window. In case of high latency, it will be responsibility of the NSI to coordinate with Telecom Service provider to rectify the latency either by replacing the local pair or by other similar measures to contain latency within the stipulated limits.

At central side, downtimes calculation is defined as follows:

1. Downtime episodes of less than a minute are ignored
2. Downtimes episodes of more than 1 minute but less than 20 minutes are counted as actuals.
3. Downtime episodes exceeding 20 minutes but less than 120 minutes are counted as twice the actual downtime.
4. Downtimes exceeding 2 hrs are treated as full-day downtimes.
5. Time between successive downtimes should be at least 6 months

29.10. Penalties for downtime will be calculated as mentioned below:

S.N.	Service Area	Expected Service Level	Penalty
1.	DC, DR and NDC Uptime % calculated on monthly basis for each solution.	99.99% or more	NA
		99.98% or more	1% of monthly Link Monitoring and Maintenance charges
		99.97% or more	2% of monthly Link Monitoring and Maintenance charges

		99.96% or more	3% of monthly Link Monitoring and Maintenance charges
		99.95% or more	4% of monthly Link Monitoring and Maintenance charges
		99.90% to 99.95%	5% of monthly Link Monitoring and Maintenance charges
		Less than 99.90%	100% of monthly Link Monitoring and Maintenance charges
2.	Uptime for Branches, Regional and Zonal offices	99% or more	NA
		98% or more	10% of monthly Link Monitoring and Maintenance charges and device rental charges for affected branches/office
		97% or more	20% of monthly Link Monitoring and Maintenance charges and device rental charges for affected branches/office
		96% or more	30% of monthly Link Monitoring and Maintenance charges and device rental charges for affected branches/office
		95% or more	40% of monthly Link Monitoring and Maintenance charges and device rental charges for affected branches/office
		95% to 90%	50% of monthly Link Monitoring and Maintenance charges and device rental charges for affected branches/office
		Less than 90%	100% of monthly Link Monitoring and Maintenance charges and device rental charges for affected branches/office

29.11. Following will be excluded while calculating the down time:

- Approved Scheduled downtime obtained through proper change management process.

- Down time due to Bank issues.
- Down time due to major ISP issues like ring failure, trunk failure, Telephone Exchange failure, fiber cut and MPLS PoP failure.
- Down time due to force measure like Earth quake, Natural calamities, Riots and major power outage

29.12. Other Service Level and associated penalties

S.N.	Service Area	Expected Service Level	Deliverables/Penalty
1.	Report and Dashboard	Periodic reports to be provided to bank	Daily Reports: Critical reports should be submitted as and when required. Timings will be mutually decided. Weekly Reports: To be decided mutually Monthly Reports: Before 10th of each month
2.	Continual Improvement	The Bidder is expected to improve the operations on an on-going basis. The Bidder is expected to provide a quarterly report of the new improvements suggested, action plans, and the status of these Improvements to the bank. Improvement areas could include: process changes/ training resulting in efficiency/SLA improvement, new correlation rules to identify threat patterns etc.	Quarterly reports need to be provided within 5 days of the end of the quarter
3.	Periodic Review	The project sponsor or locational delegate from the Bidder is expected to conduct a monthly review meeting with Bank officials resulting in a report covering details about current SLAs, status of operations, key issues and new challenges etc.	Monthly meeting for next five years to be conducted within 7 days post submission of report for each month during the operations phase.
4.	solution management - Version / Release/Upgrades / patches	Bidder to inform bank team and ensure that entire stack of - firmware, software, middleware, etc. are updated with latest firmware, patches, upgrades, release, version, etc. as per the Bank policy.	NSI has to submit firmware version report (deployed and current version) every month. Along with this NSI shall also submit Plan of Action (PoA) for version upgrade, if any
5.	Audit of Network Infrastructure	Network infrastructure may be subjected to audit from Bank and/or third party. Audit observations to be closed in mutually agreed timeframe.	Penalty of 1% of Monthly operation charges for each week of delay in implementation of critical and important observations.

		VA/PT exercises conducted by Bank's internal teams will also considered under this point	Penalty will be restricted to 3% of monthly operation charges.
6.	Manpower services	Bidder to provide experienced and certified manpower at Bank premises as per RFP. Any gap will attract penalty	After deducting pro-rata charge for absence of resource, additional penalty of 500/- Per absent recourse per day will be deducted. In case bidder provides alternate adequately qualified resource for absent resource, no penalty shall be deducted. The penalty will be restricted up to 25% of monthly FM Charges
8.	Governance Risk and Compliance	The bidder is expected to provide reports dashboards on ad-hoc basis as and when required by Bank. Bidder must provide a written/email based response to the requested dashboard/report mentioning the time of delivery of report/dashboard Service uptime SLA shall apply after the time of delivery as declared by the bidder.	Bidder failing to respond back with details of dashboard/report availability shall be penalty of 3% of the NOC monthly operations charges.

NOTE - Overall SLA penalty will be capped to 10% of contract value.

- 29.13. Solution uptime is to be maintained without any consideration of devices in HA mode. If a function at the primary site is down, the same should be shifted to DR site within the SLA parameters.
- 29.14. NOC Operation cost will include Monthly Link Maintenance Charges, Monthly Link Monitoring Charges and Monthly Rental charges.
- 29.15. Penalty will be calculated on monthly basis. Please refer clause on penalty for other details such as overall cap on penalty.

30. Authorized Signatory

The selected bidders should indicate the authorized signatories who can discuss and correspond with the BANK, with regard to the obligations under the contract. The selected bidders shall submit at the time of signing the contract a certified copy of the resolution of their board, authenticated by the company secretary, authorizing an official or officials of the bidder to discuss, sign agreements/contracts with the BANK, raise invoice and accept payments and also to correspond. The bidder shall provide proof of signature identification for the above purposes as required by the BANK.

31. Limitation of Liability

The Bidder's aggregate liability (whether in contract, tort or otherwise), shall not exceed the total contract value provided that this limitation shall not apply to any of the obligation of the bidder to the bank arising from clauses - Liquidated Damages, Indemnity, and Confidentiality / Non-Disclosure Agreement of the RFP.

32. Confidentiality

The bidder must undertake that all the employees/persons entrusted for the work shall hold in trust any Information received by them, under the Contract/Agreement, and the strictest of confidence shall be maintained in respect of such Information. The bidder has also to agree:

- 32.1. To maintain and use the Information only for the purposes of the Contract/Agreement and only as permitted by the BANK;
- 32.2. To only make copies as specifically authorized by the prior written consent of the Bank and with the same confidential or proprietary notices as may be printed or displayed on the original;
- 32.3. To restrict access and disclosure of Information to such of their employees, agents, strictly on a "need to know" basis, to maintain confidentiality of the Information disclosed to them in accordance with this Clause and
- 32.4. To treat all Information as Confidential Information.
- 32.5. The Selected Bidders shall be required to sign a Non-Disclosure Agreement with Bank as per prescribed format provided in [Annexure J](#) within thirty days of issuing the purchase order/letter of intent.

33. Indemnity

- 33.1. Bidder shall indemnify, protect and save the Bank and hold the Bank harmless from and against all claims, losses, costs, damages, expenses, action suits and other proceedings, (including reasonable attorney fees), relating to or resulting directly or indirectly from
 - 33.1.1. an act or omission of the Bidder, its employees, its agents, or employees of the consortium in the performance of the services provided by this contract,
 - 33.1.2. breach of any of the terms of this RFP or breach of any representation or warranty by the Bidder
 - 33.1.3. use of the deliverables and or services provided by the Bidder,
 - 33.1.4. Infringement of any patent trademarks copyrights etc. or such other statutory infringements in respect of all components provided to fulfill the scope of this project. Bidder shall further indemnify the Bank against any loss or damage to the Bank's premises or property, Bank's data, direct financial loss, loss of life, etc., due to the acts of the Bidder's employees or representatives. The Bidder shall further indemnify the Bank against any loss or damage arising out of loss of data, claims of infringement of third- party copyright, patents, or other intellectual property, and third-party claims on the Bank for malfunctioning of the equipment or software or deliverables at all points of time, provided however,

- 33.1.4.1 The Bank notifies the bidder in writing in a reasonable time frame on being aware of such claim,
- 33.1.4.2 The Bidder has sole control of defense and all related settlement negotiations,
- 33.1.4.3 The Bank provides the Bidder with the assistance, information and authority as it deems fit to perform the above.
- 33.2. It is clarified that the bidder shall in no event enter into a settlement, compromise or makes any statement (including failure to take appropriate steps) that may be detrimental to the Bank's (and/or its customers, users and service providers) rights, interest and reputation.
- 33.3. Bidder shall be responsible for any loss of data, loss of life, etc. due to acts of Bidder's representatives, and not just arising out of gross negligence or misconduct, etc. as such liabilities pose significant risk.
- 33.4. Bidder should take full responsibility for its and its employee's actions. Further, since the Bank's data could be integrated / used under Bidder provided software, the Bidder should be responsible for loss/compromise or damage to Bank's data and for causing reputation risk to bank.
- 33.5. The bidders should indemnify the Bank (including its employees, directors or representatives) from and against claims, losses, liabilities, penalties, fines and suits arising from:
 - 33.5.1. IP infringement under any laws including Copyrights Act 1957 & IT Act 2000 and such other statutory acts and amendments thereto.
 - 33.5.2. Negligence and misconduct of the Bidder, its employees, and agents.
 - 33.5.3. Breach of any terms of RFP, Representation or Warranty.
 - 33.5.4. Act or omission in performance of service.
 - 33.5.5. Loss of data due to any of the reasons mentioned above.
 - 33.5.6. Non-compliance of the bidder with Laws/Governmental /regulatory Requirements
- 33.6. In the event that the Bank is called as a defendant for IPR infringement of patent, trademark or industrial design rights arising from use of any of the components of the supplied solution, the Bidder on its own expense will undertake to defend the Bank.
- 33.7. It will be the Bidder's responsibility to rapidly do away with such third-party claims. The Bidder will also pay any compensation arising from the infringement claims and the Bank will in no manner be responsible for such payments. In addition, the Bidder will bear all the related expenses and legal fees.
- 33.8. On its part, the Bank will immediately relay to the Bidder any such claims and offer assistance within reasonable limits to rid the claim.
- 33.9. The Bidder must undertake to indemnify that all the components delivered are free of defects, are brand new and original. If at some stage it is discovered that the components do not meet these criteria, the Bank has the right to cancel the order and the Bidder will have to refund the total amount received from the Bank along with the interest and separate penalties. Similar conditions apply to software; as well the system software must be licensed and original.

34. Intellectual Property Rights

The Bidder claims and represents that it has obtained appropriate rights to

provide the Deliverables and Services upon the terms and conditions contained in this RFP.

- 34.1 The Bidder shall be responsible at its own cost for obtaining all necessary authorizations and consents from third party licensors of Software used by Bidder in performing its obligations under this Project.
- 34.2 If a third party's claim endangers or disrupts the Bank's use of the Deliverables, the Bidder shall at no further expense, charge, fee or cost to the Bank, (i) obtain a license so that the Bank may continue use of the Deliverables in accordance with the terms of this RFP.
- 34.3 Bidder shall indemnify and keep fully and effectively indemnified the Bank from all legal actions, claims, or damages from third parties arising out of use of software, designs or processes used by Bidder or his subcontractors or in respect of any other services rendered under this RFP.

35. Non-Transferable Offer

This Request for Proposal (RFP) is not transferable. Only the bidder who has submitted the bid will be eligible for participation in the evaluation process.

36. Responsibility for Completeness

Any supplies and services, which might not have been specifically mentioned in this tender but, are necessary for the installation, Configuration, testing, commissioning, performance or completeness of the order, shall be provided / made available as per the time schedule for smooth and efficient operation and maintenance of the system under Indian conditions.

The bidder shall be responsible for any discrepancies, errors and omissions in the technical details submitted by him/them, irrespective of whether these have been approved, reviewed or otherwise, accepted by the Bank or not. The Bidder shall take all corrective measures arising out of discrepancies, errors and omissions in drawing and other information as mentioned above within the time schedule and without extra cost to the Bank.

37. Audit

The Bidder shall at all times whenever required furnish all information, records, data stored in whatsoever form to internal, external, Bank appointed and statutory/RBI inspecting auditors and extend full cooperation in carrying out of such inspection. The Bidder will also undertake to co-operate with the RBI to carry out its supervisory functions and objectives and will furnish all records and other information as RBI may call for to carry out inspection and/or other functions. The Bidder is required to facilitate the same at no additional cost and shall provide uninterrupted access to the documents required by the auditors. Further the Bidder has to ensure rectification of all the irregularities thus pointed out by the auditor within a given time frame.

The bidder has to ensure compliance of Information Security according to policy of the Bank and mitigate the risk, if any, within the stipulated time without any additional cost to Bank.

In line of above, the selected bidder shall ensure that all regulatory, Statutory, Local Administration requirements are adhered to subsequently while undertaking deliverable and

services over the period of contract without any additional cost to Bank.

Compliance with security best practices may be monitored by periodic computer/information security audit performed by or on behalf of the Bank. The periodicity of these audits will be decided at the discretion of the Bank. These audit plan to include, but are not limited to, a review of: access and authorization procedures, physical security controls, input/output controls, DB controls, backup and recovery procedures, network security controls and program change controls.

To the extent that the Bank deems it necessary to carry out a program of inspection and audit to safeguard against threats and hazards to the confidentiality, integrity, and availability of data, the Bidder shall afford the Bank's representative access to the Bidder's facilities, installations, technical resources, operations, documentation, records, databases and personnel. The Bidder must provide the Bank access to various monitoring and performance measurement system (both manual and automated). The Bank has the right to get the monitoring and performance measurement systems (both manual and automated) audited without prior approval / notice to the bidder.

38. Force Majeure

Force Majeure is herein defined as any cause, which is beyond the control of the selected Bidders or the Bank as the case may be which they could not foresee or with a reasonable amount of diligence could not have foreseen and which substantially affect the performance of the Contract, such as:

- 38.1 Natural phenomena, including but not limited to floods, droughts, earthquakes, epidemics,
- 38.2 Acts of any Government, including but not limited to war, declared or undeclared, priorities, quarantines, embargoes,
- 38.3 Terrorist attacks, public unrest in work area;

Provided either party shall within ten (10) days from the occurrence of such a cause notify the other in writing of such causes. The Bidder or the Bank shall not be liable for delay in performing his/her obligations resulting from any Force Majeure cause as referred to and/or defined above.

39. Exit Clause

The Bank reserves the right to cancel /exit the contract with immediate effect in the event of happening one or more of the following conditions:

- 39.1 Failure of the successful bidder to accept the contract and furnish the Performance Bank Guarantee within 60 days from receipt of purchase contract.
- 39.2 Delay in delivery beyond the specified period
- 39.3 Delay in completing implementation/customization and acceptance tests/ checks beyond the specified periods;
- 39.4 Serious discrepancy in functionality to be provided or the performance levels which have an impact on the functioning of the solution

In addition to the cancellation of contract, Bank reserves the right to appropriate the damages through encashment of Bid Security /Performance Guarantee given by the Bidder. Bank reserves right to exit at any time after giving notice period of one month during the contract period.

40. Termination of Contract

If the Termination is on account of failure of the successful bidder to perform the obligations under this RFP contract, the Bank shall have the right to invoke the Performance Bank Guarantee(s) given by the selected bidders.

The Bank is entitled to terminate this Contract, without any cost to the Bank and recover expenditure incurred by Bank, on the happening of any one or more of the following by giving 30 days' notice:

- 40.1 The selected bidder commits a breach of any of the terms and conditions of the bid.
- 40.2 The Successful bidder goes into liquidation voluntarily or otherwise or facing/declared bankrupt/insolvent.
- 40.3 An attachment is levied or continues to be levied for a period of 7 days upon effects of the Agreement.
- 40.4 The progress regarding the execution of the order accepted by the selected bidder is found to be unsatisfactory or delay in execution of the contract, the Bank reserves the right to get the balance contract executed by another party of its choice by giving one month's notice for the same. In this event, the selected bidder is bound to make good the additional expenditure, which Bank may have to incur in executing the balance contract. This clause is applicable, if for any reason, the contract is cancelled.
- 40.5 Non-satisfactory performance of the selected bidder during implementation and operation.
- 40.6 An act of omission by the Bidder, its employees, its agents, or employees of the consortium in the performance of the services provided by this contract.
- 40.7 Failure to integrate/implement the Project as per the requirements of the Bank as stated in this RFP.
- 40.8 Material discrepancies in the Deliverables and Services noted in the implementation of the Project. Bank reserves the right to procure the same or similar product from the alternate sources at the risk, cost and responsibility of the selected bidder.
- 40.9 The average uptime of the "working time" in 3 (three) consecutive months of all together is less than 90%.
- 40.10 Selected bidder is found to be indulging in frauds.
- 40.11 The bank suffers a reputation loss on account of any activity of successful bidder penalty is levied by regulatory authority.
- 40.12 In the event of sub contract or assignment contrary to the terms of agreement.
- 40.13 The performance of NSI will be continuously reviewed by the Bank to maintain the terms & conditions as specified in this document. Based on the review, if the selected NSI fails to satisfy / maintain their commitment with respect to services viz. Uptime, Performance, Timely implementation of the project, SLA etc. the bank will give a cure period of 3 months to the NSI to improve their services. If NSI fails to improve their services after the escalations and cure period then contract may be terminated by giving 3 months' notice period. Bank's decision in this regard will be final.

40.14 In case of termination of this contract, the Bank shall have the right to avail services of any other bidder/ agency to continue the project without any let or hindrance from NSI and the NSI has to provide necessary help for smooth switch over.

40.15 In addition to the cancellation of purchase order/contract, Bank reserves the right to appropriate the bid security/performance Bank guarantee given by the vendor.

41. RFP Ownership

The RFP and all supporting documentation are the sole property of Union Bank of India and should NOT be redistributed without written consent of Union Bank of India. Violation of this would be breach of trust and may, inter-alia cause the bidders to be irrevocably disqualified. The aforementioned material must be returned to Union Bank of India on submitting the proposal, or upon request; however, bidders can retain one copy for reference.

42. Proposal Ownership

The proposal and all supporting documentation submitted by the bidders shall become the property of Union Bank of India unless the Bank agrees to the bidder's specific requests, in writing, the proposal and documentation to be returned.

43. Patents Rights

- 43.1. The supplier shall indemnify the Bank against all third party claims of infringement of patent, trademark or industrial design rights arising from use of the Goods, or any part thereof in India.
- 43.2. The supplier shall, at their own expense, defend and indemnify the Bank against all third party claims or infringement of intellectual Property Right, including Patent, trademark, copyright, trade secret or industrial design rights arising from use of the products or any part thereof in India or abroad.
- 43.3. The supplier shall expeditiously extinguish any such claims and shall have full rights to defend it there from. If the Bank is required to pay compensation to a third party resulting from such infringement, the supplier shall be fully responsible for, including all expenses and court and legal fees.
- 43.4. The Bank will give notice to the Supplier of any such claim without delay, provide reasonable assistance to the Supplier in disposing of the claim, and shall at no time admit to any liability for or express any intent to settle the claim.
- 43.5. The Supplier shall grant to the bank a fully paid-up, irrevocable, non-exclusive license throughout the territory of India or abroad to access, replicate and use software (and other software items) provided by the supplier, including-all inventions, designs and marks embodied therein in perpetuity.

44. Conflict of Interest

Bank requires that bidder provide professional, objective, and impartial advice and at all times hold Bank's interests paramount, strictly avoid conflicts with other Assignment(s)/ Job(s) or their own corporate interests and act without any expectations/ consideration for award of any future assignment(s) from Bank.

Bidder have an obligation to disclose any situation of actual or potential conflict in assignment/job, activities and relationships that impacts their capacity to serve the best

interest of Bank, or that may reasonably be perceived as having this effect. If the Bidder fails to disclose said situations and if Bank comes to know about any such situation at any time, it may lead to the disqualification of the Bidder during bidding process or the termination of its Contract during execution of assignment.

45. Disaster Recovery & Business Continuity Planning (BCP)

As a measure of contingency, the Bank has setup its Disaster Data Centre at Bengaluru. In case of failure of Central Data Centre located in Mumbai, it is expected that the operations will be carried out from the DRC. For this purpose, Bank has already installed servers and other equipment at the DRC to facilitate such operations. The vendors are expected to suggest suitable plans for implementing Disaster Recovery procedures for network operations and to ensure seamless shifting of network operations from Primary site to DR site in case of disasters. However, the finally selected vendor should draw out a detailed step-by-step disaster recovery plan and procedures for network operations which are required for ensuring smooth switchover from primary site to DR site and back from DR site to Primary site. The broad DR plan should inter-alia include the following.

- 45.1. The complete disaster recovery plan enumerating the technical aspects of seamlessly shifting the operations to DR site. This should include the routing plans through alternate/backup links to move the traffic to the DR servers.
- 45.2. The BCP should include stepwise procedures for declaration of disaster, entire escalation mechanism, roles and responsibilities defined for each of the team member and shifting the operations to DR site. The plan shall include prioritization of software and hardware replacement so that systems identified as 'critical' will be restored before less critical systems, wherever required. Time windows of these actions should be included. The BCP should include the DR plan for branch operations, ATM operation, Internet banking, Telebanking, Mobile banking and other centralized applications.
- 45.3. All the vendors participating in the tender should submit the BCP document, which is, accepted as best practice. Only the finally selected vendor will submit the final plan after studying the Bank's environment, infrastructure and business operations.
- 45.4. The vendor should supply, install and configure appropriate hardware, software etc., for best realization of such devised Disaster Recovery Plan so as to enable the Bank to continue to maintain its business operations during times of disaster.
- 45.5. Only the finally selected vendor along with Bank officials would be required to test the switching over activity as per BCP before acceptance of solution. The vendor should also conduct periodical drills (Mock tests) to ensure the BCP readiness once in six months.
- 45.6. It is expected that the finally selected vendor would undertake the above-mentioned activities for putting the DR & BCP plan in place within three months' time.
- 45.7. In case of disasters, the selected vendor should move the entire Network team to Bank's DR site at Bengaluru or to arrange competent technical team at DR site, Bengaluru to carry out the network management and monitoring till the main site is restored. The vendor should carry out this activity without any additional cost to the Bank.
- 45.8. The vendor should conduct training sessions on DR drills and provide detailed manuals on the same.

46. Network audit

- 46.1. During the tenure of the contract, the NSI shall conduct a network audit once in a year on the following aspects without any cost to the Bank:
- 46.1.1. To examine the health of the network by verifying the parameters such as link latency, CRC errors, link utilization during peak hours, version control of router OS and other network applications such as Centralized call switching device, ACS server etc.
 - 46.1.2. To identify the performance bottlenecks and to take suitable rectification steps, in consultation with the Bank and suggest measures for improvement.
- 46.2. The NSI will be responsible for configuration of the network devices as per the Bank's IT security policy. Bank can conduct the audit of the network as per RBI guidelines, if any or as per Bank's requirement through a third party or by Bank's Internal audit team on yearly basis. Vendor will be responsible for complying with all the audit observations.
- 46.3. Bank at its discretion may also appoint third party for auditing the activities of Services and operations of entire services provided to the BANK.
- 46.4. Bank or its regulator (i.e. Reserve Bank of India) reserves the right to audit the Bidder in terms of services offered by bidder.
- 46.5. Bidder's NOC facility center (Both Primary and DR Site) will be subject to audit by Bank, Bank's appointed consultant/auditor and Regulators/3rd Parties. Selected NSI will assist Bank in all such audit.

47. Technological Upgradation

Further, the bidder should upgrade equipments with the latest software versions as part of technological upgradation i.e., equipment OS upgradation/application upgradation etc., as and when required, without any additional cost so as to deliver the SLAs specified during the contract period. Bidder will sign up back-to-back contract with the OEM for regular upgrades.

48. End of Sale & End of Support

The Bidder will ensure that the stipulated Support and Maintenance facilities on the hardware/software will be available for a minimum period of 5 years. The vendor will constantly update the Bank on new technologies that could prove cost effective.

In case any solution/hardware/ software delivered as part of this RFP goes end of support/end of life during the contract period, the bidder has to upgrade/replace same without any cost to the Bank.

49. Tender/RFP Cancellation

The Bank reserves the right to cancel the Tender/RFP at any time without assigning any reasons whatsoever. In case of such cancellation the payment will be made to the extent of satisfactory delivery of products & services. The value of such payment shall be governed by completion certificates report and decision of Bank shall be final and binding on the bidder.

50. Compliance with Laws

Compliance with all applicable laws: The Bidder shall observe, adhere to, abide by, comply with and notify the Bank about all laws in force or as are or as made applicable in future, pertaining to or applicable to them, their business, their employees or their obligations towards them and all purposes of this RFP and shall indemnify, keep indemnified, hold harmless, defend and protect the Bank and its employees/officers/staff/personnel/representatives/agents from any failure or omission on its part to do so and against all claims or demands of liability and all consequences that may occur or arise for any default or failure on its part to conform or comply with the above and all other statutory obligations arising there from.

Compliance in obtaining approvals/permissions/licenses: The Bidder shall promptly and timely obtain all such consents, permissions, approvals, licenses, etc., as may be necessary or required for any of the purposes of this project or for the conduct of their own business under any applicable Law, Government Regulation/Guidelines and shall keep the same valid and in force during the term of the project, and in the event of any failure or omission to do so, shall indemnify, keep indemnified, hold harmless, defend, protect and fully compensate the Bank and its employees/ officers/ staff/ personnel/ representatives/agents from and against all claims or demands of liability and all consequences that may occur or arise for any default or failure on its part to conform or comply with the above and all other statutory obligations arising there from and the Bank will give notice of any such claim or demand of liability within reasonable time to the Bidder.

This indemnification is only a remedy for the Bank. The Bidder is not absolved from its responsibility of complying with the statutory obligations as specified above. Indemnity would exclude indirect, consequential and incidental damages. However, indemnity would cover damages, loss or liabilities suffered by the Bank arising out of claims made by its customers and/or regulatory authorities.

51. Information Ownership

All information processed, stored, or transmitted by Bidder equipment belongs to the Bank. By having the responsibility to maintain the equipment, the Bidder does not acquire implicit access rights to the information or rights to redistribute the information. The Bidder understands that civil, criminal, or administrative penalties may apply for failure to protect information appropriately.

This RFP document contains statements derived from information that is believed to be reliable at the date obtained but does not purport to provide all of the information that may be necessary or desirable to enable an intending Respondent to determine whether or not to enter into a contract or arrangement with Union Bank of India in relation to the provision of Contact Centre services. Neither Union Bank of India nor any of its employees, agents, contractors, or advisers gives any representation or warranty, express or implied as to the accuracy or completeness of any information or statement given or made in this RFP document.

52. Publicity

Any publicity by the Service Provider in which the name of the Bank is to be used, will be done only with the explicit written permission of the Bank.

53. Outsourcing Policy

The bidder shall adhere to the Bank's outsourcing policy and the standard terms and conditions for outsourcing attached to this RFP as [Annexure X](#) will be part and parcel of this agreement and in the event of any conflict between the terms and condition of the agreement, the terms and condition given in the standard terms and condition for outsourcing shall prevail.

54. Arbitration

All disputes and differences of any kind whatsoever arising out of or in connection with the purchase order shall be referred to arbitration. The arbitrator may be appointed by both the parties or in case of disagreement each party may appoint an arbitrator and such arbitrators shall appoint an Umpire before entering on the reference. The decision of the Umpire shall be final. Such arbitration shall be governed by the provisions of Indian Arbitration and Conciliation Act 1996. All arbitration proceedings shall be at Mumbai, Maharashtra State, India only.

55. Jurisdiction

Notwithstanding anything contained herein above, in case of any dispute, claim and legal action arising out of this RFP, the parties shall be subject to the jurisdiction of courts at Mumbai, Maharashtra State, India only.

56. Submission of Bids

The bidders have to submit bid through Online only and original document viz. Bid security, Cost of RFP and Integrity Pact should be submitted in physical form. All documents as per requirement of RFP must be uploaded on the site <https://ubi.abcprocure.com>. Original DD/BG for Cost of RFP, EMD and Integrity Pact (IP) must be submitted physically in sealed cover by dropping in tender box placed at reception at the following address on or before scheduled date and time.

To
The General Manager,
Union Bank of India,
Department of Information Technology,
Technology Centre, Adi Shankaracharya Marg,
Opposite Powai Lake, Powai,
Mumbai - 400072.

Bank may, at its discretion, extend this deadline for submission of bids by releasing corrigendum to this tender document.

57. Annexure A - Letter of Acceptance

(Letter to the bank on the bidder's letterhead)

To,

Union Bank of India
Technology Centre, 5th floor,
Adi Shankaracharya Marg,
Near Registrar of Shipping,
Powai, Andheri (East),
Mumbai-400072

Dear Sir,

Sub: Request for Proposal (RFP) for Network Management support services for Wide Area Network of the Bank

With reference to the above subject, having examined and understood the instructions, terms and conditions forming part of it, we hereby enclose our offer for the desired solution as detailed in your above referred RFP.

We further confirm that the offer is in conformity with the terms and conditions as mentioned in the RFP and all required information as mentioned is enclosed.

We also confirm that the offer shall remain valid for 180 days from the date of the offer.

We hereby undertake that supporting software supplied, if required will be licensed, legally obtained and with latest version.

We understand that the Bank is not bound to accept the offer either in part or in full and that the Bank has right to reject the RFP in full or in part without assigning any reasons whatsoever.

We understand that

- a. You are not bound to accept the lowest or any bid received by you, and you may reject all or any bid.
- b. If our Bid for the above job is accepted, we undertake to enter into and execute at our cost, when called upon by the Bank to do so, a contract in the prescribed form. Unless and until a formal contract is prepared and executed, this bid together with your written acceptance thereof shall constitute a binding contract between us.
- c. If our bid is accepted, we are to be responsible for the due performance of the contract.
- d. You may accept or entrust the entire work to one Bidder or divide the work to more than one Bidder without assigning any reason or giving any explanation whatsoever.
- e. Bidder means the bidder who is decided and declared so after examination of commercial bids.
- f. We enclose Demand Draft/Bank Guarantee for Rs.1,50,00,000/- (Rupees One Crore fifty lac only) favoring Union Bank of India and payable at Mumbai, towards bid security, details of the same is as under:

No. :

Date :

Name of Issuing Bank :

Dated at _____ this _____ day of _____ 2020

We hereby declare that all the information & Statements made in this RFP are true and accept that any misinterpretation contained in it may lead to our disqualification. We agree to all terms & conditions of the RFP.

Yours faithfully,

Date:

For _____

Signature _____

Name _____

Authorized Signatories
(Name & Designation, seal of the firm)

58. Annexure B - Bidder's Profile Format

Serial No.	Parameters	Response	
1	Name of the Firm/Company		
2	Year of Incorporation in India		
3	Names of the Partners/Directors		
4	Name and Address of the Principal Banker		
5	Addresses of Firm/Company		
	a) Head Office		
	b) Local Office in Mumbai and Bengaluru (if any)		
6	Authorized Contact person		
	a) Name and Designation		
	b) Telephone number/Mobile No.		
	c) E-mail ID.		
7	Financial parameters		
	Business Results (last three years)	Annual Turnover (Rs. In Crores)	Operating Profit (EBITDA Rs. In Crores)
	2018-19		
	2017-18		
	2016-17		
	(Only company figures need to be mentioned. Not to include group/subsidiary Company figures)	(Mention the above amount in INR only)	
8	Total number of certified professional permanent staff (please submit the curriculum vitae (CV) for the professional staff like Name, Key qualification, designation, experience, their domain etc. separately)		
9	Team composition and task assignment for the proposed assignment.		
10	Description of the methodology and activity (work) schedule for performing the assignment		
11	Number of banks / Financial Institutions to which this kind of services are being given.		
12	Name and address of the banks / financial institutions to whom this kind		

	of services was given with brief description, Location, etc.	
13	Number of other institutions to which this kind of services were given.	
14	Name and address of other institutions to whom this kind of services was given with brief description.	
15	PAN Number	
16	GST Number	
NOC Details		
17	Address	
18	Floor area in Sq ft	
19	Total no of engineers	
20	Name & Brief of Tools used for Monitoring, Reporting, Incident handling, Ticketing and Dashboard (with the version)	
21	Brief of Analytics Tool used (if any)	
22	Any other Certificates	

N.B. Enclose copies of Supporting document along with Audited Balance Sheet

Dated this..... Day of 2020

(Signature)

(In the capacity of)

Duly authorized to sign bid with seal for & on behalf of (Name & Address of the Bidder)

59. Annexure C - Eligibility Criteria

Sl. No.	Pre-Qualification Criteria	Compliance (Yes/No)	Detail of Proof Attached
1	The bidder has to submit Integrity Pact (IP) signed by authorized signatory as prescribed format mentioned in Annexure M on plain paper in advance (not prior to issuance of RFP) or at the time of bid submission. Bidder shall be liable for rejection in case of non-submission of the same.		Integrity Pact (IP) as per Annexure M
2	The bidder should be a registered/existing company under Company Act 1956/2013 or PSU/Government Organization/ partnership firm / LLP and should be in existence for last 5 years from the date of RFP.		Certificate of incorporation/certificate for commencement of business/other relevant documentary proof is to be submitted.
3	Bidder should have had a minimum annual turnover of Rs.300 Crores each during last three financial years i.e. 2016-17, 2017-18 & 2018-19. This must be the individual company turnover and not that of any group of companies. In case the audited financials for the year 2018-19 is not available, CA Certificate should be submitted.		Copies of the audited balance sheet and P&L Statement of the company showing the same is to be submitted.
4	The Bidder should have operating Profit (as EBITDA i.e. Earnings, Before Interest, Tax, Depreciation & Amortization) in the last three financial years i.e. 2016-17, 2017-18 & 2018-19. In case the audited financials for the year 2018-19 is not available, CA Certificate should be submitted.		Copies of the audited balance sheet and Profit/Loss statement of the company is to be submitted.
5	The OEMs of proposed SD-WAN, Switches, Routers & Unified Communication solution should have operating Profit (as EBITDA i.e. Earnings, Before Interest, Tax, Depreciation & Amortization) in the last three financial years i.e. 2016-17, 2017-18 & 2018-19.		Copies of the audited balance sheet and Profit/Loss statement of the company is to be submitted.
6	The bidder should have experience in setting up and/or maintaining a large wide area network based on MPLS/leased line in India (Minimum 1000 sites in one project) during last 5 years.		Letter/PO from user organization is to be submitted.
7	The bidder should have a fully operational Network Operation Center (NOC) in India for at least 5 years and must be providing 24*7*365 support to at least two corporate		Copy of certificate needs to be submitted.

	having minimum 3000 primary links between them. It is also to be noted that NOC must be ISO 27001:2013 certified. Bidder should also have BCP for NOC in place.		
8	The bidder must have employed minimum 100 certified network engineers in their organization payroll.		NSI to submit the details of network engineers employed by them with names and qualifications as per Annexure T
9	The bidder should have support infrastructure with minimum 25 own or franchisee logistical centers across India out of which at least one support infrastructure should be located in Uttar Pradesh, Karnataka and Andhra Pradesh/ Telangana each.		NSI to submit a list of own logistic centers along with full postal address, name of the center in-charge with telephone numbers.
10	Proposed SD-WAN Solution should be implemented with minimum 250 CPEs in India in one organization. The solution should be live with all SD-WAN components including but not limited to controller, Orchestrator, Analytics.		NSI/OEM needs to submit reference letter/Purchase Order/Sign-off from user organization.
11	Proposed OEM's Switch as part of the RFP should have a minimum installation base of 1500 in one Organization in India during last 5 years.		NSI/OEM needs to submit reference letter/Purchase Order/Sign-off from user organization.
12	Proposed Non-Video IP Phone as part of the RFP should have a minimum installation base of 1500 in one Organization in India during last 5 years.		NSI/OEM needs to submit reference letter/Purchase Order/Sign-off from user organization.
13	Proposed Network Performance Monitoring (NPM) Solution should have been deployed in two organization in India.		NSI/OEM needs to submit reference letter/Purchase Order/Sign
14	Proposed DNS, DHCP & IP Address Management (DDI) Solution should have been deployed in two organization in India.		NSI/OEM needs to submit reference letter/Purchase Order/Sign
15	Bidder should be either an Original Equipment Manufacturer (OEM) of devices/software solutions or authorized partner of OEM. In case the bidder is an Authorized partner of the OEM, Bidder needs to provide Manufacturer Authorization Form (MAF) from OEM stating that bidder is authorized partner of OEM and authorized to participate in this tender and in case the bidder is not able to perform obligations as per contract during the contract period, contracted services will be provided by OEM. OEM can quote directly or through authorized partners. However, both i.e. OEM & their authorized partner cannot		Manufacturer Authorization Form should be submitted.

	participate in the RFP. In case, both (OEM & his authorized partner) participate, only bid of the OEM will be considered.		
16	OEMs, whose hardware/software is proposed to be supplied to the Bank, must have presence in India and should be able to support the project in Mumbai & Bengaluru during contract period.		Document Proof should be submitted.
17	The companies or firms, bidding for the above tender, should have not been black listed by any of Government Authority or Public Sector Undertaking (PSUs). The bidder shall give an undertaking (on their letter head) that they have not been black listed by any of the Govt. Authority or PSUs. In case, in the past, the name of their Company was black listed by any of the Govt. Authority or PSUs, the same must have been removed from the black list as on date of submission of the tender, otherwise the bid will not be considered.		Undertaking on Company's letterhead as per Annexure H to be submitted by the bidder.

Note:

The Bidder must comply with all the above mentioned criteria. Non-compliance of any of the criteria will entail rejection of the offer summarily. The requirements mentioned above are mandatory. The cut-off date for the above criteria's will be the Date of submission of RFP.

Bidder should fulfill all the Eligibility criteria. Only those who fulfill all the eligibility criteria will qualify for further evaluation. Documents required to be submitted along with technical bid.

Photocopies of relevant documents / certificates as mentioned above in support of the claims made. The Bank reserves the right to verify / evaluate the claims made by the Bidder independently and can accept or reject without any explanation to the Bidder.

Reference Site Customer Name and Contact information to be provided to the Bank with whom discussion can be done.

Place:
Date:

Authorized Signatory:
Name & Designation:
Business Address & email id:

60. Annexure D - Compliance to RFP Terms & Conditions

Sl. No.	Clause Details	Bidder's Compliance (Yes/No)
1.	Introduction	
2.	Integrity Pact (IP)	
3.	Definition	
4.	Bank's Wide Area Network	
5.	Objectives of the RFP	
6.	Invitation of Tender Bids	
7.	Eligibility Criteria	
8.	Broad Scope of Work	
9.	Project Timelines (Delivery, Installation, Configuration and Integration)	
10.	Transition Period	
11.	Execution of Work	
12.	Compliance with IS Security Policy	
13.	Cost & Currency	
14.	Price Validity	
15.	Acceptance of Offer	
16.	Language of Bid	
17.	Instructions for Bid Submission	
18.	Award of Contract	
19.	Price Composition	
20.	Taxes and Duties	
21.	Rejection of Bid	
22.	Pre-Bid Meeting	
23.	Modification and Withdrawals of Bid	
24.	RFP Response	
25.	Payment Terms	
26.	Order Cancellation/ Termination of Contract	
27.	Contract Period	
28.	Liquidated Damages (LD)	
29.	Service Level Agreement	
30.	Authorized Signatory	
31.	Limitation of Liability	
32.	Confidentiality	
33.	Indemnity	
34.	Intellectual Property Rights	
35.	Non-Transferable Offer	
36.	Responsibility for Completeness	
37.	Audit	
38.	Force Majeure	
39.	Exit Clause	
40.	Termination of Contract	
41.	RFP Ownership	

42.	Proposal Ownership	
43.	Patents Rights	
44.	Conflict of Interest	
45.	Disaster Recovery & Business Continuity Planning (BCP)	
46.	Network audit	
47.	Technological Up gradation	
48.	End of Sale & End of Support	
49.	Tender/RFP Cancellation	
50.	Compliance with Laws	
51.	Information Ownership	
52.	Outsourcing Policy	
53.	Publicity	
54.	Arbitration	
55.	Jurisdiction	
56.	Submission of Bids	

Place:

Date:

Authorized Signatory: _

Name & Designation: _

Business Address & email id: _____

61. Annexure E - Technical Compliance

61.1. SD-WAN Central Solution

Sr. No.	Required Minimum Specification	Compliance (Yes / No)	Remarks
1.	The network should be implemented as true software defined network architecture with a centralized control plane residing in the software defined - Wide network controller also data Plane and control plane should be separate.		
2.	The solution components should include Centralized Network Orchestrator, Software Defined Network Controller, Analytic engine, Hub/gateway device running in central locations and edge devices running in the remote branch locations.		
3.	<p>The system should allow management of networks as software-defined network (SDN). Data and Control layers should clearly separate with control layer centralized.</p> <p><u>Control Plane:</u> Control plane is responsible to maintain centralized routing table, controls route advertisement as per policy, creates end to end segments on network, instruct data plane to change traffic flow as per policy.</p> <p><u>Data Plane:</u> Data plane is responsible to forward traffic in encrypted tunnels, apply local policy like QoS, ACL etc.</p>		
4.	All components of proposed solution should be in the form of Hardware Appliance and must be Rack Mountable with Dual Power Supply for DC, DR and NDC. For other locations, Hardware Appliance with 1U/2U form factor with single/dual power supply.		
5.	All the components of SD-WAN Suite need to be on-premises. None of the Bank's data should go to OEM cloud/premises for any reason.		
6.	The data plane at the branch locations, data center & DR should be programmable from the central software defined network controller.		
7.	The communication between the software defined network controller/Orchestrator/Analytic and the branch device running on the remote entity should be secure and encrypted.		
8.	The tunnel creation should be automatic & dynamic without any manual configuration on the edges and the controller.		
9.	The WAN path Selection at the branch locations should be based on the near real time analytics of the WAN Links Capacity & Quality (Packet loss, Latency & Jitter).		

10.	The WAN path selection should be dynamically selected based on the policy set from the network controller.		
11.	The architecture should allow for internet break out at the local at branch, centralized location, remote entity (remote location) based on the application and the policy defined in the software defined network controller.		
12.	The selection of WAN links to anchor the traffic flows for application traffic should be dynamic and policy driven.		
13.	It should be possible to have control and data communication on two different paths. For example, use only MPLS for edge device & controller communication and use internet & MPLS both for data communication.		
14.	The system architecture should allow the use the most preferred link based upon Link characteristics (Latency, Jitter, PLR) for critical applications as defined in policy		
15.	SD-WAN solution should support traffic forwarding on wan links based on SLA		
16.	The SD-WAN should be able to load balance across multiple links simultaneously (up to 4) and leverage the secondary link for spill-over if the bandwidth required for one session exceeds the available bandwidth on the best link. This lets high bandwidth applications have as much bandwidth as they need to perform optimally.		
17.	The SD-WAN should support SNMP V3 and/or Telemetry & NTP for monitoring and reporting purpose		
18.	The SD-WAN should support QoS features on edge branch devices on physical and sub-interfaces.		
19.	The SD-WAN solution must be able to apply QoS policies to all the traffic seen in network including TCP, UDP and other non-TCP traffic types.		
20.	SDWAN solution should support Forward error correction and packet duplication for real time applications like Voice and Video application experience optimization.		
21.	The SD-WAN device should be able to deploy In-line & Off-line mode		
22.	The SD-WAN should support IPv4 & IPv6 dual stack from day one		
23.	Appliance should support QoS, NAT, DHCP, DNS for IPv4 and IPv6		
24.	SD-WAN CPE must support DHCP helper address to forward DHCP request to central DHCP servers		
25.	The SD-WAN should support 802.1Q, sub-interface		

26.	SD-WAN should support PAP/ CHAP/ PIN based /any other industry standard authentication for 4G/4G LTE mode of connectivity.		
27.	The SD-WAN should support following IPv6 capability		
	IPv6 addressing architecture, IPv6 name resolution, IPv6 statics, IPv6 neighbor discovery		
	ICMPv6, IPv6 DHCP		
28.	Support for the following IPv6 features: OSPFv3, BGP Routing support for IPv6, IPv6 Dual Stack, IPv6Policy Based Routing, IPv6 QoS, NAT 64.		
29.	The system should allow creation of multiple end to end segments (up to 30) and per segment topology within network		
30.	The system should create per transport encryption keys to encrypt traffic.		
31.	The system should allow automated and policy driven refresh of the encryption key per virtual private network.		
32.	The system should allow time based refresh of the encryption key for each virtual private network.		
33.	The system should allow automatic/dynamic encrypted tunnels creation (without any manual configuring) between branch devices to enable branch to branch communication (Full Mesh/Partial Mesh).		
34.	The system should allow automatic/dynamic tunnels to be created without manually configuring any static overlays from branch devices to Hub locations.		
35.	The system should allow for Hub & Spoke, Partial Mesh, full mesh network topology. Bank at its discretion will deploy desired topology.		
36.	The system should allow for multiple hub destinations (at least 8 active Hub sites) to be created for application specific traffic using a policy defined for it. Traffic destined for a particular hub must be directly router towards that hub only.		
37.	The system should be automatically able to retrieve the network LAN information without running any separate peering protocols like BGP, OSPF on overlay WAN.		
38.	The system should ensure that any change in physical connectivity (change in service provider or IP address) does not require any change in virtual private network configuration in the controller or physical device at location.		
39.	The system should ensure that the virtual private network specific configuration is not to be attached to physical or logical WAN or LAN Links or IP addresses or physical interfaces on the		

	branch device.		
40.	The system should support GRE, IPSec encapsulation		
41.	The system should support the following authentication algorithms for Data Integrity:		
	a. SHA-512		
	b. SHA-384		
	c. SHA-256		
42.	The system should support the following encryption algorithms for Data Security		
	a. AES-256		
	b. Any other FIPS approved encryption		
43.	The Central components of SD-WAN including but not limited to Orchestrator, Controller, Analytic engine, Hub/gateway, or any other component should be scalable to support at least 12000 branches (Each branch having minimum 2 Link and having minimum two active tunnels to each 6 central location). Centralized hardware needs to be sized to handle 10000 branches (each with dual link) from Day-1. Additional hardware to cater future required shall be added later as per discretion of Bank.		
44.	The system should ensure that virtual private network configuration and policy is pre-formed in the controller. The addition of one or more branch devices in to the network should not require any changes in the virtual private network configuration in software defined network controller.		
Network Performance, Traffic Management & Path Steering			
45.	The system should be able to select the optimum path based on the network parameters like Latency, Jitter, packet loss and network capacity.		
46.	The system should be able to prioritize business critical applications and should prioritize this traffic over others during congestion.		
47.	The system should support end-to-end packet classification, marking, and bandwidth allocation.		
48.	The system should be able to automatically steer traffic flows to the optimum path, based on policy definition in the software defined network controller.		
49.	The system should always ensure granularity at a flow level while steering traffic to a given path.		
50.	The system should allow various traffic load balancing requirement like between equal and unequal bandwidth links,		

	application flow via specific link only etc.		
51.	The system should employ a centralized policy driven traffic management to steer traffic.		
52.	The system should ensure that the session is not impacted when switching between paths		
53.	The system should be able to provide a local internet break out for specific set of applications as configured in the policy while rest of internet bound applications are destined towards centralized hub.		
54.	The system should be able to support multiple internet break out points based on the application (e.g. The system should do a direct internet break out at the branch location for Microsoft Office 365 traffic while rest of the internet traffic should be egressed through a centralized security infrastructure in the data center or the cloud).		
55.	The SLA management should have fallback mechanism in place i.e. The traffic should flow to best path when all links cannot serve SLA to continue traffic flow.		
56.	The system should load balance the network traffic on per packet and/or per session based on the requirement of the Bank.		

Authentication, Authorization and Accounting (AAA)

57.	The central management system should authenticate and authorize every administrator/user accessing the Central/branch device using the central authentication solutions such as RADIUS/TACACS+		
58.	All the admin activities should be logged and stored for audit purpose		
59.	Solution should be sized for online storage of logs for minimum 90 days. Further historical logs should also be available on backup media for contract period. SI has to provide required backup solution along with tape media for same		

Security

60.	The solution should support deployment on SD-WAN Edge Device and provides consolidated SD-WAN and security capabilities without the need for additional hardware.		
61.	The solution should be able to Secures incoming and outgoing connections with Next Generation Threat Prevention solution including Firewall, IPS.		
62.	The system should implement a stateful firewall with Access Lists and/or Time based Access lists to provide supervision and control on the branch device that can be centrally provisioned and managed from the software defined network controller. All		

	their required license should be provided from Day-1.		
63.	The system should also provide Intrusion Prevention System (IPS) at all the branches with the ability to update the IPS signature database centrally from the software defined controller on a need basis or on a periodic basis.		
64.	The Solution should have consolidated logs view for Cyber Attack (Allow & Block both) for all the gateways		
65.	The Solution should support IOC sharing within all devices in case one device identified the threats.		
66.	The solution should be able to integrate with Security Information and Event Management (SIEM) solution to log forwarding.		
67.	The Solution should have Automated and centralized firmware updates and backups and setting security policy plans for common groups of SD-WAN Edge virtual security gateways (Firewall & IPS).		
68.	The SD-WAN should support DDoS mitigation functionality and protect DDOS attack like UDP Flood, Ping of Death etc.		
69.	SD-WAN Virtual Network Function Security Edge sends security logs to the central management & log server.		
70.	SD-WAN should comply with PCI DSS 3.2 requirements		
71.	The Solution should have pre-defined central reports to see Infected Hosts, Prevented Attacks, Detected Attacks and Attack Trends.		
72.	SD-WAN devices should have authentication and authorization only with the pre-configured Controller/Management server/Management Console which is placed in DC/DR.		
73.	There has to be minimum two factor authentication between Controllers and central and branch devices before they established communication with each other. Out of two factors, one factor has to be PKI (certificate). The communication between the software defined network controller and the branch device running on the remote entity should be secure and encrypted.		
74.	SD-WAN Devices should not communicate with cloud controller which is placed by the OEM in cloud. All the updates and operations should be carried from DC/DR Controller/Management server/Management Console.		
75.	It should possible to create end to end segmentation within network where traffic in different segment will be separated at layer 3 level. Segmentation should be done from central controller. Branch devices should support minimum 10 segments and DC/DR devices should support minimum 30 segments.		

76.	<p>From the central controller Bank must be able to fix the location of the SDWAN edge devices geographically based on the Latitude and Longitude position using GPS. If Latitude and Longitude of the mapped SDWAN device changes (precision 10m) at controller, then the SDWAN device should be disabled automatically from the central controller. Precision can be set for SDWAN device wise/location wise, and should not be only global parameter.</p> <p>OR</p> <p>SD-WAN devices should have capability to bind with any static hardware (i.e. switch, ATM etc.) MAC IDs available in the LAN at respective location. The Control/Management of MAC-ID binding and MAC-ID repository should be at central controller. The central controller/SDWAN device should probe the binded MAC-IDs for that SDWAN device on periodical basis/reboot/restart/power-on time. The SDWAN device should be automatically disabled if binded MAC IDs are Unrecognized/Unreachable by the SD-WAN device.</p> <p>OR</p> <p>SD-WAN devices should have capability to white-list devices (i.e. PC, NW Switch, ATM, Kiosk etc.) MAC IDs available in the LAN at respective location and SDWAN device should not allow access to any unrecognized/unknown MAC ID(s). The control/management of MAC-ID white-listing and MAC-ID repository should be at central controller.</p> <p>(The Bidders must be able to showcase the above feature during PoC)</p>		
Visibility, Analytics, Monitoring & Reporting			
77.	There should be one single centralized management console for SD-WAN solution irrespective of number of controllers, orchestrator, analytics, or any other Head-end devices installed to match Bank's scalability requirement.		
78.	The system should provide a mechanism to monitor the performance for Links and Virtual Private Network.		
79.	The system must be able to monitor ISP link parameters like link quality, link usage and link congestion and should be able to provide historical data on the same for a period of minimum 30 days		
80.	The system should support application-level monitoring and traffic control to improve business-critical application performance, facilitate capacity management and planning, and reduce network operating costs.		
81.	The system should be able to track the reliability and performance of WAN links.		
82.	The system should have the ability to provide visualization of traffic flows.		

83.	The system should support the ability to automatically detect applications, report the application traffic, and allow for marking and filtering via policy.		
84.	The system should allow to create/define custom application based on various parameters including but not limited to IP address, Port, etc		
85.	The system should be able to gather application and flow information		
86.	The system should show real time traffic on Web GUI interface		
87.	The system should support role based management		
88.	The system should actively measure the link capacity without impacting more than 10% of the capacity of the link to carry traffic.		
89.	The SD-WAN should have GUI (Graphical User Interface) for Report Generation		
90.	The SD-WAN controller should contain single dashboard which includes all other device status like CPU, Link status, event logs etc.		
91.	The SD-WAN should support granular Real-Time/near real time Monitoring and Historical Reporting like:		
92.	a. Statistic bandwidth usage of available links		
93.	b. Network statistics, including continuous performance monitoring of loss, latency, and packet ordering for all network paths and link utilization		
94.	The SD-WAN should be able to generate report for		
	a. Traffic statistics of all the included path		
	b. Specific application utilization		
	c. Path performance		
95.	The software defined controller must be able to monitor, and report top 10 applications by usage across all branch locations, in a branch locations along with the data rate and flow usage. This data must be stored by the controller for a minimum of 30 days.		
96.	The software defined controller must be able to monitor, and report top 10 applications by usage, Top 10 LAN user by bandwidth usage and applications accessed by them across all branch locations, in a branch locations along with the data rate and flow usage. This data must be stored by the controller for a minimum of 30 days.		
97.	The administration should be able to drill down these reports for troubleshooting. For e.g. application accessed by specific		

	users along with bandwidth consumed during defined amount of time.		
Management & Orchestration			
98.	The system should support a centralized single plane of management system to allow device configuration, policy provisioning, software updates and assurance capabilities for all component including security capabilities i.e. Firewall, IPS		
99.	The Solution should have simplified orchestration which should be placed in DC and DR site in HA for provisioning, automation to control and to push configuration for all the devices.		
100.	The solution should support management via CLI, Web GUI administration interface		
101.	Central Management Console to be provided in DC & DR in HA. Both DC and DR SD-WAN controllers should be in active-standby mode.		
102.	The DC and DR management console should have the capacity and Scalability to manage 12,000 edge devices with horizontal and vertical scalability		
103.	The system should support application visibility, application reporting, marking, filtering, and policy.		
104.	The system should provide a dashboard that provides state of appliances (Online, Offline, Not connected)		
105.	The system should support Zero Touch provision/minimum touch provisioning for Rapid site provisioning, Rapid deployment of new policies, configuration in a way that is secure and offers high performance.		
106.	The system should be able to notify external systems of events such as faults/alarms as Syslog messages, SNMP (SNMPv3) traps, Telemetry		
107.	The system must be able to send e-mail / SMS notification for events and alerts. The valid email addresses and numbers for receiving the SMS notifications should be configurable centrally.		
Network wide Policy Enforcement			
108.	The system should support centralized application of policies network wide or across subset of branch locations from the centralized software defined network controller.		
109.	The policy should include the traffic steering based on the WAN link type (MPLS, Internet, or any of the type of WAN link) available at the branch location.		
110.	The system should allow definition and enforcement of traffic forwarding policies that allow traffic to be forwarded to a particular site (branch), all sites (full mesh topology), hub		

	location (hub and spoke topology), at the same branch location or a to a custom location based on the traffic from specific subnet(s), to specific subnet(s) and custom IP Address(es) for traffic from LAN to WAN on a branch.		
111.	The system should allow definition and enforcement of WAN link load balancing policies that allow steering of application flows on a WAN link with best quality (flow based and packet-based load balancing) with the quality defined in terms of latency, packet loss and jitter.		
112.	The SD-WAN must integrate transparently into the existing routing infrastructure. The solution must be completely transparent to existing routing protocols (e.g. OSPF, BGP (iBGP and eBGP), IPSEC etc.). All routing functions, including "dynamic path selection" or any other network routing decisions		
Provisioning & Deployment			
113.	The system should allow for plug and play installation of branch devices without requiring any manual configuration or minimal manual configuration at the remote location		
114.	The system should allow automatic and centralized software, patch, version upgrades from the software defined network controller across all deployed devices in the branch offices, data center, NDC and DR. This including upgradation of all modules of SD-WAN including but not limited to Router, Firewall, IPS.		
115.	The system should allow for modular upgrade of the software running on the branch devices from the centralized software defined network controller in order conservatively use the bandwidth at the remote branch locations for software upgrades		
116.	The system should be available and running when the software is being downloaded in to the branch device from the central software defined controller.		
117.	The system should support software rollback		
118.	The system should allow for the automatic failover of the VPN tunnels to the disaster recovery data center from the branch if the data center is not reachable from the branch location or if the WAN connectivity to the Data Center is down or if the application hosted in the data center is not accessible.		
119.	DC and DR architecture for controllers and devices should be designed in redundant mode		
120.	Branch device should have simultaneous persistent connectivity to 6 Hub locations (DC, DR and NDCs) and traffic destined to one particular hub should directly be routed towered same.		

Software Defined Network (SDN) Controller

121.	The software defined controller must be able to scale minimum 12K branch locations. Hardware and license need to be provisioned for 6K devices from day-1.		
122.	Controller needs to be deployed in active-active or active-passive redundancy mode in DC and DR. Controller architecture needs to be flexible to create redundancy within DC and between DC and DR.		
123.	The software defined network controller must have REST APIs available for 3rd party integration or integration with custom automation tools		
124.	It should possible to scale controller architecture independently of data plane as per bank requirement		

License and Support

125.	The devices and software should be supported by the OEM on 24X7X365 basis through a global Technical Assistance Center (TAC).		
126.	The TAC support should be provided direct from OEM and not through any intermediate partner.		
127.	All the functionality and feature license should be pre-installed and it should be usable from day one of operation.		
128.	During the tenure, all the software/Patch/OS upgradation should be done by the Bidder/OEM with no Cost to Bank.		
129.	All the license part should be applied to all SD-WAN devices through central controller and not from cloud		
130.	Security features in devices should be from reputed OEMs which has their own security intelligence center and should able to provide periodic update/signatures without any cost to bank.		

61.2. SD-WAN hardware

61.2.1. SD-WAN Gateway appliance for DC, NDC and DR

Sr. No.	Required Minimum Specification	Compliance (Yes / No)	Remarks
1.	Appliance should able to connect in SD-WAN architecture and should meet requirements as per specification mentioned under SD-WAN		
2.	Appliance should have 4x10Gig and 8x1Gig Ethernet interface		
3.	Appliance should have separation of control and data plane		
4.	Appliance hardware should be scalable to support up to 10Gbps of encryption throughput		
5.	Appliance should support at least 1000000 IP routes		
6.	Device Should support minimum 30 segments/VRF/virtual domain for End to End Segmentation of traffic like - ATM, Corporate Users, Vendors		
7.	Appliance should support PPPoE		
8.	Appliance should support common routing protocols like Static, RIP, OSPFv3, BGPv4, Policy based routing, GRE, ECMP etc.		
9.	Should have AES-256 Standards. Should support IPSec with IKEv2 and PKI.		
10.	Shall have traffic load balancing capability on all available WAN Links based on based on advanced criteria, such as reachability, delay, loss, jitter and bandwidth utilization.		
11.	Appliance should support QoS on physical and sub interface, NAT, NAT64, DHCP, DNS for IPv4 and IPv6 traffic		
12.	Appliance should support Radius and/or TACACS+, SSHv2, SNMPv3 and/or Telemetry, Netflow/sflow/IPFix, Syslog		
13.	Appliance should support deep packet inspection to identify applications and should able to apply QoS based on application		
14.	Should be rack mountable and should come with rack mounting kit.		
15.	Appliance should be hardened appliance from OEM and should have capability to boot from OEM provided image only and not from non-standard/unauthorized software		
16.	Appliance should be IPv6 compatible from day-1		
17.	Appliance should be provided with redundant AC power supplies and power cords		
18.	Appliance should have minimum 10 Gbps SDWAN license (in each direction)		

61.2.2. SD-WAN CPE for RO/ZO and large branches

Sr. No.	Required Minimum Specification	Compliance (Yes / No)	Remarks
1.	Proposed appliance should able to connect in SD-WAN architecture and should meet requirements as per specification mentioned under SD-WAN		
2.	Proposed appliance should have modular architecture with 2x10/100/1000T WAN ports and 4x100/1000T LAN Ports. Device should also have two free slots for future scalability to support Gigabit Ethernet/3G/4G/LTE.		
3.	Appliance should have and support minimum 400 Concurrent IPSec tunnels		
4.	Appliance hardware should be scalable to support up to 300 Mbps of throughput with all services like IPSec, Firewall, IPS, URL filtering etc.		
5.	Appliance should support at least 100000 IP routes		
6.	Device Should support minimum 25 segments/VRF/virtual domain for End to End Segmentation of traffic like - ATM, Corporate Users		
7.	Appliance should support PPPoE, HDLC protocol		
8.	Appliance should support common routing protocols like Static, RIP, OSPFv3, BGPv4, Policy based routing, GRE, ECMP etc.		
9.	Should have AES-256 Standards. Should support IPSec with IKEv2 and PKI.		
10.	Shall have traffic load balancing capability on all available WAN Links based on based on advanced criteria, such as reachability, delay, loss, jitter and bandwidth utilization.		
11.	Appliance should support QoS on physical and sub interface, NAT, NAT64, DHCP, DNS for IPv4 and IPv6 traffic		
12.	Appliance should support Radius and TACACS+, SSHv2, SNMPv3/telemetry, Netflow/sflow/IPFix, Syslog		
13.	Appliance should support deep packet inspection to identify applications and should able to apply QoS based on application		
14.	Should be rack mountable and should come with rack mounting kit.		
15.	Appliance should be hardened appliance from OEM and should have capability to boot from OEM provided image only and not from non-standard/unauthorized software		
16.	Appliance should be IPv6 compatible from day-1		
17.	Appliance should be provided with AC power supply and Indian standard power cord		
18.	Appliance should have minimum 100 Mbps SDWAN license (in each direction)		

61.2.3. SD-WAN CPE for branch locations

Sr. No.	Required Minimum Specification	Compliance (Yes / No)	Remarks
1.	Proposed appliance should able to connect in SD-WAN architecture and should meet requirements as per specification mentioned under SD-WAN		
2.	Proposed appliance should have modular architecture with 2x10/100/1000T WAN ports and 4x100/1000T LAN Ports. Device should also have one free slot for future scalability to support Gigabit Ethernet/3G/4G/LTE.		
3.	Appliance should support minimum 100 concurrent IPSec tunnels		
4.	Appliance hardware should be scalable to support up to 50 Mbps of throughput with all services enabled like IPSec, Firewall, IPS, URL filtering etc.		
5.	Appliance should support at least 10000 IP routes		
6.	Should support minimum 10 segments/VRF/virtual domain for End to End Segmentation of traffic like - ATM , Corporate Users , Vendors		
7.	Appliance should support PPPoE, HDLC protocol		
8.	Appliance should support common routing protocols like Static, RIP, OSPFv3, BGPv4, Policy based routing, GRE, etc.		
9.	Should have AES-256 Standards. Should support IPSec with IKEv2 and PKI.		
10.	Shall have traffic load balancing capability on all available WAN Links based on based on advanced criteria, such as reachability, delay, loss, jitter and bandwidth utilization.		
11.	Appliance should support QoS on physical and sub interface, NAT, NAT64, DHCP, DNS for IPv4 and IPv6 traffic		
12.	Appliance should support Radius and/or TACACS+, SSHv2, SNMPv3/Telemetry, Netflow/sflow/IPFix, Syslog		
13.	Appliance should support deep packet inspection to identify applications and should able to apply QoS based on application		
14.	Should be rack mountable and should come with mounting kit.		
15.	Appliance should be hardened appliance from OEM and should have capability to boot from OEM provided image only and not from non-standard/unauthorized software		
16.	Appliance should be IPv6 compatible from day-1		
17.	Appliance should be provided with AC power supply and India Standard power cord		
18.	Appliance should have minimum 20 Mbps SD-WAN license (in each direction)		

61.3. Router

61.3.1. Router Type-1

Sr. No.	Required Minimum Specification	Compliance (Yes / No)	Remarks
1	The router should be modular in architecture to support variety of ports like 10Gig and 1Gig		
2	Router should have a separate data and control plane.		
3	The router must be able to support services like IPSec, NAT, multicast with high performance from day-1. All modules/license needs to be provided from day-1.		
4	Router should support a dedicated Processor for forwarding and encryption functions, independent of the Route Processor, capable of supporting at least 30Mpps.		
5	Route Processor should have at least 4 GB of DRAM to support large routing tables & other memory intensive processes.		
6	The router should support multiple 1Gig and 10Gig WAN ports		
7	The router must support minimum 10 Gbps of encryption throughput and 5000 IPSec tunnels from day-1 with no degraded performance for encrypted process.		
8	The router must support minimum 1000000 IPv4 and IPv6 routes		
9	The router should support 1000 unique ACL and 50000 Access control entries		
10	Preferable be a single chassis solution and be NEBS or equivalent compliant		
11	Should have status and health LEDs to diagnose system status on the front panel.		
12	All modules, fan trays & Power supplies should be hot swappable and must support online insertion and removal		
13	The router must be able to provide accessibility even if the primary route processor or supervisor is down.		
Support IPv6 feature			
14	IPv6 addressing architecture, IPv6 name resolution, IPv6 statistics		
15	IPv6 translation-transport packets between IPv6-only and IPv4-only endpoints		
16	ICMPv6, IPv6 DHCP		
18	Support for the following IPv6 features: RIP NG , OSPF v3 , BGP Support for V6, IP V6 Dual Stack, IP v6 Policy based Routing, and IP v6 QoS.		

19	Should support following IPv6 Tunneling mechanisms: Automatic 6 to 4 tunnels, Automatic IPv4 compatible tunnels, IPv6 over IPv4 GRE Tunnels, ISATAP Tunneling Support.		
Interface required			
21	The router should be populated with 8x10Gig SFP+ (Fully Populated) and 8x1Gig ports from day-1.		
High Availability			
22	Should have Fast software Upgrades while the router is in service		
23	The Router must support nonstop forwarding (NSF)		
24	Router should have redundant power supply from day-1		
25	Should have modular software images, so that each software process runs independent of the other thus allowing for higher stability. Should also support online upgrade of patches for specific processes without affecting traffic forwarding operations on the router.		
Network Protocol			
28	Should support RIPv2, OSPF, IS-IS and BGPv4 routing protocols, with support for all the features like OSPF on demand etc. & IP multicast routing protocols: PIM Version 2 (Sparse Mode & Dense Mode), IGMP v1, v2, v3		
29	Should have support for protocols like Multiprotocol Label Switching (MPLS) & Virtual Route Forwarding (VRF)		
Router Security			
30	Support of Standard Access Lists, Extended Access Lists and Time based Access lists		
31	NAT Support		
32	Hardware-accelerated 3DES for IPSec, Hardware-accelerated AES for IPSec		
33	Should be able to manage & administer point-to-point VPNs by actively pushing new security policies from a single head end to remote sites		
34	Should be able to build IPSec tunnel dynamically, point to point or point to Multipoint		
35	Should be able to secure large Layer 2 or MPLS networks requiring partial or full-mesh connectivity by forming IPsec VPN through centralized policy server		
36	Support for RADIUS/ TACACS+ for AAA functionality		
37	Control SNMP access through the use of SNMP V3 with MD5 authentication.		
38	Implement Access Lists on the router to ensure SNMP access only to the SNMP manager or the NMS workstation.		

39	Should support MD5 authentication for routing protocols.		
40	The router should support IPSec encryption for data confidentiality, with support for dedicated hardware modules to offload encryption processes from the CPU.		
41	IPSec implementation should be IETF compliant.		
Quality of service			
42	Weighted Fair Queuing (WFQ), Class-Based WFQ (CBWFQ),		
43	Class-Based Traffic Shaping (CBTS), Class-Based Traffic Policing (CBTP), Class-Based QoS MIB		
44	Support for Priority and custom queuing, Class-Based Weighted Random Early Detection (CBWRED)		
45	Support for RSVP, cRTP, DiffServ, QoS Pre-classification, Pre-fragmentation, Class-Based Marking (CBM)		
46	The router should be able to support IP precedence and also able to configure six classes of service		
47	Should be able to do accounting based on IP precedence		
48	The router should support congestion management techniques like RED and WRED.		
Management Features			
49	SNMP over IPV6 & AES & 3DES encryption support for SNMP Version 3		
50	Management should support: SSHv1, SSHv2, Simple Network Management Protocol (SNMPv3), CLI		
51	The router should support in-band and out of band management		
52	The router should be able to support multiple OS images for smoother up gradation		
53	Should support fine grained data collection including detail traffic statistics by protocol and IP address.		
54	All the proposed router must have all required licenses to achieve all above features from Day-1 of Hardware installation		

61.3.2. Router - Type 2

Sr. No.	Required Minimum Specification	Compliance (Yes / No)	Remarks
1.	The router should be modular in architecture with services-based hardware architecture.		
2.	Router should have a separate data and control plane.		
3.	The router must be able to support services like IPSec, NAT, multicast with high performance from day-1. All modules/license needs to be provided from day-1.		
4.	The router should have adequate DRAM, Flash Memory, CPU and other hardware to support all the services configured		
5.	The router should have adequate flash memory and other hardware to ensure storage of multiple router operating system images (minimum 2), configuration file backups, event logs etc.		
6.	Further, the router should have adequate memory, storage, processing power, other components so that router should be able to upgrade and patch the operating system till the end of life date without any additional hardware requirement such as flash memory, storage etc.		
7.	The router should support multiple variety of port including Ethernet, E1, PRI, Serial, etc		
8.	The router must support minimum 2 Gbps of encryption throughput and 1000 IPSec tunnels from day-1 with no degraded performance for encrypted process.		
9.	The router must support minimum 400000 IPv4 and IPv6 routes		
10.	The router should support 100 unique ACL and 5000 Access control entries		
11.	Preferable be a single chassis solution and be NEBS or equivalent compliant		
12.	Should have status and health LEDs to diagnose system status on the front panel.		
13.	All modules, fan trays & Power supplies should be hot swappable and must support online insertion and removal		
Support IPv6 feature			
14.	IPv6 addressing architecture, IPv6 name resolution, IPv6 statistics		
15.	IPv6 translation-transport packets between IPv6-only and IPv4-only endpoints		
16.	ICMPv6, IPv6 DHCP		

17.	Support for the following IPv6 features: RIP NG, OSPFv3, BGP Support for V6, IPv6 Dual Stack, IPv6 Policy based Routing, and IPv6 QoS.		
18.	Should support following IP v6 Tunneling mechanisms: Automatic 6 to 4 tunnels, Automatic IPv4 compatible tunnels, IPv6 over IPv4 GRE Tunnels, ISATAP Tunneling Support.		
Interface required			
19.	The router should be populated with 12 no. of 10/100/1000T port and 2 E1/T1 PRI ports from day-1.		
20.	Router should have 2 additional modules to future scalability apart from above mentioned ports		
High Availability			
21.	Should have Fast software Upgrades while the router is in service		
22.	The Router must support nonstop forwarding (NSF)		
23.	Router should have redundant power supply from day-1		
24.	Should have modular software images, so that each software process runs independent of the other thus allowing for higher stability. Should also support online upgrade of patches for specific processes without affecting traffic forwarding operations on the router.		
Network Protocol			
25.	Should support RIPv2, OSPF, IS-IS and BGPv4 routing protocols, with support for all the features like OSPF on demand etc.& IP multicast routing protocols: PIM Version 2 (Sparse Mode & Dense Mode), IGMPv1,v2,v3		
26.	Should have support for protocols like Multiprotocol Label Switching (MPLS) & Virtual Route Forwarding (VRF)		
Router Security			
27.	Support of Standard Access Lists, Extended Access Lists and Time based Access lists		
28.	NAT Support		
29.	Hardware-accelerated 3DES for IPSec, Hardware-accelerated AES for IPSec		
30.	Should be able to manage & administer point-to-point VPNs by actively pushing new security policies from a single head end to remote sites		
31.	Should be able to build IPSec tunnel dynamically, point to point or point to Multipoint		

32.	Should be able to secure large Layer 2 or MPLS networks requiring partial or full-mesh connectivity by forming IPsec VPN through centralize policy server		
33.	Support for RADIUS/ TACACS+ for AAA functionality		
34.	Control SNMP access through the use of SNMP V3 with MD5 authentication.		
35.	Implement Access Lists on the router to ensure SNMP access only to the SNMP manager or the NMS workstation.		
36.	Should support MD5 authentication for routing protocols.		
37.	The router should support IPsec encryption for data confidentiality, with support for dedicated hardware modules to offload encryption processes from the CPU.		
38.	IPSec implementation should be IETF compliant.		
Quality of service			
39.	Weighted Fair Queuing (WFQ), Class-Based WFQ (CBWFQ),		
40.	Class-Based Traffic Shaping (CBTS), Class-Based Traffic Policing (CBTP), Class-Based QoS MIB		
41.	Support for Priority and custom queuing, Class-Based Weighted Random Early Detection (CBWRED)		
42.	Support for RSVP, cRTP, DiffServ, QoS Preclassify & Pre-fragmentation, Class-Based Marking (CBM)		
43.	The router should be able to support IP precedence and also able to configure six classes of service		
44.	Should be able to do accounting based on IP precedence		
45.	The router should support congestion management techniques like RED and WRED.		
Management Features			
46.	SNMP over IPv6 & AES & 3DES encryption support for SNMPv3		
47.	Management should support: SSHv1, SSHv2, Simple Network Management Protocol (SNMPv3), CLI		
48.	The router should support in-band and out of band management		
49.	The router should be able to support multiple OS images for smoother up gradation		
50.	Should support fine grained data collection including detail traffic statistics by protocol and IP address.		
51.	All the proposed router must have all required licenses to achieve all above features from Day-1 of Hardware installation		

61.3.3. Router -Type 3

Sr. No	Interfaces:	Compliance (Yes / No)	Remarks
1.	Router should be populated with at least 2 numbers of WAN/L3/Routed Gig Ethernet Port (10/100/1000 Mbps), minimum 2 numbers of LAN Gig Ethernet Port (10/100/1000 Mbps).		
2.	Apart from above, the router should have at least One slots wherein bank can place any of the following cards: V.35 Serial interface card with minimum 1 serial interface GSM, 3G, 4G LTE SIM based Inbuilt card with antenna and 10-meter cable		
3.	Synchronous Serial Interface should support speeds up to 2 Mbps		
4.	Solution should be able to support Cellular WAN (4G LTE, GSM) interface for cellular multihoming without changing the base router along with the above supplied configuration. The router shall support 4G (LTE), 3G (HSPA+/HSPA) internal Module and should be able to display the Received Signal Strength, Current Channel, the MDN & MSID, the ESN Number/ SID/NID through CLI command model.		
5.	The router should have 4G LTE, 3G, GSM or Interface Detection and Noise Reduction feature for diversity signal capture		
6.	Solution should not use USB dongle for 4G/GSM/3G connectivity		
General Features			
7.	Router should have a minimum performance throughput of 32 Mbps or more with all services enabled and at least 24 Mbps throughput for IPSec		
8.	The router should have adequate DRAM, Flash Memory, CPU and other hardware to support all the services configured		
9.	The router should have adequate flash memory and other hardware to ensure storage of multiple router operating system images (minimum 2), configuration file backups, event logs etc.		
10.	Further, the router should have adequate memory, storage, processing power, other components so that router should be able to upgrade and patch the operating system till the end of life date without any additional hardware requirement such as flash memory, storage etc.		

11.	It must be possible to fast boot the router to ensure that software upgrades can be done with minimum network downtime.		
12.	Extensive debugging capabilities to assist in hardware problem resolution.		
13.	The router should be capable of IP routing protocols like RIPV1 & V2, OSPF, BGP-IBGP & EBGp, Policy routing, NAT etc.		
14.	The router should be capable of WAN protocols like PPP, Multilink PPP, etc.		
15.	Control SNMP access through the use of SNMP V3 with MD5/SHA-1, 2 authentication and Seamless integration with existing authentication services.		
16.	Implement Access Lists on the router to ensure SNMP access only to the SNMP manager or the NMS workstation.		
17.	The router should support multiple privilege levels to support role based access control even without use of external RADIUS or TACACS+		
18.	Support for Remote Authentication Dial-In User Service (RADIUS), TACACS+ and AAA.		
19.	MD5 Route Authentication.		
20.	PPP PAP & CHAP support		
21.	Should support ability to Layer 2 P2P (Point to point) or MPLS networks to provide full-mesh connectivity by providing tunnel-less VPN's, without any impact on the router performance		
22.	The router should be able to make use of dynamic routing adjustments based on criteria such as reachability, response time, packet loss, jitter, path availability, traffic load distribution, and cost minimization policies when doing path selection.		
23.	Router should support for sending logs to multiple centralized Syslog server for monitoring and audit trail		
24.	Router should provide remote logging for administration using: a. SSH V.2 b. CLI		
25.	Router should have capability to upgrade, patch the operating system automatically, manually and remotely		
Support IPv6 feature			
26.	The Device should be on the IPv6 compliant		

27.	IPv6 addressing architecture, IPv6 name resolution, IPv6 statistics		
28.	IPv6 translation-transport packets between IPv6-only and IPv4-only endpoints		
29.	ICMPv6, IPv6 DHCP		
30.	Support for the following IPv6 features: RIP NG, OSPFv3, BGP Support for V6, IPv6 Dual Stack, NAT64, IPv6 Policy based Routing, and IPv6 QoS.		
31.	Should support following IP v6 Tunneling mechanisms: Automatic 6 to 4 tunnels, Automatic IPv4 compatible tunnels, IPv6 over IPv4 GRE Tunnels, ISATAP Tunneling Support.		
Software Features:			
32.	The router should support at least 3,00,000 routes in the routing information base using any of the routing protocol including RIPv1 & V2, OSPF, BGP-IBGP & EBGp, policy routing, NAT etc.		
33.	Dynamic Host Control Protocol (DHCP) server/relay/client		
34.	Dynamic DNS Support		
35.	Support for 802.1q VLANs		
36.	Support for Multicast Routing Protocol -PIM Sparse Mode, PIM Sparse-Dense Mode, Auto route processing (Auto-RP).		
37.	Router should have the capability of holding multiple OS images to support resilience & easy rollbacks during the version upgrades etc. and should support in service software upgrade including: -Multiple System image -Multiple system configuration -Option of Configuration roll-back		
Security Features:			
38.	Support of Standard Access Lists, Extended Access Lists and Time based Access lists		
39.	NAT Support		

40.	The router should support IPSec Framework for Secured Data transfer with standard Suite B algorithms: a. IPSec Data Encapsulation AH and ESP b. Key Exchange : Internet Key Exchange (IKE), IKEv2, Pre-Shared Keys (PSK), Public Key Infrastructure PKI (X.509), RSA encrypted nonce etc. c. Encryption Algorithm: AES-256 and upcoming encryption algorithms also d. Authentication Algorithm: SHA1 and SHA2 e. Group: Diffie-Hellman (DH) Group 1, 2, 5, 14, 15,19 f. Different mode of communication: Tunnel mode and Transport mode g. Router should support minimum 20 IPSec tunnels		
41.	Router should support embedded hardware based IP SEC encryption and acceleration		
42.	IPSec AES-128/192/256 termination/initiation, IPSec pass through		
43.	Should be able to manage & administer point-to-point VPNs by actively pushing new security policies from a single head end to remote sites		
44.	Should be able to build IPSec tunnel dynamically, point to point or point to Multipoint		
45.	Should be able to secure large Layer 2 or MPLS networks requiring partial or full-mesh connectivity by forming IPsec VPN through centralize policy server		
46.	Support for RADIUS/ TACACS for AAA functionality		
QoS Features:			
47.	Support for Weighted Fair Queuing (WFQ), Support for IPSec QoS Pre classification & Pre-fragmentation, Class-Based Marking (CBM), Priority and custom queuing, Weighted Random Early Detection.		
48.	Class-Based Traffic Shaping (CBTS), Class-Based Traffic Policing (CBTP), Class-Based QoS MIB		
49.	Support for Priority and custom queuing, Class-Based Weighted Random Early Detection (CBWRED)		
50.	Support for RSVP, cRTP, DiffServ, QoS Pre classify & Pre-fragmentation, Class-Based Marking (CBM)		
51.	Router should support managing congested network connectivity using: a.TCP congestion protocol b. IP Precedence c. Ingress and Egress Rate limiting		
52.	Router should support hierarchical QoS for providing granular policy per application basis for providing bandwidth provisioning and management		

Management Features:

53.	Management should support: SSHv1, SSHv2, Simple Network Management Protocol (SNMPv1,2,3), CLI		
54.	SNMP over IPV6 & AES & 3DES encryption support for SNMP Version 3		
55.	Solution should have enterprise license without any restrictions. If during the contract, solution is not performing as per specifications in this RFP, bidder has to upgrade/enhance the devices or place additional devices and reconfigure the system without any cost to bank		

61.3.4. Router - Type - 4

Sr. No.	Interfaces/Descriptions	Compliance (Yes / No)	Remarks
1.	Router should be populated with at least 2 routed 10/100/10000 interfaces used for WAN, 2 numbers of LAN Gig Ethernet Port (10/100/1000 Mbps), 2 serial port & 2 E1/T1 PRI ports		
2.	Apart from above, the router should have at least One free slot wherein bank can place any of the module		
3.	Synchronous Serial Interface should support speeds up to 2 Mbps		
General Features			
4.	Router should have a minimum performance throughput of 32 Mbps or more with all services enabled including IPSec		
5.	The router should have adequate DRAM, Flash Memory, CPU and other hardware to support all the services configured		
6.	The router should have adequate flash memory and other hardware to ensure storage of multiple router operating system images (minimum 2), configuration file backups, event logs etc.		
7.	Further, the router should have adequate memory, storage, processing power, other components so that router should be able to upgrade and patch the operating system till the end of life date without any additional hardware requirement such as flash memory, storage etc.		
8.	It must be possible to fast boot the router to ensure that software upgrades can be done with minimum network downtime.		
9.	Extensive debugging capabilities to assist in hardware problem resolution.		
10.	The router should be capable of IP routing protocols like RIPV1 & V2, OSPF, BGP-IBGP & EBGp, Policy routing, NAT etc.		
11.	The router should be capable of WAN protocols like PPP, Multilink PPP, etc.		
12.	Control SNMP access through the use of SNMP V3 with MD5/SHA-1, 2 authentication and Seamless integration with existing authentication services.		
13.	Implement Access Lists on the router to ensure SNMP access only to the SNMP manager or the NMS workstation.		
14.	The router should support multiple privilege levels to		

	support role based access control even without use of external RADIUS or TACACS+		
15.	Support for Remote Authentication Dial-In User Service (RADIUS), TACACS+ and AAA.		
16.	MD5 Route Authentication.		
17.	PPP PAP & CHAP support		
18.	Should support ability to Layer 2 P2P (Point to point) or MPLS networks to provide full-mesh connectivity by providing tunnel-less VPN's, without any impact on the router performance		
19.	The router should be able to make use of dynamic routing adjustments based on criteria such as reachability, response time, packet loss, jitter, path availability, traffic load distribution, and cost minimization policies when doing path selection.		
20.	Router should support for sending logs to multiple centralized syslog server for monitoring and audit trail		
21.	Router should provide remote logging for administration using: a. Telnet b. SSH V.2 c. CLI		
22.	Router should have capability to upgrade, patch the operating system automatically, manually and remotely		
23.	The router should be capable of booting from a remote node, where the router image is present.		
24.	The router software must support the flash file system to easily store and load multiple images.		
25.	Extensive debugging capabilities to assist in hardware problem resolution.		
26.	The router should be capable of IP routing protocols like RIP, OSPF, OSPF on demand, policy routing, BGPv4.		
27.	The router should be capable of WAN protocols like PPP, Multilink PPP, etc.		
28.	Multiple Privilege Levels.		
29.	Dynamic Host Control Protocol (DHCP) server/relay/client		
30.	Dynamic DNS Support		
31.	Support for 802.1q VLANs		
32.	Support for Multicast Routing Protocol -PIM Sparse Mode, PIM Sparse-Dense Mode, Auto route processing (Auto-RP).		

33.	PPP PAP & CHAP support		
34.	Support IPv6 feature		
35.	The Device should be on the IPv6 compliant		
36.	IPv6 addressing architecture, IPv6 name resolution, IPv6 statistics		
37.	IPv6 translation-transport packets between IPv6-only and IPv4-only endpoints		
38.	ICMPv6, IPv6 DHCP		
39.	Support for the following IPv6 features: RIP NG, OSPFv3, BGP Support for V6, IPv6 Dual Stack, NAT64, IPv6 Policy based Routing, and IPv6 QoS.		
40.	Should support following IPv6 Tunneling mechanisms: Automatic 6 to 4 tunnels, Automatic IPv4 compatible tunnels, IPv6 over IPv4 GRE Tunnels, ISATAP Tunneling Support.		
Security Features:			
41.	Support of Standard Access Lists, Extended Access Lists and Time based Access lists		
42.	NAT Support		
43.	<p>The router should support IPSec Framework for Secured Data transfer with standard Suite B algorithms:</p> <ul style="list-style-type: none"> a. IPSec Data Encapsulation AH and ESP b. Key Exchange : Internet Key Exchange (IKE), IKEv2, Pre-Shared Keys (PSK), Public Key Infrastructure PKI (X.509), RSA encrypted nonce etc. c. Encryption Algorithm: AES-256 and upcoming encryption algorithms also d. Authentication Algorithm: SHA1 and SHA2 e. Group: Diffie-Hellman (DH) Group 1, 2, 5, 14, 15,19 f. Different mode of communication: Tunnel mode and Transport mode g. Router should support minimum 20 IPSec tunnels 		
44.	Router should support embedded hardware based IP SEC encryption and acceleration		
45.	IPSec AES-128/192/256 termination/initiation, IPSec pass through		
46.	Should be able to manage & administer point-to-point VPNs by actively pushing new security policies from a single head end to remote sites		
47.	Should be able to build IPSec tunnel dynamically, point to point or point to Multipoint		

48.	Should be able to secure large Layer 2 or MPLS networks requiring partial or full-mesh connectivity by forming IPsec VPN through centralize policy server		
49.	Support for RADIUS/ TACACS for AAA functionality		
QoS Features:			
50.	Support for Weighted Fair Queuing (WFQ), Support for IPSec QoS Pre classification & Pre-fragmentation, Class-Based Marking (CBM), Priority and custom queuing, Weighted Random Early Detection.		
51.	Class-Based Traffic Shaping (CBTS), Class-Based Traffic Policing (CBTP), Class-Based QoS MIB		
52.	Support for Priority and custom queuing, Class-Based Weighted Random Early Detection (CBWRED)		
53.	Support for RSVP, cRTP, DiffServ, QoS Preclassify & Pre-fragmentation, Class-Based Marking (CBM)		
54.	Router should support managing congested network connectivity using: a. TCP congestion protocol b. IP Precedence c. Ingress and Egress Rate limiting		
55.	Router should support hierarchical QoS for providing granular policy per application basis for providing bandwidth provisioning and management		
Management Features:			
56.	Management should support: SSHv1, SSHv2, Simple Network Management Protocol (SNMPv1,2,3), CLI		
57.	SNMP over IPV6 & AES & 3DES encryption support for SNMP Version 3		
58.	Solution should have enterprise license without any restrictions. If during the contract, solution is not performing as per specifications in this RFP, bidder has to upgrade/enhance the devices or place additional devices and reconfigure the system without any cost to bank		

61.4. Network Switch

61.4.1. Network Switch - Type 1 - 24 Ports/1G

Sr. No.	Required Minimum Specification	Compliance (Yes / No)	Remarks
1	Proposed switch should be Rack Mountable physical appliance and supplied with rack mounting kit		
2	24 RJ-45 autosensing 10/100/1000 ports and 2x1Gig Base-T uplink port		
3	The switch must have 1 dual-personality (RJ-45 or USB micro-B) serial console port		
4	Switch must have switching capacity of at least 52 Gbps		
5	The Switch must support 16000 MAC address		
6	The switch should have at least 41 Mpps forwarding rate.		
Quality of Service (QoS)			
7	The switch must support Traffic prioritization (IEEE 802.1p) to allow real-time traffic classification into eight priority levels mapped to eight queues		
8	The switch must support Layer 4 prioritization to enable prioritization based on TCP/UDP port numbers		
9	The switch must support Class of Service (CoS) to sets the IEEE 802.1p priority tag based on IP address, IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and DiffServ		
10	The switch must support Rate limiting to sets per-port ingress enforced maximums and per-port, per-queue minimums		
11	The switch must Provide congestion management		
Connectivity			
12	The switch must support Auto-MDIX to provide automatic adjustments for straight-through or crossover cables on 10/100/1000 ports		
IPv6 Feature			
13	The switch must support IPV6 host to enable switches to be managed in an IPV6 network		
14	The switch must support Dual stack (IPV4 and IPV6) to transition from IPV4 to IPV6, supporting connectivity for both protocols		
15	The switch must support MLD snooping to forward IPV6 multicast traffic to the appropriate interface		

16	The switch must support ACL with access control entries and QoS for IPv6 network traffic		
Convergence			
17	The switch must support LLDP-MED (Media Endpoint Discovery)		
18	The switch must support IEEE 802.1AB Link Layer Discovery Protocol (LLDP)		
19	The switch must support Local MAC Authentication		
Resiliency and high availability			
20	The switch must support IEEE 802.3ad link-aggregation-control protocol (LACP) and port trunking		
21	The switch must provide easy-to-configure link redundancy of active and standby links		
Monitoring & Management			
22	The switch must support SNMPv3		
23	The switch must support Zero-Touch Provisioning (ZTP)/Minimum Touch Provisioning with minimal manual configuration using proposed Centralized Network Management Tool		
24	Proposed switch must be able to integrate with proposed centralized network switch management tool for management and monitoring		
25	The switch must support onsite management platform to offer simple, secure, and cost-effective way to manage switches		
26	The switch must support Dual flash images		
27	The switch must allow assignment of descriptive names to ports		
28	The switch must have the capability to find and fixes common network problems automatically, then informs administrator		
29	The switch must allow multiple configuration files to be stored to a flash image		
30	The switch must support RMON and sFlow or Netflow or equivalent		
31	The switch must provide advanced monitoring and reporting capabilities for statistics, history, alarms, and events		
32	The switch must support ingress and egress port monitoring enable network problem solving		
33	The switch must support Unidirectional link detection (UDLD)		
34	Switch should identify phones on the port and should able to apply QoS automatically		
Layer 2 switching			

35	The switch must support IEEE 802.1Q (4094 VLAN IDs) and 256 VLANs simultaneously		
36	The switch must support Jumbo packet support		
37	The switch must allow automatic learning and dynamic assignment of VLANs		
38	The switch must support IEEE 802.1S, 802.1W and 802.1D standards to protect from STP loops		
Redundancy: -			
39	Link Aggregation		
40	Spanning Tree (802.1d) with support for spanning tree per VLAN		
41	Quick Failover over redundant links for improved network stability and reliability		
42	Support for IEEE rapid spanning tree.		
Security			
43	The switch must support IEEE 802.1X with radius change of authorization-CoA to have integration with NAC		
44	To support 802.1x network authentication and port security on a port basis which will help to deploy Network Access Control (NAC)		
	1. IEEE 802.1x		
	2. 802.1x with VLAN Assignment		
	3. 802.1x Guest VLAN		
	4. 802.1x - Auth-Fail VLAN or equivalent. (An auth fail VLAN allows users without valid credentials to access a limited set of services which can be controlled by an administrator. Please note that at present the Bank is using dACLs to achieve this functionality.)		
	5. 802.1x - Auth Fail Open or equivalent. (Auth Fail Open feature enables the administrator to apply a policy that allows users to have network access when the AAA server is unreachable.)		
	6. 802.1x with ACLs		
	7. 802.1x with Port Security		
	8. 802.1x Accounting		
	9. Web Authentication for Non-802.1x Clients		
	10. Multi Domain Authentication (802.1x for IP phone + 1 host behind phone)		
	11. Switch should support concurrent deployment of 802.1x and MAB authentication.		

45	The switch must support Web-based authentication		
46	The switch must support MAC-based authentication		
47	The switch must support Multiple IEEE 802.1X users per port		
48	The switch must support Concurrent IEEE 802.1X, Web, and MAC authentication schemes per port and accept up to 32 sessions of IEEE 802.1X, Web, and MAC authentications		
49	The switch must provide IP Layer 3 filtering based on source/destination IP address/subnet and source/destination TCP/UDP port number		
50	The switch must support RADIUS/TACACS+ for CLI administrator logging in		
51	The switch must support Secure shell protocol and Secure Sockets Layer (SSL)		
52	The switch must support Per-port broadcast throttling		
53	The switch must support Port security		
54	The switch must prevent particular configured MAC addresses from connecting to the network		
55	The switch must support Secure FTP		
56	The switch must support Identity-driven ACL with 250 Access Control Entries		
57	The switch must support STP BPDU port protection		
58	The switch must support DHCP protection		
59	The switch must support Dynamic ARP protection		
60	The switch must support STP root guard		
Other General Features			
61	Should support Link layer Discovery Protocol		
62	Secure access to switch management, limiting management applications from specific hosts only		
63	Should support BPDU guard to avoid topology loop.		
64	Unicast MAC filtering, unknown Unicast and multicast Port blocking		
65	The operating system should have a self-healing mechanism for the automatic recovery of the switch when a specified event occurs		
66	The software should have a mechanism to proactively detect and address potential hardware and software faults during runtime.		
67	Should have functionality to add new features like OS/Firmware upgrades from central location, etc.		

68	Support for Dynamic VLAN assignment should be supported to provide flexibility in assigning ports to VLANs.		
Environmental Features			
69	must support IEEE 802.3az Energy-efficient Ethernet (EEE) to reduce power consumption		
70	Operating temperature of 0°C to 45°C		
71	Safety and Emission standards including EN 60950; IEC 60950; VCCI Class A; FCC Class A		

61.4.2. Network Switch- Type 2- 24 Port/1G/POE+

Sr. No.	Required Minimum Specification	Compliance (Yes / No)	Remarks
1.	Proposed switch should be Rack Mountable physical appliance and supplied with rack mounting kit		
2.	24 RJ-45 autosensing 10/100/1000 ports and 2x1Gig Base-T port for uplink.		
3.	The switch must have 1 dual-personality (RJ-45 or USB micro-B) serial console port		
4.	The switch should support POE, POE+ on 24 ports		
5.	Switch must have switching capacity of at least 52 Gbps		
6.	The Switch must support 16000 MAC address		
7.	The switch should have at least 41 Mpps forwarding rate.		
Quality of Service (QoS)			
8.	The switch must support Traffic prioritization (IEEE 802.1p) to allow real-time traffic classification into eight priority levels mapped to eight queues		
9.	The switch must support Layer 4 prioritization to enable prioritization based on TCP/UDP port numbers		
10.	The switch must support Class of Service (CoS) to sets the IEEE 802.1p priority tag based on IP address, IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and DiffServ		
11.	The switch must support Rate limiting to sets per-port ingress enforced maximums and per-port, per-queue minimums		
12.	The switch must Provide congestion management		
Connectivity			
13.	The switch must support Auto-MDIX to provide automatic adjustments for straight-through or crossover cables on 10/100/1000 ports		
IPv6 Feature			
14.	The switch must support IPV6 host to enable switches to be managed in an IPv6 network		
15.	The switch must support Dual stack (IPV4 and IPV6) to transition from IPv4 to IPv6, supporting connectivity for both protocols		
16.	The switch must support MLD snooping to forward IPv6 multicast traffic to the appropriate interface		
17.	The switch must support ACL with access control entries and QoS for IPv6 network traffic		

Convergence			
18.	The switch must support LLDP-MED (Media Endpoint Discovery)		
19.	The switch must support IEEE 802.1AB Link Layer Discovery Protocol (LLDP)		
20.	The switch must support Local MAC Authentication		
Resiliency and high availability			
21.	The switch must support IEEE 802.3ad link-aggregation-control protocol (LACP) and port trunking		
22.	The switch must provide easy-to-configure link redundancy of active and standby links		
Monitoring & Management			
23.	The switch must support SNMPv3		
24.	The switch must support Zero-Touch Provisioning (ZTP)/Minimum Touch Provisioning with minimal manual configuration		
25.	Proposed switch must be able to integrate with proposed centralized network switch management tool for management and monitoring		
26.	The switch must support onsite management platform to offer simple, secure, and cost effective way to manage switches		
27.	The switch must support Dual flash images		
28.	The switch must allow assignment of descriptive names to ports		
29.	The switch must have the capability to find and fixes common network problems automatically, then informs administrator		
30.	The switch must allow multiple configuration files to be stored to a flash image		
31.	The switch must support RMON and sFlow or Netflow or equivalent		
32.	The switch must provide advanced monitoring and reporting capabilities for statistics, history, alarms, and events		
33.	The switch must support ingress and egress port monitoring enable network problem solving		
34.	The switch must support Unidirectional link detection (UDLD)		
35.	Switch should identify phones on the port and should able to apply QoS automatically		
Layer 2 switching			
36.	The switch must support IEEE 802.1Q (4094 VLAN IDs) and 256 VLANs simultaneously		

37.	The switch must support Jumbo packet support		
38.	The switch must allow automatic learning and dynamic assignment of VLANs		
39.	The switch must support IEEE 802.1S, 802.1W and 802.1D standards to protect from STP loops		
Redundancy: -			
40.	Link Aggregation		
41.	Spanning Tree (802.1d) with support for spanning tree per VLAN		
42.	Quick Failover over redundant links for improved network stability and reliability		
43.	Support for IEEE rapid spanning tree.		
Security			
44.	The switch must support IEEE 802.1X with radius change of authorization-CoA to have integration with NAC		
45.	To support 802.1x network authentication and port security on a port basis which will help to deploy Network Access Control (NAC)		
	1. IEEE 802.1x		
	2. 802.1x with VLAN Assignment		
	3. 802.1x Guest VLAN		
	4. 802.1x - Auth-Fail VLAN or equivalent. (An auth fail VLAN allows users without valid credentials to access a limited set of services which can be controlled by an administrator. Please note that at present the Bank is using dACLs to achieve this functionality.)		
	5. 802.1x - Auth Fail Open or equivalent. (Auth Fail Open feature enables the administrator to apply a policy that allows users to have network access when the AAA server is unreachable.)		
	6. 802.1x with ACLs		
	7. 802.1x with Port Security		
	8. 802.1x Accounting		
	9. Web Authentication for Non 802.1x Clients		
	10. Multi Domain Authentication (802.1x for IP phone + 1 host behind phone)		
	11. Switch should support concurrent deployment of 802.1x and MAB authentication.		
46.	The switch must support Web-based authentication		

47.	The switch must support MAC-based authentication		
48.	The switch must support Multiple IEEE 802.1X users per port		
49.	The switch must support Concurrent IEEE 802.1X, Web, and MAC authentication schemes per port and accept up to 32 sessions of IEEE 802.1X, Web, and MAC authentications		
50.	The switch must provide IP Layer 3 filtering based on source/destination IP address/subnet and source/destination TCP/UDP port number		
51.	The switch must support RADIUS/TACACS+ for CLI administrator logging in		
52.	The switch must support Secure shell protocol and Secure Sockets Layer (SSL)		
53.	The switch must support Per-port broadcast throttling		
54.	The switch must support Port security		
55.	The switch must prevent particular configured MAC addresses from connecting to the network		
56.	The switch must support Secure FTP		
57.	The switch must support Identity-driven ACL with 250 Access Control Entries		
58.	The switch must support STP BPDU port protection		
59.	The switch must support DHCP protection		
60.	The switch must support Dynamic ARP protection		
61.	The switch must support STP root guard		
Other General Features			
62.	Should support Link layer Discovery Protocol		
63.	Secure access to switch management, limiting management applications from specific hosts only		
64.	Should support BPDU guard to avoid topology loop.		
65.	Unicast MAC filtering, unknown Unicast and multicast Port blocking		
66.	The operating system should have a self healing mechanism for the automatic recovery of the switch when a specified event occurs		
67.	The software should have a mechanism to proactively detect and address potential hardware and software faults during runtime.		
68.	Should have functionality to add new features like OS/Firmware upgrades from central location, etc.		

69.	Support for Dynamic VLAN assignment should be supported to provide flexibility in assigning ports to VLANs.		
Environmental Features			
70.	must support IEEE 802.3az Energy-efficient Ethernet (EEE) to reduce power consumption		
71.	Operating temperature of 0°C to 45°C		
72.	Safety and Emission standards including EN 60950; IEC 60950; VCCI Class A; FCC Class A		

61.4.3. Network Switch- Type 3- 48 Port/1G/POE+

Sr. No.	Required Minimum Specification	Compliance (Yes / No)	Remarks
1	Proposed switch should be Rack Mountable physical appliance and supplied with rack mounting kit		
2	Switch should have minimum 48 10/100/1000 Base-T ports. with additional 2 Nos. Populated of 10G SFP+ Based ports for uplink connectivity and 2 stacking ports with all accessories for stacking purpose		
3	The switch must have 1 dual-personality (RJ-45 or USB micro-B) serial console port		
4	The switch should support POE, POE+ on all 48 ports		
5	Switch must have switching capacity of at least 128 Gbps		
6	The Switch must support 16000 MAC address		
7	Proposed switch should support stacking		
8	The switch should have at least 65 Mpps forwarding rate.		
Quality of Service (QoS)			
9	The switch must support Traffic prioritization (IEEE 802.1p) to allow real-time traffic classification into eight priority levels mapped to eight queues		
10	The switch must support Layer 4 prioritization to enable prioritization based on TCP/UDP port numbers		
11	The switch must support Class of Service (CoS) to sets the IEEE 802.1p priority tag based on IP address, IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and DiffServ		
12	The switch must support Rate limiting to sets per-port ingress enforced maximums and per-port, per-queue minimums		
13	The switch must Provide congestion management		
Connectivity			
14	The switch must support Auto-MDIX to provide automatic adjustments for straight-through or crossover cables on 10/100/1000 ports		
IPv6 Feature			
15	The switch must support IPV6 host to enable switches to be managed in an IPv6 network		
16	The switch must support Dual stack (IPV4 and IPV6) to transition from IPV4 to IPV6, supporting connectivity for both protocols		
17	The switch must support MLD snooping to forward IPv6 multicast		

	traffic to the appropriate interface		
18	The switch must support ACL with access control entries and QoS for IPv6 network traffic		
Convergence			
19	The switch must support LLDP-MED (Media Endpoint Discovery)		
20	The switch must support IEEE 802.1AB Link Layer Discovery Protocol (LLDP)		
21	The switch must support Local MAC Authentication		
Resiliency and high availability			
22	The switch must support IEEE 802.3ad link-aggregation-control protocol (LACP) and port trunking		
23	The switch must provide easy-to-configure link redundancy of active and standby links		
Monitoring & Management			
24	The switch must support SNMPv3		
25	The switch must support Zero-Touch Provisioning (ZTP)/Minimum touch provisioning using proposed Centralized Network Management Tool		
26	Proposed switch must be able to integrate with proposed centralized management tool		
27	The switch must support onsite management platform to offer simple, secure, and cost effective way to manage switches		
28	The switch must support Dual flash images		
29	The switch must allow assignment of descriptive names to ports		
30	The switch must have the capability to find and fixes common network problems automatically, then informs administrator		
31	The switch must allow multiple configuration files to be stored to a flash image		
32	The switch must support RMON and sFlow or Netflow or equivalent		
33	The switch must provide advanced monitoring and reporting capabilities for statistics, history, alarms, and events		
34	The switch must support ingress and egress port monitoring enable network problem solving		
35	The switch must support Unidirectional link detection (UDLD)		
36	Switch should identify phones on the port and should able to apply QoS automatically		
Layer 2 switching			

37	The switch must support IEEE 802.1Q (4094 VLAN IDs) and 512 VLANs simultaneously		
38	The switch must support Jumbo packet support		
39	The switch must allow automatic learning and dynamic assignment of VLANs		
40	The switch must support IEEE 802.1S, 802.1W and 802.1D standards to protect from STP loops		
Redundancy: -			
41	Link Aggregation across stack should be supported		
42	Spanning Tree (802.1d) with support for spanning tree per VLAN		
43	Quick Failover over redundant links for improved network stability and reliability		
44	Support for IEEE rapid spanning tree.		
Security			
45	The switch must support IEEE 802.1X with radius change of authorization-CoA to have integration with NAC		
	To support 802.1x network authentication and port security on a port basis which will help to deploy Network Access Control (NAC)		
	1. IEEE 802.1x		
	2. 802.1x with VLAN Assignment		
	3. 802.1x Guest VLAN		
	4. 802.1x - Auth-Fail VLAN or equivalent. (An auth fail VLAN allows users without valid credentials to access a limited set of services which can be controlled by an administrator. Please note that at present the Bank is using dACLs to achieve this functionality.)		
	5. 802.1x - Auth Fail Open or equivalent. (Auth Fail Open feature enables the administrator to apply a policy that allows users to have network access when the AAA server is unreachable.)		
	6. 802.1x with ACLs		
	7. 802.1x with Port Security		
	8. 802.1x Accounting		
	9. Web Authentication for Non 802.1x Clients		
	10. Multi Domain Authentication (802.1x for IP phone + 1 host behind phone)		
46	11. Switch should support concurrent deployment of 802.1x and MAB authentication.		

47	The switch must support Web-based authentication		
48	The switch must support MAC-based authentication		
49	The switch must support Multiple IEEE 802.1X users per port		
50	The switch must support Concurrent IEEE 802.1X, Web, and MAC authentication schemes per port and accept up to 32 sessions of IEEE 802.1X, Web, and MAC authentications		
51	The switch must provide IP Layer 3 filtering based on source/destination IP address/subnet and source/destination TCP/UDP port number		
52	The switch must support RADIUS/TACACS+ for CLI administrator logging in		
53	The switch must support Secure shell protocol and Secure Sockets Layer (SSL)		
54	The switch must support Per-port broadcast throttling		
55	The switch must support Port security		
56	The switch must prevent particular configured MAC addresses from connecting to the network		
57	The switch must support Secure FTP		
58	The switch must support Identity-driven ACL with 500 Access control entries		
59	The switch must support STP BPDU port protection		
60	The switch must support DHCP protection		
61	The switch must support Dynamic ARP protection		
62	The switch must support STP root guard		
Other General Features			
63	Should support Link layer Discovery Protocol		
64	Should Support DNS		
65	Secure access to switch management, limiting management applications from specific hosts only		
66	Should support BPDU guard to avoid topology loop.		
67	Unicast MAC filtering, unknown Unicast and multicast Port blocking		
68	The operating system should have a self-healing mechanism for the automatic recovery of the switch when a specified event occurs		
69	The software should have a mechanism to proactively detect and address potential hardware and software faults during runtime.		
70	Should have functionality to add new features like OS/Firmware		

	upgrades from central location, etc.		
71	Support for Dynamic VLAN assignment should be supported to provide flexibility in assigning ports to VLANs.		
Environmental Features			
72	must support IEEE 802.3az Energy-efficient Ethernet (EEE) to reduce power consumption		
73	Operating temperature of 0°C to 45°C		
74	Safety and Emission standards including EN 60950; IEC 60950; VCCI Class A; FCC Class A		

61.4.4. Network Switch - Type 4 - 48Port/10G/Base-T

Sr. No.	Required Minimum Specification	Compliance (Yes / No)	Remarks
1	The switch must have at least 48 fixed 1/10GbE (10GBASE-T) ports and 6 x QSFP+ ports populated with 4 nos. of 40G optics		
2	The switch must have 1.44 Tbps switching capacity		
3	The switch must have 64K MAC entries		
4	The switch must have Modular operating system		
5	The switch must have Distributed architecture with separation of data and control planes.		
6	The switch must have independent monitoring and restart of individual software modules, and enhanced software process serviceability functions.		
7	The switch must have individual software modules to be upgraded for higher availability.		
8	The switch must have built-in framework for monitoring, troubleshooting and capacity planning.		
9	The switch must support Jumbo frames size of 9K bytes		
10	The switch must support internal loopback testing for maintenance purposes and an increase in availability		
11	The switch must support Redundant and load-sharing fans, and power supplies. The switch should be supplied with Indian standard power cable		
12	The switch must support hot-swappable modules		
13	The switch must protect against unknown broadcast, unknown multicast, or unicast storms with user-defined thresholds		
14	The switch must support internal Redundant power supplies		
15	The Switch must have built-in tool for monitoring, troubleshooting and capacity planning and also provide automatic base-lining to automatically generate thresholds for alerts which eliminates manual configuration of thresholds.		
16	Packet buffer size of minimum 32 MB or higher		
Resiliency and high availability			
17	The switch must support MLAG or equivalent		

18	The switch must support Separate data and control paths		
19	The switch must support VRRP or HSRP		
20	The switch must support Unidirectional Link Detection (UDLD)		
21	The switch must support IEEE 802.3ad LACP with support up to 24 trunks and eight links per trunk		
22	The switch must support Generic Routing Encapsulation (GRE)		
23	The switch must support strict priority (SP) queuing and weighted fair queuing		
24	The switch must support VoQ technology or intelligent Buffering		
Management			
25	The switch must support automation and programmability using built-in REST APIs and Python scripts		
26	The switch must support built-in framework for monitoring, troubleshooting and capacity planning.		
27	The switch must support time series database to analyze trends, identify anomalies and predict future capacity requirements.		
28	The switch must have the capability to enable or disable console port, or reset button interfaces depending on security preferences		
29	The switch must support Industry-standard CLI		
30	The switch must restrict access to critical configuration commands and support multiple privilege levels with password protection		
31	The switch must provide SNMP read and trap support of industry standard Management Information Base (MIB), and private extensions		
32	The switch must support sFlow (RFC 3176) or Netflow or equivalent		
33	The switch must support Remote monitoring (RMON)		
34	The switch must support TFTP, and SFTP support		
35	The switch must support Debug and sampler utility		
36	The switch must support ping and traceroute for both IPv4 and IPv6		
37	The switch must support Network Time Protocol (NTP)		

38	The switch must support IEEE 802.1AB Link Layer Discovery Protocol (LLDP)		
39	The switch must support Multiple configuration files		
Layer 2 feature			
40	The switch must support up to 3500 port-based or IEEE 802.1Q-based VLANs and supports MAC-based VLANs, protocol-based VLANs, and IP-subnet-based VLANs		
41	The switch must support Port mirroring		
42	The switch must support IEEE 802.1D STP, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for faster convergence, and IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)		
43	The switch must support Internet Group Management Protocol (IGMP)		
44	The switch must support Rapid Per-VLAN spanning tree plus (RPVST+)		
45	The switch must support IGMPv1, v2, and v3 and support Any-Source Multicast (ASM)		
46	The switch must support congestion actions and support strict priority (SP) queuing and weighted fair queuing		
Layer 3 feature			
47	The switch must support Address Resolution Protocol (ARP) and supports static ARPs, gratuitous ARP to allows detection of duplicate IP addresses and proxy ARP		
48	The switch must support UDP helper		
49	The switch must support DHCP Relay		
50	The switch must support Multicast VLAN		
51	The switch must support Protocol Independent Multicast (PIM) and supports Sparse Mode (SM)		
52	The switch must support Static, Open shortest path first (OSPF), Border Gateway Protocol IPv4 routing		
53	The switch must support Static IPv6 routing, OSPFv3 and BGP-4		
54	The switch must support Dual IP stack		
55	The switch must support Equal-Cost Multipath (ECMP)		
Security			

56	The switch must support ACLs for both IPv4 and IPv6 based on a Layer 2 header or a Layer 3 protocol header		
57	The switch must support Remote Authentication Dial-In User Service (RADIUS)		
58	The switch must support Terminal Access Controller Access-Control System (TACACS+)		
59	The switch must support Secure shell (SSHv2)		
Environmental Features			
60	EN 60950		
61	IEC 60950-1:2005 Ed.2; Am 1:2009+A2:2013		
62	UL 60950-1, CSA 22.2 No 60950-1		
63	EN 50581:2012 (RoHS)		

61.4.5. Network switch - Type 5 - 48Port/10G/SFP+

Sr. No.	Required Minimum Specification	Compliance (Yes / No)	Remarks
1	The switch must have at least 48 fixed 1/10GbE (SFP+) ports and 6 x QSFP+ ports populated with 4 nos. of 40G optics		
2	The switch must have 1.44 Tbps switching capacity		
3	The switch must have 64K MAC entries		
4	The switch must have Modular operating system		
5	The switch must have Distributed architecture with separation of data and control planes.		
6	The switch must have independent monitoring and restart of individual software modules, and enhanced software process serviceability functions.		
7	The switch must have individual software modules to be upgraded for higher availability.		
8	The switch must have built-in framework for monitoring, troubleshooting and capacity planning.		
9	The switch must support Jumbo frames size of 9K bytes		
10	The switch must support internal loopback testing for maintenance purposes and an increase in availability		
11	The switch must support Redundant and load-sharing fans, and power supplies. The switch should be supplied with Indian standard power cable		
12	The switch must support hot-swappable modules		
13	The switch must protect against unknown broadcast, unknown multicast, or unicast storms with user-defined thresholds		
14	The switch must support internal Redundant power supplies		
15	The Switch must have built-in tool for monitoring, troubleshooting and capacity planning and also provide automatic base-lining to automatically generate thresholds for alerts which eliminates manual configuration of thresholds.		
16	Packet buffer size of minimum 12 MB or higher		
Resiliency and high availability			
17	The switch must support MLAG or equivalent		
18	The switch must support Separate data and control paths		

19	The switch must support VRRP or HSRP		
20	The switch must support Unidirectional Link Detection (UDLD)		
21	The switch must support IEEE 802.3ad LACP with support up to 24 trunks and eight links per trunk		
22	The switch must support Generic Routing Encapsulation (GRE)		
23	The switch must support strict priority (SP) queuing and weighted fair queuing		
24	The switch must support VoQ technology or intelligent Buffering		
Management			
25	The switch must support automation and programmability using built-in REST APIs and Python scripts		
26	The switch must support built-in framework for monitoring, troubleshooting and capacity planning.		
27	The switch must support time series database to analyze trends, identify anomalies and predict future capacity requirements.		
28	The switch must have the capability to enable or disable console port, or reset button interfaces depending on security preferences		
29	Proposed switch must be able to integrate with proposed centralized Network management tool		
30	The switch must support Industry-standard CLI		
31	The switch must restrict access to critical configuration commands and support multiple privilege levels with password protection		
32	The switch must provide SNMP read and trap support of industry standard Management Information Base (MIB), and private extensions		
33	The switch must support sFlow (RFC 3176) or Netflow or equivalent		
34	The switch must support Remote monitoring (RMON)		
35	The switch must support TFTP, and SFTP support		
36	The switch must support Debug and sampler utility		
37	The switch must support ping and traceroute for both IPv4 and IPv6		
38	The switch must support Network Time Protocol (NTP)		

39	The switch must support IEEE 802.1AB Link Layer Discovery Protocol (LLDP)		
40	The switch must support Multiple configuration files		
Layer 2 feature			
41	The switch must support minimum 3500 port-based or IEEE 802.1Q-based VLANs and supports MAC-based VLANs, protocol-based VLANs, and IP-subnet-based VLANs		
42	The switch must support Port mirroring		
43	The switch must support IEEE 802.1D STP, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for faster convergence, and IEEE 802.1s Multiple Spanning Tree Protocol (MSTP)		
44	The switch must support Internet Group Management Protocol (IGMP)		
45	The switch must support Rapid Per-VLAN spanning tree plus (RPVST+)		
46	The switch must support IGMPv1, v2, and v3 and support Any-Source Multicast (ASM)		
47	The switch must support congestion actions and support strict priority (SP) queuing and weighted fair queuing		
Layer 3 feature			
48	The switch must support Address Resolution Protocol (ARP) and supports static ARPs, gratuitous ARP to allows detection of duplicate IP addresses and proxy ARP		
49	The switch must support UDP helper		
50	The switch must support DHCP Relay		
51	The switch must support Multicast VLAN		
52	The switch must support Protocol Independent Multicast (PIM) and supports Sparse Mode (SM)		
53	The switch must support Static, Open shortest path first (OSPF), Border Gateway Protocol IPv4 routing		
54	The switch must support Static IPv6 routing, OSPFv3 and BGP-4		
55	The switch must support Dual IP stack		
56	The switch must support Equal-Cost Multipath (ECMP)		
	Security		
57	The switch must support ACLs for both IPv4 and IPv6 based on a Layer 2 header or a Layer 3 protocol header		
58	The switch must support Remote Authentication Dial-In		

	User Service (RADIUS)		
59	The switch must support Terminal Access Controller Access-Control System (TACACS+)		
60	The switch must support Secure shell (SSHv2)		
Environmental Features			
61	EN 60950		
62	IEC 60950-1:2005 Ed.2; Am 1:2009+A2:2013		
63	UL 60950-1, CSA 22.2 No 60950-1		
64	EN 50581:2012 (RoHS)		

61.4.6. Network switch - Type 6 - 24Port/1G/L3

Sr. No.	Specification	Compliance (Yes/No)	Remarks
Physical			
1.	1RU fixed form factor		
2.	24 x 10/100/1000 Mbps RJ-45 Ports as host ports + 2 SFP/SFP+ 1/10 Gigabit Ethernet as uplinks ports		
3.	2 redundant power supplies		
4.	Redundant and hot swappable fans		
5.	Management, console, and USB flash-memory ports		
6.	Minimum shared Buffer size should be 9 MB or more		
Layer 2 and Layer 3 Performance			
7.	Minimum 80 Gbps switching capacity		
8.	Minimum Forwarding rate of up to 65 mbps		
9.	Line-rate traffic throughput (both Layer 2 and 3) on all ports		
10.	Configurable maximum transmission units (MTUs) of up to 9216 bytes (jumbo frames)		
11.	Minimum Number of MAC addresses 20,000		
12.	Minimum Number of VLANs 2000		
13.	Minimum Number of ACL entries - 1000 ingress and 500 egress		
14.	Minimum Routing table - 1000		
15.	Minimum Multicast Routing table - 6000		
Minimum Number of EtherChannels should be 64			
16.	IEEE 802.1Q VLAN encapsulation		
17.	LACP: IEEE 802.3ad		
18.	Advanced Ether Channel hashing based on Layer 2, 3, and 4 information		
19.	Storm control (unicast, multicast, and broadcast)		
20.	Private VLANs		
21.	IPV4 Routing protocols: Static, RIPv2, OSPF, and BGP		
22.	VRRP OR HSRP		
23.	VRF: VRF-lite (IP VPN), VRF-aware unicast (BGP, OSPF, and RIP), and VRF-aware multicast		
Multicast			
24.	Multicast: PIM-SMv2, and PIM-SSM		

25.	Bootstrap router (BSR) and Static RP		
26.	Multicast Source Discovery Protocol (MSDP) and Anycast RP		
27.	Internet Group Management Protocol (IGMP) Versions 2 and 3		
28.	Quality of Services (QOS)		
Layer 2 IEEE 802.1p (class of service [CoS])			
29.	8 hardware queues per port and should support per port QOS Configuration		
30.	ACL-based QoS classification (Layers 2, 3, and 4), DSCP Marking and WRED		
Security			
31.	Standard and extended Layer 3 and 4 ACLs include IPv4, Internet Control Message Protocol (ICMP), TCP, and User Datagram Protocol (UDP)		
32.	VLAN-based ACLs (VACLs), Port-based ACLs (PACLs) and Named ACLs		
33.	CoPP (Control plane protection)		
34.	Switched Port Analyzer (SPAN) on physical, PortChannel and VLAN interfaces		
35.	Encapsulated Remote Switched Port Analyzer (ERSPAN)		
Management and troubleshooting			
36.	Zero Touch provisioning of firmware and configuration of the switch to reduce provisioning time using proposed Centralized Network Management tool.		
37.	The Switch Should support monitor events and take corrective action like a script when the monitored events occurs.		
38.	Configuration rollback and NTP Support		
39.	SSHv2, SNMPV3, Syslog, Telnet, AAA and XML Support		
40.	sFlow - industry standard technology for monitoring high speed switched networks. It gives complete visibility into the use of networks enabling performance optimization, accounting/billing for usage, and defense against security threats		

61.5. Centralized Network Management (CNM)

Sr. No.	Required Minimum Specification	Compliance (Yes / No)	Remarks
1	The proposed Network Management Software shall be a comprehensive management platform that delivers integrated, modular management capabilities across fault, configuration, accounting, performance, and security needs.		
2	The proposed Solution must be multivendor solution with no restriction to any one OEM routers - switches from day one. It should be able to manage Switches/routers from major OEM vendors including but not limited to CISCO, HP, and Juniper.		
3	The proposed NMS must be redundant (DC & DR) and must be supplied with necessary hardware and OS/VM licenses for its installation		
4	Centralized Network management System shall be able to manage the proposed and existing Network switches spread across PAN India at bank branch locations, DC & DR from a centralized location (DC-DR)		
5	The software shall come with an initial license for 12000 managed devices. Additional node licenses shall be available to extend the node limit. The solution should be scalable to support 20,000 managed devices without any additional hardware.		
6	The software shall enable centralized management of proposed network elements with a variety of automated tasks, including discovery, categorization, baseline configurations, software images, configuration comparison tools, version tracking, change alerts, and more.		
7	End-to-end visibility of views across network, historical views, ability to follow the network path.		
8	Should able to collect logs from Network and provide analytical data like user, device, location etc.		
9	Must provide single dashboard for monitoring network health, identifying issue, root causes, and remediating issues		
10	Solution shall provide reporting tools that will give the capability to produce reports. It should also provide a database, from which customized reports can be generated		
11	Network should support sending real-time telemetry data/SNMP/Netconf to controller for higher visibility and troubleshooting accuracy.		
12	Automatic discovery of IP devices on the network and does Inventory Management		

13	The solution shall manage layer 3 and heterogeneous layer 2 switched networks over WANs and MPLS.		
14	Shall support correlation of layer 2 switches information, including trunks and meshes.		
15	Should provide custom visual mapping of layer 2 and 3 devices, connectivity and relationships.		
16	Should be able to provide Configuration management of all the network devices in the network.		
17	The solution should provide user roles and controlled access and RBAC to the various network segments.		
18	Proactive insights to help remediate issues quickly and also detailed drill-downs to identify the impact quickly.		
19	Network equipment health monitoring		
20	centralized repository of software images and Software		
21	Solution should have centralized repository of software images and Software Maintenance Updates (SMUs) and apply them to devices from central location		
22	Shall support centralized VLAN Management to view current VLAN configuration, VLAN topology, bulk VLAN deployment etc		
23	Shall have integrated ACL Management to simplify definition and deployment of ACLs and perform ACL rule optimization		
24	Shall support comprehensive configuration Management like Bulk configuration, scheduled backup and restore, baselining and notification of changes etc.		
25	Shall provide flexible reporting capabilities including pre-defined and custom reports with scheduled and flexible delivery options		

61.6. Unified Communication - IP Telephony

Sr. No.	Required Minimum Specification	Compliance (Yes / No)	Remarks
1	The Architecture of the exchange must be completely IP based Server & Gateway type communications system with ability to run both IP and TDM (Analog & Digital) end points with controlling signaling purely on IP across LAN/WAN. The legacy PCM/TDM based systems are not acceptable.		
2	The IP based EPABX system should support VOIP solutions as an integral part of the system. No separate/dedicated hardware, unit/module shall be required for providing telephone services for IP phones. It also should not involve any dedicated external gateways, routers etc. for VoIP support		
3	Offered solution should provide enterprise-grade, communication platform thus delivering a collaborative business application extending features instant messaging/telephony presence, click to call (dial by name, answer, release), call log, P2P audio/video/screen sharing feature should be available from day one for the Type A extensions equipped in the IP EPABX.		
4	The Communication Servers / Call Managers would be deployed in active-active mode. The call control system should be fully redundant solution with no single point of failure and should provide 1:1 redundancy with full capacity. The system should support geographical redundancy across the DC and the DR with minimum bandwidth requirement. Both the servers should do call processing all the time and act as backup in case of the failure of one communication server / Call Manager. The failover should be without disruption of ongoing calls.		
5	Call control server / appliance should be hardware based with necessary configuration to support the desired scalability.		
6	Proposed system architecture should be based on Open Standard Protocols such as SIP, etc. technology. The proposed system should support SIP based applications, SIP trunks and / or terminals. If additional components are required for achieving SIP functionality across the architecture the same needs to be included in the proposal.		
7	The system should support tenant partitioning for not allowing VoIP (CUG calls) and PSTN calls to be bridged. As also all other requirements in respect of complying to the existing DOT/TRAI regulations need to be supported and		

	implemented by the SI. Appropriate documents to be submitted by the OEM / SI.		
8	The entire UC solution (IP PBX, IP Phones, Video Phones and its corresponding hardware/software) have to come from a single OEM or they should complement each other by integrating and collaborating		
Supported Standards:			
9	The communication feature server, IP phones and gateway should support IPV4 & IPV6 from day 1.		
10	The system should be fully compliant to VOIP standards like H.323 and SIP (session initiation protocol). The system should be able to operate with any H.323/SIP compliant.		
11	The SIP proxy, sip registrar should be inbuilt in the system and should support any open & standards based sip stack compliant hard phones or soft phones, if required, it should be able to inter operate with H.323 standard based external gatekeepers.		
12	The offered system should have Voice compression and decompression in accordance with G.711, G.722, G.729AB, wide band audio H.264 ITC recommendations and optional echo-cancellation in accordance.		
13	System should support the QOS features for the VOIP implementation. it should be compliant with both QOS standards (layer 2 - 802.1 p/q) and layer 3- diffserv/tos).		
14	The System must support Network Time Protocol (NTP) to synchronize the system data/time of network devices.		
15	The exchange including Servers, Operating System, System Software etc, must support dual stack network stack and should interoperate with other systems and protocols		
16	System should have commercial grade encryption security with minimum 128-bit key security for both signaling and voice with in a node for all IP subscribers.		
Scalability			
17	The proposed IP PBX system shall support up to 20,000 users scalability to achieve future growth requirements without any additional server or cluster server. Hardware to cater this scalability must be provided from day-1		
18	It should be possible to add more sites and users without the need to change the software and existing configuration.		
Security			
19	The system shall include but not limited to following		

	security features:		
	a. System should have commercial grade encryption security with minimum 128-bit key security for both signaling and voice with in a node for all IP subscribers.		
	b. Strong password policy for accesses		
	c. must have Local authentication database with password policy enforcement		
	d. External authentication protocols (Radius , LDAP/LDAPs)		
	e. Telephony device shall support IEEE 802.1x (MD5 and TLS)		
	f. The telephony server shall allow traffic filtering		
	g. Telephony server shall support SSH and SSL for secure connection		
	h. Telephony software shall provide protection to ensure software integrity of telephony server, media gateway and telephony devices		
	i. Telephony system shall support secure SIP/SRTP		
	Telephony Supported Feature		
20	IP EPABX should be suitable for up to 8-digit extension numbering scheme. This numbering scheme should be flexible. System should also allow mixed numbering scheme.		
21	System should support the attribution of an external number DID or individual line, a group of attendance. the unanswered DID communication can overflow, to attendant or attendant group, voice mailbox, automated attendant, abbreviated number, external number.		
22	Video calling, IP video phones must be able to make video calls using extension numbers between 2 extension.		
23	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.		
24	The IP based EPABX system should support automatic route selection to route the calls based on user definable priorities. This service will be transparent for users and irrespective of the physical carrier connection.		
25	The IP based EPABX shall be equipped with integrated / in-built Automatic Attendant application, which shall automate the handling of incoming calls. The system shall		

	answer the incoming call & guide the caller through a voice guidance menu of various options - to choose extension, operator, or directory service. The call shall be automatically routed to the destination. In case of non-response from the caller's end, the call will automatically flow over to the operator, after a pre-set delay.		
26	Auto-attended system should be able to answer minimum 8 incoming calls simultaneously.		
27	The switchover from night message to daytime message must be automatic. It should provide Seamless routing of calls to Voice Mail System.		
28	Corporate Logo/Wallpapers on IP Phone: The application should allow display of Bank's Corporate Logo, Customized wallpaper		
	Basic Telephone fracture		
29	speed dialing		
30	call forwarding unconditional on busy/no reply to extension, hunt group, voice mail, operator, paging		
31	call pick-up		
32	call log (minimum 100 Number of entries per user)		
33	hot line		
34	call waiting indication		
35	calling line identification restriction for internal calls and external call		
36	conditional external forwarding (busy or no reply)		
37	call waiting		
38	Boss Secretaries		
39	do not disturb		
40	hunting group		
41	immediate forwarding		
42	individual hold		
43	individual call directory		
44	internal/external music on hold		
45	last internal/external number redial		
46	local and external call		
47	Multiline appearance (MLA) on applicable sets.		
48	multiline selective forwarding		

49	multiple conference calls		
50	digit-by-digit dialing mode		
51	ISDN, H.323 or SIP identification (CLIP) converted into name		
52	Voice Broadcast feature: This shall allow unlimited voice broadcast (Voice Paging) on IP Phones		
53	Specific extension shall be able to broadcast a live or pre-recorded message on the loudspeakers of one set or of a group of sets.		
54	When launching a voice broadcast, the operator can select the group/area of sets and the pre-recorded message to broadcast.		
Conference feature			
55	Operational staff shall be able to initiate multi-party conference		
56	The system should be supplied with conferencing facility and the software should be loaded in the same servers		
57	Audio Conference shall support up to 25 participants		
IM Features			
58	Solution should allow users, to check the availability status of their contacts in their contact list.		
59	The common supported status for this application should be available, busy, idle, away etc.		
60	The instant messaging application should support manual setting of user status to: Available, Away, Do Not Disturb (DND) etc.		
61	Shall provide support for open protocols like XMPP.		
62	Should support click to call, click to Video and click to conference features.		
63	The Soft Client should have soft phone capability and should support desktop based point to point video calls.		
64	Should allow users to send and receive messages through their soft clients		
Video Telephony Support			
65	The call control system should provide integrated video telephony features to the users so that user with IP Phone and Soft phone should be able to place video calls with the same user model as audio calls.		
66	Call control system should handle CODEC and video capabilities of the endpoints, bandwidth negotiation to		

	determine if video/audio call can take place.		
67	Unified communication IP telephony should be able to integrate with Polycom video conferencing solution.		
Soft client Features			
68	In addition to the required telephony services and equipments, the IP based telephone exchange system shall also provide Unified Communication application/client for desktops which should be able to work as soft IP Phone		
69	Soft Client should be able to fully integrate with proposed UC server and shall have a friendly, intuitive and easy to use graphical interface		
70	The Proposed soft client should be able to integrate with IP PBX on SIP platform to allow click to call functionality on proposed same client.		
71	Should support basic call control from PC		
72	Integration should be able to provide: Initiate Call, terminate (Hang-Up Call), Hold, Transfer, Divert if Busy		
73	These soft clients should provide all basis call features as per specification mentioned above		
74	Soft clients should support click to call features		
75	Call Conferencing Capability: Should be able to Initiate a conference call involving multiple participants. Should be able to Conference with participants using computer audio for voice Should be able to Conference with participants using IP phone for voice Should be able to Conference with participants using PBX extension for voice		
76	Propose soft client should support video calling from end point using inbuilt/attached camera in endpoint		
77	Video Standard support for soft client is H.264 and above		
78	The video calling capability to be part of the same soft client		
79	User should be able to participate in the video conferencing call.		
80	The user should be able to make point-to-point video calls		
81	UC client / Video Phone should be able to integrate with Polycom Video Conference System		

82	The same soft client should also provide IM feature.		
83	IM Capabilities		
	One-to-one and multi-party messaging		
	Send Multimedia (Text, voice, video and photo) messages between users		
	Store messages centrally and be able to deliver them when users connect. Senders should be able to send to offline receivers and messages should be able to be delivered on demand.		
	Conversation persistency should be maintained so that users can view and participate in active conversations until they leave the conversation		
	The IM messages must be time-stamped.		
	The UC Client should provide Visual & Audio Tone Alerts on incoming Alerts		
84	The UC client must be able to work in tandem with an IP phone also so that when a call is made, the wide band speaker/mic capabilities of the phone are used for the audio stream and video is processed by the UC client. Users must be able to mute, disconnect and control the call from the UC client.		
85	The UC client must be able to integrate with outlook, IBM Lotus Notes for click to call functionality as well. All necessary licenses must be provided to achieve this.		
Helpdesk System			
86	The solution must provide a centralized helpdesk environment.		
87	Solution must have omni-channel capabilities including support for inbound voice, outbound voice, chat, email, bot integration, etc.		
88	Agents must be provided option to login and logout as per their shifts.		
89	Solution must allow single agent to handle any combination from chat, email, inbound and outbound voice calls. This would be defined by supervisor.		
90	Should be highly available with hot standby and seamless failover in case of main server failure. There should not be any downtime of Contact Center in case of single server failure.		
Automatic Call Distribution (ACD)			
91	Should support skill based routing and it should be possible		

	to put all the agents in to a single skill group and different skill groups		
92	ACD support routing of incoming calls based upon caller input to menus, real-time queue statistics, time of day, day of week, ANI, dialed number etc.		
93	ACD should support call routing based on longest available agent, circular agent selection algorithms.		
94	ACD should support the playing of customizable queuing announcements based upon the skill group that the call is being queued to, including announcements related to position in queue and expected delay.		
95	Agents should be able to chat with other Agents or supervisors.		
96	Supervisor should be able to see the real-time status of agents, supervisors should be able to make agent ready or logout from the supervisor desktop		
97	Should support Queuing of calls and playing different prompts depending on the type of call and time in the queue.		
98	The ACD must be implemented in an active and standby server architecture mode from, where the servers can be put in DC and DR. In case the main server in the DataCenter fails, the standby server in DR should take over seamlessly. Upon recovery of main server, there should be automatic fallback to the primary system. ACD solution should support placing of Main and Stand by server in DC and DR respectively.		
Interactive Voice Response (IVR)			
99	IVR should play welcome messages to callers Prompts to press and collect DTMF digits		
100	IVR should be able to integrate with backend database for self-service, as and when required.		
101	GUI based tool to be provided for designing the IVR and ACD call flow.		
102	IVR should support VoiceXML for ASR, TTS, and DTMF call flows for future integrations		
103	IVR should be able to Read data from HTTP and XML Pages		
104	IVR should be able to run outbound campaigns		
Reporting			
105	System to provide report of IVR Application Performance Analysis, Call by Call details for all the calls, Traffic		

	analysis reports etc		
106	Reporting platform to support Agent level reports, Agent login, logout report, report on agent state changes		
107	Queue reports, abandon call reports all the reports should be summary, tabular and detailed report format to be available for the agents.		
108	Reporting platform to support customization of reports without need of third-party tools.		
109	Users of the Historical Reports should be able to perform the following functions View and save reports. System should also allow to export, sort & filter reports, and send scheduled reports to email.		
110	Supervisors must also be able to look at real-time reports that must show current statistics of the system.		

61.6.1. IP Phone Specifications

Sr. No.	Required Minimum Specification	Compliance (Yes / No)	Remarks
1	To support both in-line power, such that power can be directly supplied by the Ethernet switch via LAN cabling and external power		
2	The phone should have 2 x 1GE ports, one for the LAN connection and the other for connecting to PC/laptop.		
3	A large pixel based LCD display, displaying date and time, extension number, calling party name, calling party number and digits dialed		
4	Corporate directory and Lightweight Directory Access Protocol (LDAP) integration.		
5	Ready access to missed, received or placed calls (plus intercom history and directories).		
6	The phone should support QoS mechanism through 802.1p/q.		
7	IP address Assignment by DHCP or statically configured		
8	Hands-free operation with full-duplex speaker-phone		
9	The phone should be a SIP based Phone i.e session Initiation protocol (SIP) supported		
10	The phone should support XML based services and applications.		
11	Should have keys for specific functionalities such as - voicemail, directories, settings, transfer, speakerphone, mute on/off, headset etc		
12	caller's identity should be displayed to a user		
13	Support SRTP / TLS / AES		
14	Should support 802.1x		
15	The phone should support IPv4 and IPv6 from day one.		
16	Should have minimum 5 inch screen with colour display with at least 4 programmable line keys		
17	Should support following audio codec - G.711, G.729a, G.722		
18	The phone should support entries for call history i.e. missed, received, placed etc.		
19	Should support boss-secretary feature, so that secretary can answer calls on behalf of Manager/Executive		

20	The phone should support the following features at a minimum:		
	a.Call forward		
	b.Call pickup		
	c.Call waiting		
	d.Calback		
	e.Conference		
	f.Personal directory		
	g.Call history lists		
21	IP Phone should have following keys at minimum:		
	Volume control keys (+ and -)		
	Hands-free on/off key		
	Mute key		
	Message keys		
	End Call Key		
	Directory key		
22	Latest features to be included to the phone via a software update to the phone's flash memory from a Centralized Location		
23	To support comfort noise generation and voice activity detection programming		
24	Adjustable ringer tones, brightness/contrast and volume levels		
25	Should include a dedicated headset port		
26	Should have Auto Echo Cancellation		
27	Should have Last Number Redial		
28	Should be able to share Extensions on Multiple Phones		
29	The Phone should QOS like Voice activity detection, silence suppression, comfort-noise generation, error concealment, media and signaling marking or similar features		
30	IP Phone should be proposed with a power supply adaptor with Indian standard power cord		
31	IP phone should be supplied with required license		

61.6.2. Video IP Phone

Sr. No.	Required Minimum Specification	Compliance (Yes / No)	Remarks
1	To support both in-line power, such that power can be directly supplied by the Ethernet switch via LAN cabling and external power		
2	The phone should have 2 x 1GE ports, one for the LAN connection and the other for connecting to PC/laptop.		
3	The phone should support Corporate directory and Lightweight Directory Access Protocol (LDAP) integration.		
4	Should have Ready access to missed, received or placed calls (plus intercom history and directories).		
5	The phone should support QoS mechanism through 802.1p/q.		
6	IP address Assignment by DHCP or statically configured		
7	Hands-free operation with full-duplex speaker-phone		
8	The phone should be a SIP based Phone i.e. session Initiation protocol (SIP) supported		
9	Should support IPv4 and IPv6		
10	The phone should support XML based services and applications.		
11	Media Encryption (SRTP) using AES		
12	Signaling Encryption (TLS) using AES		
13	802.1x support		
14	Should have minimum 5 inch screen with colour display with at least 4 programmable line keys		
15	caller's identity should be displayed to a user		
16	Should have Touch-Screen		
17	Video IP Phone should have adjustable foot-stand and/or adjustable screen for better viewing angle of LCD display		
18	Should support following audio codec - G.711a, G.711u, G.729a, G.722		
19	Should have a built-in camera with 720p resolution (encode & decode). Should support standards based video protocol H.264		
20	The camera should have a shutter to open/close camera.		
21	Should support Picture-In-Picture (self-preview overlay)		

22	The phone should support the following features at a minimum:		
	a. Call forward		
	b. Call pickup		
	c. Call waiting		
	d. Callback		
	e. Conference		
	f. Personal directory		
	g. Call history lists		
23	Latest features to be included to the phone via a software update to the phone's flash memory from a Centralized Location		
24	To support comfort noise generation and voice activity detection programming		
25	Adjustable ringer tones, brightness/contrast and volume levels		
26	Should include a dedicated headset port		
27	Should have Auto Echo Cancellation		
28	Should have Last Number Redial		
29	Should be able to share Extensions on Multiple Phones		
30	The Phone should QOS like Voice activity detection, silence suppression, comfort-noise generation, error concealment, media and signaling marking or similar features		
31	IP Phone should be proposed with a power supply adaptor with Indian power cord		
32	IP phone should be supplied with required license		

61.7. AAA Server

Sr. No.	Required Minimum Specification	Compliance (Yes / No)	Remarks
1	Should be a hardware based appliance solution for Authentication, Authorization and Accounting and 802.1x implementation.		
2	Should be a clustered solution with at least two appliances at DC and One in DR so that there is no single point of failure of the AAA implementation for all regions.		
3	Shall perform AAA function for all configured networking devices that includes routers, switches, firewalls in the network.		
4	Should support up to 20000 networked devices without any additional hardware.		
RADIUS conformance to the following IETF RFCs			
5	RFC 2138, Remote Authentication Dial In User Service		
6	RFC 2139, RADIUS Accounting		
7	RFC 2865, RFC 2866, RFC 2867, RFC 2868, RFC 2869		
8	Should provide login authentication functionality.		
9	Upon successful login, the system shall be configurable in way so that command access to certain devices for a particular username can be restricted.		
10	The system should log failed attempts of authentication and command execution.		
11	Should allow the network administrators to control who can log in to the network from wired connections, What privileges each user has in the network, What accounting information is recorded in terms of security audits or account billing, What access and command controls are enabled for each configuration administrator		
12	Should support downloadable ACLs for any Layer 3 devices like routers, firewalls.		
13	Should support user and administrative access reporting, dynamic quota generation and time based restrictions based time of day and day of week		
14	Should support PAP, CHAP and MS-CHAP, EAP-MD5, EAP-TLS password protocols.		
15	Should support PEAP to provide a new, secure, and client-server authentication method for wireless networks.		
16	Should support packet-filtering mechanism to block traffic		

	on all but the apart from necessary AAA-specific TCP and User Datagram Protocol (UDP) ports.		
17	Should support SSL for administrative access		
18	Should support integration with Windows user database and LDAP database.		
19	Should allow the main network administrator to control whether other network administrators can change passwords during Telnet sessions.		
20	Should support PKI		
21	Should support Network Time Protocol for time synchronization with the network.		
22	Should be integrable with the offered Security management system.		
23	Should support Windows user database integration for authentication function		
24	Should support access connection type of wired/wireless LAN, dialup, broadband, and virtual private networks (VPNs)		
25	Should support 801.1x authentication for end stations of the campus network.		
26	Automatic service monitoring, database synchronization, and importing of tools for large-scale deployments		
27	Flexible 802.1X authentication type support including Extensible Authentication Protocol Transport Layer Security (EAP-TLS), Protected EAP (PEAP), EAP-Flexible Authentication via Secure Tunneling (EAP-FAST), and EAP-Message Digest Algorithm 5 (EAPMD5)		
28	Downloadable access control lists for any Layer 3 device		
29	Device command set authorization		
30	Network access restrictions		
31	User and administrative access reporting		
32	Restrictions such as time of day and day of week		
33	User and device group profiles		
34	Should support IPv6 features		

61.8. Network Performance Monitoring

Sr. No.	Required Minimum Specification	Compliance (Yes / No)	Remarks
General Requirement			
1.	Solution should be available on physical appliance		
2.	Solution should support NPM (Network Performance Monitoring, APM (Application Performance Monitoring) and End User Response time monitoring in a single solution.		
3.	Solution should support capture of application data flowing in the Data Center network for analysis. It should be a passive deployment of the solution without need for any agents to be deployed on the applications.		
4.	Solution should provide data collection and intelligence to help baseline performance, alert on deviations and aid in root cause analysis for performance issues with applications, servers or network.		
5.	Solution should provide a converged, all-in-one Network, Application and Unified Communication Performance Management solution. The solution should be vendor agnostic		
6.	Solution should support scalability with an extremely small footprint to provide long-term historical trending with trace-level diagnostics		
7.	Solution should provide complete visibility into an organization's entire enterprise network, while presenting integrated data from multiple environments into a common unified dashboard.		
8.	The solution should provide network path monitoring along with latency between each hop.		
9.	Solution should provide alerting view on Business dashboard in with different colors (to indicate severity) showing the EURT (End User Response Time) metric for Business applications		
10.	The Business Critical Application dashboard should clearly give the detail metrics associated with HIGH end user response time which includes Server response time, Network round Trip Time and Data transfer time.		
11.	Solution Should also give business critical network dashboard to understand the Traffic, latency and Bandwidth utilization per location/site/branches		
12.	Solution should provide drill down feature to understand		

	the End user response time giving breakdown by servers and location/zones wise.		
13.	Solution should propose automated /manual baseline for end user response time and provide visual alert if any deviation on baseline happens		
14.	Solution should capture packets automatically, in case abnormal values are observed on critical servers. These packets are presented for later analysis as PCAP files, which can be downloaded through the web graphical interface at the conversation level.		
15.	Solution should provide single pane of glass for complete network and application visibility		
16.	Solution should support easy integration with other data sources and monitoring tools using Open APIs.		
17.	The solution MUST include a comprehensive logging capability to log all the system events		
18.	Solution should support NTP, for Time Synchronization		
19.	Solution should offer a 100% Web-based user interface for centralized monitoring, configuration and reporting purposes.		
Network Performance Monitoring			
20.	Solution should support Modular configuration to support minimum 20 SPAN/TAP at a given location/instant		
21.	Solution should be able to Monitor network performance in real-time through custom dashboards		
22.	Solution should be able to Visualize network performance and usage trends		
23.	Solution should be able to Pinpoint abnormal behaviours and diagnose network errors		
24.	Solution should be able to identify Network latency (RTT, client-side and server-side), Retransmission rate & Data transfer time (client-side and server side)		
25.	Solution should show any TCP anomalies like Reset, retransmission from client or server ends, connection attempt, established, retransmission delays, timeouts, etc		
26.	Solution should be able to perform Deep Packet Inspection (DPI) on the captured data for analysis.		
27.	Solution should provide KPIs like One-way delay, jitter, Packet statistics like packet lost, loss bursts, reorder packets and Packet delay variance,		
28.	The solution should offer an integrated alert viewer to look		

	at alerts generated based on real time monitoring where thresholds are exceeded for service parameters.		
29.	Solution should offer ability to filter alerts by baseline, availability, threshold etc. and support grouping by alert type/device.		
30.	Solution should support visibility into east-west traffic in VMware NSX environments for application and user experience service assurance.		
31.	Solution should have technology support dedicated, always on, monitoring and continuous capture capabilities to enable real time and back-in-time analysis		
32.	Solution should index and store packets crossing the wire for comprehensive deep-dive forensic analysis activities. It should be stored locally.		
33.	Solution should analyze network traffic in real-time for KPI monitoring and alerting.		
34.	Solution should generate scalable metadata that enables comprehensive views of service, network, application, and server performance across multi-tier, multi-domain service delivery environments		
35.	Solution should support analyzing protocol-specific details for DNS, LDAP, DHCP, and RADIUS		
36.	Solution should provide deep monitoring of web traffic to understand performance by different HTTP request types.		
37.	Solution should support inbuilt decryption of SSL/TLS traffic if decryption keys are available.		
38.	Solution should support multi-segment analysis to troubleshoot issues by capturing similar traffic before and after each capture points (firewall/load balancers etc.) to understand packet loss or latency.		
39.	Solution should clearly identify number of request, latency and failures associated with Get, Head, Put/post, others.		
40.	Solution shall display the status of all SSL certificates being used across the monitored network		
41.	Solution should provide session views of SSL/TLS certificates approaching expiration dates, the issuer of the certificate, the hostnames of the servers to which certificates were issued, and whether the certificates are self-signed		
42.	Solution should also monitor the associated services required to access business applications like DNS, LDAP, DHCP, etc. creating single Dashboard.		

43.	Volumetric: Total Traffic, IP Fragment, TCP SYN/ACK Amplification, Invalid TCP Flags, Charge Amplification, TCP RST, DNS Amplification, MS SQLRS Amplification.		
44.	VOIP performance monitoring including following parameters:		
	SIP/SCCP/MGCP, RTP/RTCP		
	Jitter, Latency, packet loss		
	MOS		
	QOS enforcement		
	Error codes, codecs used, conversation duration etc.		
Application Performance Monitoring			
45.	Solution should monitor all the business-critical applications including standard and custom applications and provide real-time transaction level monitoring		
46.	Performance monitoring of all application operations (web, database, file sharing etc.)		
47.	All application errors are traced and categorized based on their origin and severity		
48.	Identify slowdowns, pinpoint their origin and instantly understand their scope (which users for which transactions)		
49.	Solution should be able to sort data by multiple criteria: number of queries, individual response codes, error statuses, processing times, network data, transfer times, etc.		
50.	Evaluate the impact of deployments and migrations on network resources and end-user experience		
51.	Solution should be able to monitor the application transactions decoded in real time include:		
52.	Web applications (HTTP/HTTPS), SQL databases transactions (MS-SQL, Oracle, MySQL, PostgreSQL), Name resolution and other common network services, Storage and file transfer (CIFS, SMB v1, v2, v3) and VoIP calls (RTP, SIP)		
53.	Solution should also monitor the associated services require to access business applications like DNS, LDAP, DHCP, etc. creating single Dashboard.		
54.	Solution should provide Web transactions metrics like page Hit response time, Page load time, error counts, page count		
55.	Solution should provide search function that allows users to search for IP addresses, server names, server aliases,		

	applications etc.		
56.	Solution should have the interface provide a high-level access point for troubleshooting and drilldown into affected server or application		
57.	The dashboard should support view of worst performing servers.		
58.	Solution should support Layer 7 application based visibility directly from the VM/hypervisor for more than 500 applications including voice, video and data.		
59.	Solution should have feature to provide map of servers associated with a service/application, along with the user communities served by those servers and the dependent servers providing an enabling function to them (e.g., DNS)		
60.	Solution should display error codes associated with standard applications like Oracle, web, DNS, LDAP, etc while monitoring these applications		
61.	Solution should provide application session analysis provide a multi-hop/multi - segment, session-by-session analysis		
62.	Solution should proactively monitor DB related issues like timeouts and failures which may be related to database transactions.		
End User Performance Monitoring			
63.	Solution should measure end-user experience against Service Level Agreements		
64.	Solution should offer a host analysis to view performance for a specific user.		
65.	Solution should provide End-user diagnosis in a few clicks and drills down to detailed infrastructure system and application levels without having to manipulate packets		
66.	The solution should support packet decode using web based console for multiple users (minimum 10 concurrent) to perform troubleshooting concurrently.		
67.	Solution should allow to define threshold based on End user response time		
68.	Solution should alert based on threshold define for End user response time		
Reporting and Dashboard			
69.	Solution should be able to create reports of application, service and network conditions that can be shared.		
70.	Solution should offer Daily / Weekly / Monthly trend-based reporting.		

71.	Solution should offer role based access for report which include create, schedule, and view reports		
72.	Solution should offer integrated application and network performance dashboard views. These should be customizable based on applications and network elements/subnet being monitored and the metrics of interest.		
73.	Drill-down from the performance dashboard view should be available to jump into detailed performance for the specific application/network metrics		
74.	Dashboards should be single view which should be completely configurable and must provide dynamic view in order to radically improve early diagnostics and impact analysis.		
75.	Solution should provide dashboard which should provide drill down option from the general view to detailed analysis and problem resolution views.		
76.	The dashboard should provide status of alerts based on per application/per location.		
77.	Solution should offer an integrated reporting module to generate reports in multiple formats (pdf, csv, rtf etc.) for performance of application, network, voice/video applications.		
78.	Solution should support customized scheduling of reports. Solution should have scheduled report be sent in an email as a PDF, RTF, or CSV file attachment		
79.	The NSI must offer a scalable monitoring solution that could handle current demands, while providing seamless expansion/instrumentation.		
Sizing Details			
80.	Solution should have 40 TB storage and should support optimization on data storage which can help improve storage for key KPI based metrics		
81.	Probe should support packet capture rate of 10 Gbps data for forensic & troubleshooting and shall support additional capacity by adding more probes.		
82.	The Synthetic transaction and business transaction testing required for 10 branches/locations and shall be scalable to all branches/locations		
83.	The packet capture solution should be deployed at both DC and DR		
84.	The solution should support monitoring of 20,000 elements.		

61.9. DDI (DNS, DHCP & IP Address Management Solution)

Sr. No.	Required Minimum Specification	Compliance (Yes / No)	Remarks
General Requirement			
1.	DDI System must be an Appliance based solution providing all DNS, DHCP & IPAM with defined features & capacity.		
2.	DDI System must provide integrated support for high availability configurations without the requirement for licensing of additional third -software components.		
3.	DDI System must support System logs forwarding/redirection of logs to a defined syslog host.		
4.	DDI system must support monitoring using SNMPv3		
5.	DDI system must support NTP time synchronization (client-mode) to multiple servers.		
6.	DDI system must integrate with multiple pass-through authentication options including RADIUS, LDAP, Active Directory		
7.	DDI Solution must support GUI & CLI based configuration.		
8.	DDI Solution must have DNS, DHCP & IPAM solution be integrated together		
9.	Proposed solution should be vendor agnostic for integration with network devices (Switch/Router) (solution should not have any dependency on any Network switches/router OEM to operate smoothly)		
DDI Specific Requirements			
Internal DNS Server			
10.	Solution must support standards-based DNS services.		
11.	The solution must support the ability to act as an internal Authoritative name server		
12.	The Solution must support 2,00,000 DNS QPS acting as internal DNS Server.		
13.	The Solution must support to configure 100 Zone on single instance.		
14.	The Solution must support Master-Slave, Multi Master or Stealth Mode deployment architecture.		
15.	The solution must be able to automate common tasks such as maintaining synchronization between forward and reverse records		
16.	Authoritative Name Servers must have the built-in protection using Response Rate limiting		
17.	The solution must allow adding the following types of zones: Forward Mapping (Authoritative, Forward, Stub), Reverse Mapping (IPv4 and IPv6)		

18.	Authoritative Name Servers must have the built-in protection using DNS DDoS protection - DNS Amplification/DNS reflection/Flooding attacks - UDP, TCP and ICMP/ DNS tunneling/ DNS Reconnaissance		
19.	The Solution must support A, NAPTR, SRV, NS, MX, CNAME records		
20.	The Solution must support IPv6: AAAA, PTR, host, ip6.arpa, DDNS records		
21.	The Solution must support multiple DNS views based on IPv4/Ipv6 Addresses		
22.	The Solution must support Instant propagation of changes to the architecture, such as ACLs, DNS Server Options, Forwarders, etc.		
23.	The solution must support easy search, sort and filter on any DNS Zone or RR, using any field		
24.	The product must support the ability to control DNS logging: DNS query and response logging		
25.	The solution must provide a simplified/streamlined process to identify and manage DKIM, DMARC, ADSP, SPF and/or other similar DNS TXT records.		
26.	The system must be able to display all hosted DNS Resource Records in one GUI pane		
27.	The Solution must have Import Wizard be built-in solution by the DNS Appliance and should not require any external Java program or external Virtual Machines		
28.	The solution must provide a means to track changes to made via Dynamic DNS record assignment		
29.	The solution must support the standard DNSSEC specifications for serving of DNSSEC signed zones and the pass through of client resolution of external zones		
30.	The solution must support secure dynamic updates from Microsoft clients using the Microsoft Generic Security Service Transaction Signature (GSS-TSIG) standard		
31.	The solution must support TSIG for authentication of zone transfers and dynamic updates		
32.	The solution must have inbuilt reports & Stats.		
DHCP			
33.	The solution must provide an easy to use "import wizard" to import DHCP records from legacy DHCP Solution		
34.	Import Wizard solution must be supported by the DHCP Appliance and must not require any external Java program or external Virtual Machines		
35.	The DHCP solution must provide high-availability across two (2) datacenters		

36.	The solution must track and log all user changes to DHCP configurations. The audit logs must be able to identify the change(s) made, the user/system making the change, and a timestamp. The solution should also be able to identify the client IP address from where the change was made.		
37.	The solution must be able to handle 1200 DHCP Lease/sec		
38.	The solution must be able to perform Dynamic DNS for both IPv4 and IPv6 while linking all associated IP addresses to a single device/object.		
39.	The solution must graph (visually display) the different scopes based on number of IP's used/available over a set period of time		
40.	The DHCP solution must support one IP per MAC address (one lease per client).		
41.	The DHCP solution must be able to release the DHCP lease if the MAC address has moved to another IP		
42.	The solution must provide device finger printing and display or report the data in the GUI		
43.	The solution must support creating DHCP custom options.		
44.	The solution must provide the ability to detect or block devices attempting to use DHCP based on various attributes. These attributes must include MAC address but can include device fingerprint, DHCP options, etc		
45.	The DHCP Solution must integrate to IPAM for lease consolidation and capacity planning		
46.	The DHCP Solution must have its built-in security mechanism against Rogue Clients performing DHCP Storm attacks without the need for additional licenses		
47.	The DHCP Solution must be able to send alerts in case of DHCP related attacks		
48.	The DHCP Solution must have inbuilt Reports & stats.		
IPAM			
49.	The IPAM Solution must support 2,50,000 IP Address Management for both IPv4 & IPv6 together.		
50.	The solution must NOT use software agents or thick clients		
51.	The IPAM solution must provide high-availability across DC & DR		
52.	The solution must be flexible to allow the creation of custom fields for objects in IPAM. This must be configurable via the Web GUI.		
53.	The solution must include an application programming interface (API) in order to interface with network and/or asset management systems, a configuration management database (CMDB) solution or other applications.		

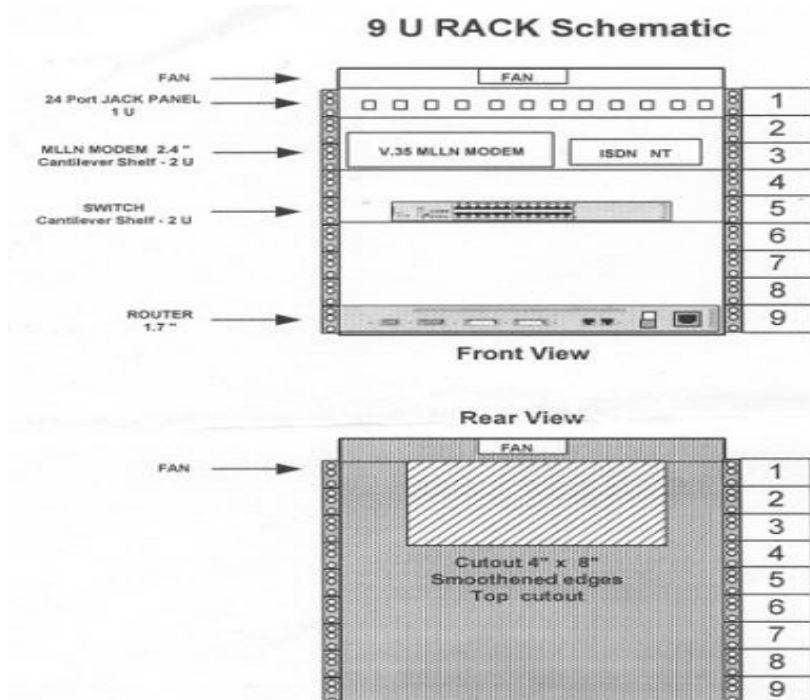
54.	The IPAM solution should be able to seamlessly integrate with DNS and DHCP Records		
55.	The IPAM solution should be able to create its own widget to display customized subnet reports, free IP, used IP.		
56.	The IPAM solution should have the ability to locate the available subnets inside a Supernet. This is to provide assistance to users when creating subnets inside an aggregated Network.		
57.	DDI IPAM user interface must be web-based without specific browser vendor requirements		
58.	DDI IPAM system should support seamless failover between DC and DR		
59.	DDI IPAM system should support VLSM (Variable Length Subnet Masks)		
60.	DDI IPAM system should be able to export reports in PDF, CSV format		
61.	DDI IPAM system should have support for workflow process for various administrator roles and should include a change approval oversight capability.		
62.	DDI audit records should contain a timestamp, username and record modified.		
63.	DDI Reporting engine should include audit reports.		
64.	DDI system should support granular rights administration limiting the function and rights to user and record level		
65.	IPAM Solution should provide centralized Inventory reporting showing which device is assigned to which IP address within the network at any time.		
66.	The tool must have the capability to find free address space across a range		
67.	The IPAM Solution must provide integration with devices (Switch/Router) and provide at least following: Should show IP Details IP Address DNS name Last alive time Status (Used, Unused) Location name Should show Device Details Mac Address Device type Device name Port Number		
Network Discovery, Inventory, Backup and Archiving			
68.	Solution should have the ability to add network devices into inventory via auto-discovery. The proposed infrastructure		

	should be able discover 35,000 network devices.		
69.	Solution should have the ability to add network devices into inventory via manual add/edit/delete methods		
70.	The IPAM Solution component must perform host discovery using a variety of methods including ping, TCP port 80 connections, Address Resolution Protocol (ARP), cache data, and device OS mapping		
71.	Solution should have the ability to add network devices into inventory via manual add/edit/delete methods		
72.	Solution should have the ability to add network devices into inventory via integration with third-party products that perform an auto-discovery		
73.	Solution should have the ability to capture, archive and view device properties for devices in inventory (for example, changes to OS version, IP address, hostname, textual configuration files, and hardware, software and modeled) for devices in inventory		
74.	Solution should have the ability to create and manage custom/manual attributes per device (e.g., asset ID#, street address, State/Province, region, etc.)		
75.	Can the solution create Hardware inventory reports such as listing serial numbers, physical		
76.	Solution should be able create reports be generated in different formats. (PDF, DOC, XLS and HTML formats)		
User and End Tracking and Port Analysis			
77.	Solution should offer infrastructure device port consumption tracking		
78.	Can a user display port usage history		
79.	Solution should offer end host/MAC address location identification and tracking		
80.	Solution should offer end host/MAC address location history and auditing		
81.	Solution should enable port availability calculations based on configurable periods consistent free time		
82.	Solution should report on new and no-longer-present devices on the network		
83.	Solution should highlight location and status changes of devices and interfaces		
84.	Solution should have the ability to search by hardware and software attributes		
85.	Solution should provide following reports at minimum: End host history Device inventory/components/port capacity DHCP lease history		

	DHCP usage trend DHCP usage statistics DHCP top utilized range DHCP fingerprint - trend DNS reply trend DNS Cache hit ratio trend DNS Query Rate DNS top Clients DNS Top Clients per domain DNS Statistics/zone IPAM network usage statistics IPAM usage trend IPAM top utilized networks		
--	---	--	--

61.10. Network Rack

	Network Rack for Branches
Dimension	Table top 19" 9U Rack with 500D
Material	Steel Rack (Body should be at least 1.2mm thick)
Finish	Powder coated and uniform finish
Shelves	Cantilever shelves - 2 nos. 250 mm depth Max. 2U
Fans	1 no. AC power supplied from the power strip fans
Cable manager	1 no. of cable Manager
Power Strip	19" mounted strip with Anchor universal power sockets (6 nos) of 5 Amps each with Surge Suppressor & Fuse
Power Cord	2.5 Mtrs with 15 Amps plug
Front Door	Fiber Glass or plain white glass with lock & key
Rear	Rear Cover with rectangle cut to route cables and push in jack panel
Screws	Pack of 10 nos. Only
	There should be a provision for the side door. This is required to route the cables and remove the power strip or fan easily, if required. Schematic diagram of the 9 U rack is furnished below:



61.11. Modem**61.11.1. G.SHDSL 2 MBPS G.703(E1(nx64Kbps) with Ethernet PAIR**

Sr. No.	Required Minimum Specification	Compliance (Yes / No)	Remarks
G.SHDSL Line Interface:			
1.	Line Code: TCPAM as per ITU-T G.991.2		
2.	Line Type: 2-wire (single pair) twisted copper wire. 0.5 mm.Dia. (or) Optional 4-Wire		
3.	Line Impedance: 135 Ohms.		
4.	Connector: RJ 45		
5.	Transmit Signal Power: 13.5 dBm +/- 0.5 dBm		
6.	Range: Minimum 6 Km. on 0.5 mm. Dia. Copper cable @ 2 Mbps in 2-wire; Minimum 7 Km. on 0.5 mm. Dia. Copper cable @ 2 Mbps in 4-wire; 10 Kms at lower speeds.		
Digital Interface (G.703):			
7.	Line Rate: 2048 Kbps.		
8.	Line Code: HDB3.		
9.	Interface: E1 Interface (4-wire) as per CCITT G.703, G.704.		
10.	Should support Framed and Unframed Channel.		
11.	User selectable CRC4 detection and generation.		
12.	Data Rates: 2.048 Mbps (nx64 Kbps, n=1 to 32)		
13.	Programmable Time Slot selection.		
14.	Impedance: 120 Ohms (Balanced) OR 75 Ohms (Unbalanced)		
15.	Connector: 1 No. RJ 45 for Balanced OR 2 Nos. BNC for Unbalanced		
16.	Transmit Clock: Internal/Recovered from G.703/Recovered from Line		
Diagnostics:			
17.	Local Loop back, Digital Loop back and Remote Digital Loop back		
18.	Test Pattern Generator and Checking (BERT).		
19.	Local loop back test should be operated through Front Panel switches		
Configuration & Monitoring:			
20.	Via DIP Switches, NOT Menu Driven LCD and Keys on Front Panel.		

21.	Via Built-in Ethernet Port with Telnet & HTTP		
22.	Monitoring through ICMP Ping.		
23.	SNMP V1/V2 Supporting RFCs 1213, 3895 (E1) & 3276 (G.SHDSL) with Traps		
24.	SNMP Support for Remote Modem through Proxy.		
25.	SNMP Based 15-minute interval Performance reports for 30 days on SHDSL & 1 Day for E1.		
Indicators:			
26.	Power, Line Sync, G.703/DTE, BER, Test, TD, RD.		
Power			
27.	Dual Mode AC/DC; 230V AC +/- 10%, AND -48 V DC +/- 10%.		
28.	Line Protection		
29.	Should comply to ITU K.20/K.21 using a combination of PTC, GDT & Sidactor. It should be Module based and should not be "On- Board"		
TEC approval:			
30.	The TEC certificate should clearly specify approval for both single and double pair operation as well as the Range of the modem and also the supported interfaces (E1, V.35 , Ethernet etc,.) in the single TEC document.		
31.	Ethernet Router/Bridge/Converter with Built-in G.SHDSL 2 MBPS Modem. Management using HTTP or SNMP with Traps		
LAN Side Interface:			
32.	IEEE 802.3 COMPLIANT		
33.	10/100 BASE T SUPPORT		
34.	RJ45 FEMALE CONNECTOR		
Line Interface - DSL			
35.	G.SHDSL FULL DUPLEX ON 2-WIRE or Optional 4-Wire		
36.	DRIVING DISTANCE AT LEAST 6 km @ 2 MBPS for 2-Wire and 7 km @ 2 MBPS for 4-Wire		
37.	RJ45 CONNECTOR		
38.	TRANSMISSION RATE AT LEAST 2 Mbps (nX64Kbps, n=1to32)		
39.	Modem interface should be able to connect to another modem with G.703 interface located the PCM/Exchange to increase the range beyond the local loop.		
Routing/Bridging/Converter Features (Availability in the single device)			

40.	Routing Mode: RIPv1, RIPv2, Static Route, ICMP, ACL		
41.	Bridging Mode: MAC Address Filtering with Auto Learning & Ageing with 10K Addresses		
42.	Converter Mode: Ethernet to Serial PPPoHDLCL Converter between Ethernet Router & Serial Router		
43.	Support for configuring multiple Static Routes on LAN and WAN along with Hop Count		
44.	Compatible with MLLN Bridge Mode, Routing Mode and support MLLN V-Mux		
45.	Loopback detection based on Magic Number		
46.	Support Compression Control Protocol		
47.	Support for UDP Broadcast and Multicast		
Security Features			
48.	WAN Protocol should be PPP and support PAP & CHAP Authentication		
49.	MAC Based Security Authentication		
Management Features			
50.	There should be provision for Data Rate (nx64K) selection.		
51.	There should be provision for Clock (Internal or Recovered) selection.		
52.	Configuration should be from a supervisory port		
53.	It should have diagnostic facility Digital Loopback on the Front Panel		
54.	LAN/WAN Statistics to be provided on the supervisory port		
55.	Storage and Retrieval of Configuration from supervisory port		
56.	Management through HTTP Web Browser AND SNMP		
Line Protection for DSL Interface			
57.	Should comply to ITU K.20/K.21 using a combination of PTC, GDT & Sidactor		
58.	It should be Module based & and should not be "On- Board"		
Indicators			
59.	Power, Sync, PPP, LAN Tx & Rx, BER , Test ,TD,RD		
Power:			
60.	Dual Mode AC/DC; 230V AC + / - 10%, 50 Hz +/- 5% AND -48 V DC +/- 10%		
TEC approval:			

61.	The TEC certificate should clearly specify approval for both single and double pair operation as well as the Range of the modem and also the supported interfaces (E1, V.35, Ethernet etc.) in the single TEC document. Certificate should clearly mention the TEC Approval of Ethernet Interface.		
-----	---	--	--

61.11.2. 2Mbps V.35 Ethernet Converter

Sr. No.	Required Minimum Specification	Compliance (Yes / No)	Remarks
Specifications			
LAN Side Interface:			
1.	IEEE 802.3 Compliant		
2.	10/100 Base T Support		
3.	RJ45 Female Connector		
WAN Interface: V.35			
4.	Support up to 2Mbps on Serial Sync Interface V.35		
5.	25 Pin DTE Connector		
	Routing / Bridging / Converter Features (Availability in the single device)		
6.	Routing Mode: RIPv1, RIPv2, Static Route, ICMP, ACL		
7.	Bridging Mode: MAC Address Filtering with Auto Learning & Ageing with 10K Addresses		
8.	Converter Mode: Ethernet to Serial PPPoHDLCL Converter between Ethernet Router & Serial Router		
9.	Support for configuring multiple Static Routes on LAN and WAN along with Hop Count		
10.	Compatible with MLLN Bridge Mode, Routing Mode and support MLLN V-Mux		
11.	Loopback detection based on Magic Number		
12.	Support Compression Control Protocol		
13.	Support for UDP Broadcast and Multicast		
Security Features			
14.	WAN Protocol should be PPP and support PAP & CHAP Authentication		
15.	MAC Based Security Authentication		
Management Features			
16.	There should be provision for Data Rate (nx64K) selection.		
17.	There should be provision for Clock (Internal or Recovered) selection.		
18.	Configuration should be from a supervisory port		
19.	It should have diagnostic facility Digital Loopback on the Front Panel		

20.	LAN/WAN Statistics to be provided on the supervisory port		
21.	Storage and Retrieval of Configuration from supervisory port		
Indicators			
22.	Power, Sync, PPP, LAN Tx & Rx, BER , Test ,TD,RD		
Power			
23.	Dual Mode AC/DC; 230V AC + / - 10%, 50 Hz +/- 5% AND - 48 V DC +/- 10%		

61.11.3. LAN Extender

Sr. No.	Required Minimum Specification	Compliance (Yes / No)	Remarks
1.	The LAN extender is required for interconnecting two LAN's using conventional Under-ground telecom copper cable pair without degradation in the LAN performance as per the following specifications:		
Specifications			
2.	DSL/Line Interface - 1/2/4 Wire Pair		
3.	Should support IEEE 802.3ah Ethernet in the First Mile (EFM)		
4.	Line Code: TCPAM as per ITU-T G.991.2, G.SHDSL.bis		
5.	Support Extended TCPAM 32,64 & 128 for higher speeds		
6.	Support speed up to 15 MBPS on 0.5 mm dia single pair cable, 30 MBPS on 0.5 mm dia Two pair cable and 60Mbps on 0.5 mm dia Four pair cable		
7.	Support speed of 15Mbps for a distance coverage of up to 0.8Km, 10Mbps up to 1.4Km, 5Mbps up to 3.5km and 256KBPS for distance coverage up to 10km on 0.5 mm dia single pair cable		
8.	Line Impedance: 135 Ohms Balanced		
9.	Support RJ 45 for connecting Copper cable pair.		
Ethernet Interface			
10.	Should operate in half/full duplex mode with minimum 4 nos. of 10/100 base T Ethernet port (IEEE 802.3 compliance).		
11.	Support Port & ID based VLAN		
12.	Support 4 Priority queues based on 802.1P & DSCP		
13.	Support Rate Limiting in steps of 64Kbps		
14.	Support for broadcast and multicast storm protection		
15.	Support Self learning up to 1K MAC		
16.	Protocols Support: ARP, IP, ICMP, TCP, UDP, HTTP, SNMP, FTP, TELNET		
17.	Support RJ 45 for connecting to Ethernet ports		

Management			
18.	Support In-Band local & remote management via HTTP, Telnet & SNMP. Out-of-Band Management Via any FE Port.		
19.	Configurable through Telnet & HTTP (web browser)		
20.	Online Performance Monitoring as per ITU-T G.826 with Attenuation, NMR/SNR and CRC Errors		
21.	Firmware Upgrade via FTP		
Diagnostics			
22.	Digital Loop-Backs & Test Pattern on SHDSL port		
Indicators			
23.	Visual indications to know the status of Line, Ethernet and Power - MR, ETH, SY1, SY2, SYNC3, SYNC4, TST, TP		
Power			
24.	Support Built in SMPS with Dual Power supply 230V AC +/- 10% & 48VDC +/- 10%		
Line Protection			
25.	Protection against Line Surges as per ITU-T K.20/21 with field replaceable modules		
Environment			
26.	Temperature range (0-50 degree C).		

Authorized Signatory:

Name & Designation & mail id:

Business Address:

Place:

Date:

62. Annexure E (A) - Configuration of proposed solutions

Sr. No.	Equipment Description	Make and model	Hardware/Software configuration details
1. SD-WAN Management Devices (Vendor has to provide proper break up for all component required to end to end deployment)			
1.1.	SD-WAN Controller, Manager, orchestrator, Analytics, Head End Gateway and any other component to be placed at DC and DR in HA		
1.2	Additional hardware and Software for adding additional 6000 branches (each with dual link)		
2. SD-WAN CPE Hardware with all required licenses including NGFW features			
2.1	CPE Hardware supporting 50 Mbps		
2.2	CPE Hardware supporting 300Mbps		
2.3	CPE Hardware Supporting 10 Gbps for DC, NDC and DR in HA at each site		
3. Routers			
3.1	Router -Type 1		
3.2	Router -Type 2		
3.3	Router - Type 3		
3.4	Router - Type 4		
4. Network Switches			
4.1	Switch Type 1 - 24Port/1G		
4.2	Switch Type 2 - 24Port/1G/POE+		
4.3	Switch Type 3 - 48Port/1G/POE+		
4.4	Switch Type 4 - 48Port/10G/Base-T		
4.5	Switch Type 5 - 48Port/10G/SFP+		
4.6	Switch Type 6 - 24Port/1G/L3		
5. Centralized Network Management Solution			
5.1	Centralized Network Management at DC & DR		
6. Unified Communication - IP Telephony (Vendor has to provide proper break up for all component required to end to end deployment)			
6.1	IP Telephony Server infrastructure with all required Hardware and Software components at DC an DR		

6.2	IP Phone with license		
6.3	Video IP Phone with license		
6.4	Soft IP Phone with all required license		
7. Modems			
7.1	2Mbps LAN Extender Pair		
7.2	2Mbps Modem G.703 & Ethernet Pair		
7.3	2Mbps V.35 Converter		
8. Network Performance Monitoring Solution			
8.1	Centralized network performance monitoring solution with all required Hardware and Software at DC		
8.2	End User Performance Monitoring Licenses		
9. DDI Solution			
9.1	Centralized DDI Solution at DC & DR		
10. Other Hardware Components			
10.1	AAA Server in DC and DR		
10.2	Backup solution in DC with Hardware and Software		
10.3	9U RACK		

Note:

- Bidder needs to provide the technical documentation for all proposed hardware, software and solutions.
- Bidder need to provide the architecture and design documents for implementation of the solution along with technical bids.

Authorized signatory

Place:

Name & Designation & mail id:

Date:

Business Address:

63. Annexure F - Unpriced Indicative Commercial Bid

A. Rental charges of network equipment at CO & AO

Sr. No.	Equipment Description	Make and model	Base rental per year	Qty.	Total rental charges per year (in Rs)	Total rental charges for 5 years (in Rs)	Submitted (Yes/No)
			(in Rs) (a)		(c=a*b)	(d=c*5)	
	SD-WAN Management Devices						
1	SD-WAN Controller, Manager, orchestrator, Analytics or any other component to be placed at DC and DR		xx	xx	xx	xx	
	SD-WAN CPE Hardware with all required licenses including NGFW features						
2	SD-WAN CPE hardware Supporting 10 Gbps for DC, NDC and DR in HA at each site		xx	xx	xx	xx	
3	SD-WAN CPE hardware supporting 300 Mbps for RO and large branches		xx	100	xx	xx	
	Routers						
4	Router Type 1 - for DC, DR and NDC		xx	14	xx	xx	
5	Router Type 2 - for Third party segment		xx	4	xx	xx	
6	Router Type 3 - for TP		xx	10	xx	xx	
7	Router Type 4 - for TP		xx	10	xx	xx	
	Network Switches						
8	Switch Type 2 - 24Port/1G/POE+		xx	300	xx	xx	
09	Switch Type 3 - 48Port/1G/POE+		xx	100	xx	xx	
10	Switch Type 4 - 48Port/10G/Base-T		xx	20	xx	xx	
11	Switch Type 5 - 48Port/10G/SFP+		xx	20	xx	xx	
12	Switch Type 6 - 24Port/1G/L3		xx	20	xx	xx	
	Unified Communication						
13	IP Telephony Server infrastructure with all required Hardware and Software components at DC and DR		xx	2 set	xx	xx	
14	IP Phone with all required license for AO		xx	3000	xx	xx	
15	Video IP Phone with all required license for Executives		xx	200	xx	xx	
16	Soft IP Phone client Licenses		xx	500	xx	xx	

17	Licenses for helpdesk agents		xx	100	xx	xx	
	Centralized Network Switches Management						
18	Centralized Network Management at DC & DR in HA		xx	2 set	xx	xx	
19	License cost for 12000 devices		xx	12000	xx	xx	
	Network Performance Monitoring Solution						
20	Centralized network performance monitoring solution with all required Hardware and Software at DC & DR		xx	2 set	xx	xx	
21	End User Performance Monitoring Licenses (Bundle of 10 Users)		xx	1	xx	xx	
	DDI Solution						
22	Centralized Hardware and Software for DDI Solution at DC & DR		xx	2 set	xx	xx	
	Other Hardware Components						
23	AAA Server at DC & DR		xx	2	xx	xx	
24	AAA license cost for 20000 devices		xx	20000	xx	xx	
25	Backup solution with Hardware, Software and tape library at DC		xx	1 set	xx	xx	
TOTAL (A)							

B. Rental charges of network equipment at branches

Sr. No.	Equipment Description	Make and model	Base rental per year	Qty.	Total rental charges per year (in Rs)	Total rental charges for 5 years (in Rs)	Submitted (Yes/No)
			(in Rs) (a)		(c=a*b)	(d=c*5)	
1	SD-WAN CPE hardware supporting 50 Mbps		xx	4400	xx	xx	
2	Switch Type 1 - 24Port/1G		xx	5000	xx	xx	
3	IP Phone with all required license		xx	5000	xx	xx	
4	2Mbps Modem G.703 & Ethernet Pair		xx	2000	xx	xx	
5	2Mbps V.35 Converter		xx	2500	xx	xx	
6	2Mbps LAN Extender Pair		xx	500	xx	xx	
7	9U RACK for branches/offices		xx	4500	xx	xx	
8	Charges for link management, monitoring and maintenance from NOC		xx	9000	xx	xx	
9	Charges for BSNL/MTNL link maintenance		xx	4500	xx	xx	
TOTAL (B)							

C. One Time Cost

Sr. No.	Description	Base Unit cost (In Rs)	Quantity	Total Cost	Submitted (Yes/No)
		(a)	(b)	(c = a*b)	
1	Charges for commissioning new link (BSNL/MTNL)	xx	1000	xx	
2	Charges for upgrading existing link (BSNL/MTNL)	xx	1000	xx	
3	Charges for shifting existing link (including all network devices) (BSNL/MTNL)	xx	1000	xx	
Total (C)					

D. Facility Management Charges

Details	Unit Cost for Year 1 (In Rs) (a)	Unit Cost for Year 2 (In Rs) (b)	Unit Cost for Year 3 (In Rs) (c)	Unit Cost for Year 4 (In Rs) (d)	Unit Cost for Year 5 (In Rs) (e)	Qty (f)	Total Cost for 5 years (In Rs) [g=(a+b+c+d+e) *f)]	Submitted (Yes/No)
Project Manager at Mumbai	XX	XX	XX	XX	XX	1	XX	
Network Specialist	XX	XX	XX	XX	XX	6	XX	
Network Engineers	XX	XX	XX	XX	XX	16	XX	
Network cum Telecom Member	XX	XX	XX	XX	XX	63	XX	
DDI Engineer	XX	XX	XX	XX	XX	1	XX	
NPM Engineer	XX	XX	XX	XX	XX	1	XX	
UC Engineer	XX	XX	XX	XX	XX	2	XX	
	Total (D)					90	XX	

E. Price Discovery for additional Quantity of NW Equipment after 6 months of Go-live

Sr. No.	Equipment Description	Make and model	Base rental per year	Qty.	Total rental charges per year (in Rs)	Total rental charges for 5 years (in Rs)	Submitted (Yes/No)
			(in Rs) (a)		(c=a*b)	(d=c*5)	
1	SD-WAN CPE hardware Supporting 10 Gbps for DC and DR		xx	04	xx	xx	
2	SD-WAN CPE hardware supporting 300 Mbps for RO and large branches		xx	100	xx	xx	
3	SD-WAN CPE hardware supporting 50 Mbps		xx	2900	xx	xx	
4	Switch Type 1 - 24Port/1G		xx	3200	xx	xx	
5	IP Phone with all required license		xx	4000	xx	xx	
6	Video IP Phone with all required for Executives		xx	100	xx	xx	
7	2Mbps Modem G.703 & Ethernet Pair		xx	1000	xx	xx	
8	2Mbps V.35 Converter		xx	2000	xx	xx	
9	2Mbps LAN Extender Pair		xx	100	xx	xx	
10	9U RACK for branches/offices		xx	3000	xx	xx	
11	Charges for link management, monitoring and maintenance from NOC		xx	6000	xx	xx	
12	Charges for BSNL/MTNL link maintenance		xx	3000	xx	xx	
TOTAL (E)							

F. Price Discovery for additional Quantity of NW Equipment after 1 Year of Go-live

Sr. No.	Equipment Description	Make and model	Base rental per year	Qty.	Total rental charges per year (in Rs)	Total rental charges for 5 years (in Rs)	Submitted (Yes/No)
			(in Rs) (a)	(b)	(c=a*b)	(d=c*5)	
1	SD-WAN CPE hardware Supporting 10 Gbps for DC and DR		xx	04	xx	xx	
2	SD-WAN CPE hardware supporting 300 Mbps for RO and large branches		xx	100	xx	xx	
3	SD-WAN CPE hardware supporting 50 Mbps		xx	2400	xx	xx	
4	Switch Type 1 - 24Port/1G		xx	2800	xx	xx	
5	IP Phone with all required license		xx	3000	xx	xx	
6	Video IP Phone with all required for Executives		xx	100	xx	xx	
7	2Mbps Modem G.703 & Ethernet Pair		xx	1000	xx	xx	
8	2Mbps V.35 Converter		xx	1500	xx	xx	
9	2Mbps LAN Extender Pair		xx	100	xx	xx	
10	9U RACK for branches/offices		xx	2500	xx	xx	
11	Charges for link management, monitoring and maintenance from NOC		xx	5000	xx	xx	
12	Charges for BSNL/MTNL link maintenance		xx	2500	xx	xx	
TOTAL (F)							

G. Post Implementation Audit by OEM

Sr. No.	RFP Particular	One time Audit cost per year (In Rs) (a)	Total Cost for 5 years (In Rs) (b=a*5)	Submitted (Yes/No)
1.	Post Implementation Audit by SD-WAN OEM	XX	XX	
2.	Post Implementation Audit by DDI OEM	XX	XX	
3.	Post Implementation Audit by NPAM OEM	XX	XX	
Total (G)			XX	

H. Buy Back Cost

Item	Make Model	Unit Buy Back Cost (Rs.) (a)	Quantity (b)	Total Cost (Rs.) (C) = (a)*(b)	Submitted (Yes/No)
CISCO UCS Server	UCS C210 M2	XX	2	XX	
Cisco MCS Server	MCS-7845-I3-RC2	XX	2	XX	
Webex Node	Cisco 7835-I3-RC1	XX	2	XX	
Open LDAP Server	Cisco 7816-I4 -V01	XX	2	XX	
Video Communication Server	CISCO VCS	XX	2	XX	
Parsec Server	Parsec Server	XX	1	XX	
IP Phones	CISCO (7941 & 7942)	XX	1000	XX	
TOTAL(H)				XX	

I. Total Cost to Ownership

Sr. No.	Details of Annexure	Total amount (Rs.)	Submitted (Yes/No)
1.	Rental charges of network equipment at CO & AO (A)	XX	
2.	Rental charges of network equipment at branches (B)	XX	
3.	One Time Cost (C)	XX	
4.	Facility Management Charges (D)	XX	
5.	Price Discovery for additional Quantity of NW Equipment after 6 months of Go-live (E)	XX	
6.	Price Discovery for additional Quantity of NW Equipment after 1 Year of Go-live (F)	XX	
7.	Post Implementation Audit by OEM (G)	XX	
8.	Buy Back Cost (H)	XX	
Total Cost (TCO)= (I)=(A)+(B)+(C)+(D)+(E)+(F)+(G)-(H)		XX	
TCO in Words (In Rupees)			

Note:

1. Apart from Facility Management cost, all other recurring cost including rental, services, managed services, Post implementation audit cost shall be quoted equally across all years.
2. Considering the inflation and other market factors, Bidder can quote different amount per year for facility management services as per Table D. It is to be noted that if unequal cost is quoted, cost for any year cannot be less than preceding years.
3. The price quoted by Bidder shall be inclusive of Excise Duty and all other charges but exclusive of Goods and Service Tax (GST) and other local taxes, if any, shall be payable by the Bank at actual on date of invoicing.
4. Bank will not pay any labor charges for transportation, installation of hardware items separately.
5. All deliverables and Services to be provided as per requirements for proposed solution specified in the RFP.
6. If the cost for any line item is indicated as zero then it will be assumed by the Bank that the said item is provided to the Bank without any cost.
7. The bidder should ensure that required numbers of officials are available 24*7*365 at Bank's premises to support the Bank's Officials/customers.
8. The Bidder has to make sure all the arithmetical calculations are accurate. Bank will not be held responsible for any incorrect calculations however for the purpose of calculation Bank will take the corrected figures / cost.

9. Bank shall not pay any implementation effort both by OEM & SI. Same should be absorbed in above mentioned TCO.
10. For buy-back, the units will be offered “as is where is” basis and may not be in working condition.
11. Considering falling of prices of electronic goods every year, price discovery is made for large quantity network equipment in three slabs. First slab of price discovery is for equipment to be delivered immediately at Bank’s CO & AO for the quantity as per table A & at Bank’s branches for the quantity as per table B. Second slab of price discovery is for equipment to be delivered after 6 months of go-live for the quantity as per Table E. Third slab of price discovery is for equipment to be delivered after 1 year of go-live for the quantity as per Table F.
12. Contract period is of 5 years from the date of post go-live of SD-WAN Solution with 4500 branches/offices or 6 months from date of 1st Installation, whichever is earlier. However, location wise rental payment will commence from the date of completion of all equipments installed at Branch/office. Bidder need to submit the duly signed copy of installation report.
13. Quantity mentioned against each devices are indicative only and the requirement may increase or decrease as per the actual requirement of the Bank. The actual quantity of FMS/Hardware/Software rental charges may vary and purchase order shall be placed in phased manner based on actual requirements of the Bank from time to time during the contract period.

Authorized Signatory:

Name & Designation & mail id:

Business Address:

Place:

Date:

64. Annexure F (A) - Indicative Commercial Bid

A. Rental charges of network equipment at CO & AO

Sr. No.	Equipment Description	Make and model	Base rental per year	Qty.	Total rental charges per year (in Rs)	Total rental charges for 5 years (in Rs)
			(in Rs) (a)		(c=a*b)	(d=c*5)
	SD-WAN Management Devices					
1	SD-WAN Controller, Manager, orchestrator, Analytics or any other component to be placed at DC and DR in HA for 5000 SD-WAN CPE			xx		
	SD-WAN CPE Hardware with all required licenses including NGFW features					
2	SD-WAN CPE hardware Supporting 10 Gbps for DC, NDC and DR in HA at each site			xx		
3	SD-WAN CPE hardware supporting 300 Mbps for RO and large branches			100		
	Routers					
4	Router Type 1 - for DC, DR and NDC			14		
5	Router Type 2 - for Third party segment			4		
6	Router Type 3 - for TP			10		
7	Router Type 4 - for TP			10		
	Network Switches					
8	Switch Type 2 - 24Port/1G/POE+			300		
09	Switch Type 3 - 48Port/1G/POE+			100		
10	Switch Type 4 - 48Port/10G/Base-T			20		
11	Switch Type 5 - 48Port/10G/SFP+			20		
12	Switch Type 6 - 24Port/1G/L3			20		
	Unified Communication					
13	IP Telephony Server infrastructure with all required Hardware and Software components at DC and DR			2 set		
14	IP Phone with all required license for AO			3000		
15	Video IP Phone with all required license for Executives			200		
16	Soft IP Phone client Licenses			500		
17	Licenses for helpdesk agents			100		
	Centralized Network Switches Management					
18	Centralized Network Management at DC & DR in HA			2 set		

19	License cost for 12000 devices			12000		
	Network Performance Monitoring Solution					
20	Centralized network performance monitoring solution with all required Hardware and Software at DC & DR			2 set		
21	End User Performance Monitoring Licenses (Bundle of 10 Users)			1		
	DDI Solution					
22	Centralized Hardware and Software for DDI Solution at DC & DR			2 set		
	Other Hardware Components					
23	AAA Server at DC & DR			2		
24	AAA license cost for 20000 devices			20000		
25	Backup solution with Hardware, Software and tape library at DC			1 set		
TOTAL (A)						

B. Rental charges of network equipment at branches

Sr. No.	Equipment Description	Make and model	Base rental per year	Qty.	Total rental charges per year (in Rs)	Total rental charges for 5 years (in Rs)	Submitted (Yes/No)
			(in Rs) (a)		(c=a*b)	(d=c*5)	
1	SD-WAN CPE hardware supporting 50 Mbps			4500			
2	Switch Type 1 - 24Port/1G			5000			
3	IP Phone with all required license			5000			
4	2Mbps Modem G.703 & Ethernet Pair			2000			
5	2Mbps V.35 Converter			2500			
6	2Mbps LAN Extender Pair			500			
7	9U RACK for branches/offices			4500			
8	Charges for link management, monitoring and maintenance from NOC			9000			
9	Charges for BSNL/MTNL link maintenance			4500			
TOTAL (B)							

C. One Time Cost

Sr. No.	Description	Base Unit cost (In Rs)	Quantity	Total Cost (In Rs)
		(a)	(b)	(c = a*b)
1	Charges for commissioning new link (BSNL/MTNL)		1000	
2	Charges for upgrading existing link (BSNL/MTNL)		1000	
3	Charges for shifting existing link (including all network devices)		1000	
Total (C)				

D. Facility Management Charges

Details	Unit Cost for Year 1 (In Rs) (a)	Unit Cost for Year 2 (In Rs) (b)	Unit Cost for Year 3 (In Rs) (c)	Unit Cost for Year 4 (In Rs) (d)	Unit Cost for Year 5 (In Rs) (e)	Qty (f)	Total Cost for 5 years (In Rs) [g=(a+b+c+d+e) *f)]
Project Manager at Mumbai						1	
Network Specialist						6	
Network Engineers						16	
Network cum Telecom Member						63	
DDI Engineer						1	
NPM Engineer						1	
UC Engineer						2	
	Total (D)					90	

E. Price Discovery for additional Quantity of NW Equipment after 6 months of Go-live

Sr. No.	Equipment Description	Make and model	Base rental per year	Qty.	Total rental charges per year (in Rs)	Total rental charges for 5 years (in Rs)
			(in Rs) (a)		(c=a*b)	(d=c*5)
1	SD-WAN CPE hardware Supporting 10 Gbps for DC and DR			04		
2	SD-WAN CPE hardware supporting 300 Mbps for RO and large branches			100		
3	SD-WAN CPE hardware supporting 50 Mbps			2900		
4	Switch Type 1 - 24Port/1G			3200		
5	IP Phone with all required license			4000		
6	Video IP Phone with all required for Executives			100		
7	2Mbps Modem G.703 & Ethernet Pair			1000		
8	2Mbps V.35 Converter			2000		
9	2Mbps LAN Extender Pair			100		
10	9U RACK for branches/offices			3000		
11	Charges for link management, monitoring and maintenance from NOC			6000		
12	Charges for BSNL/MTNL link maintenance			3000		
TOTAL (E)						

F. Price Discovery for additional Quantity of NW Equipment after 1 Year of Go-live

Sr. No.	Equipment Description	Make and model	Base rental per year	Qty.	Total rental charges per year (in Rs)	Total rental charges for 5 years (in Rs)
			(in Rs) (a)		(c=a*b)	(d=c*5)
1	SD-WAN CPE hardware Supporting 10 Gbps for DC and DR			04		
2	SD-WAN CPE hardware supporting 300 Mbps for RO and large branches			100		
3	SD-WAN CPE hardware supporting 50 Mbps			2400		
4	Switch Type 1 - 24Port/1G			2800		
5	IP Phone with all required license			3000		
6	Video IP Phone with all required for Executives			100		
7	2Mbps Modem G.703 & Ethernet Pair			1000		
8	2Mbps V.35 Converter			1500		
9	2Mbps LAN Extender Pair			100		
10	9U RACK for branches/offices			2500		
11	Charges for link management, monitoring and maintenance from NOC			5000		
12	Charges for BSNL/MTNL link maintenance			2500		
TOTAL (F)						

G. Post Implementation Audit by OEM

Sr. No.	RFP Particular	One time Audit cost per year (In Rs) (a)	Total Cost for 5 years (In Rs) (b=a*5)
1.	Post Implementation Audit by SD-WAN OEM		
2.	Post Implementation Audit by DDI OEM		
3.	Post Implementation Audit by NPAM OEM		
Total (G)			

H. Buy Back Cost

Item	Make Model	Unit Buy Back Cost (Rs.) (a)	Quantity (b)	Total Cost (Rs.) (C) = (a)*(b)
CISCO UCS Server	UCS C210 M2		2	
Cisco MCS Server	MCS-7845-I3-RC2		2	
Webex Node	Cisco 7835-I3-RC1		2	
Open LDAP Server	Cisco 7816-I4 -V01		2	
Video Communication Server	CISCO VCS		2	
Parsec Server	Parsec Server		1	
IP Phones	CISCO (7941 & 7942)		1000	
TOTAL(H)				

I. Total Cost to Ownership

Sr. No.	Details of Annexure	Total amount (Rs.)
1.	Rental charges of network equipment at CO & AO (A)	
2.	Rental charges of network equipment at branches (B)	
3.	One Time Cost (C)	
4.	Facility Management Charges (D)	
5.	Price Discovery for additional Quantity of NW Equipment after 6 months of Go-live (E)	
6.	Price Discovery for additional Quantity of NW Equipment after 1 Year of Go-live (F)	
7.	Post Implementation Audit by OEM (G)	
8.	Buy Back Cost (H)	
Total Cost (TCO)= (I)=(A)+(B)+(C)+(D)+(E)+(F)+(G)-(H)		
TCO in Words (In Rupees)		

Note:

1. Apart from Facility Management cost, all other recurring cost including rental, services, managed services, Post implementation audit cost shall be quoted equally across all years.
2. Considering the inflation and other market factors, Bidder can quote different amount per year for facility management services as per Table D. It is to be noted that if unequal cost is quoted, cost for any year cannot be less than preceding years.
3. The price quoted by Bidder shall be inclusive of Excise Duty and all other charges but exclusive of Goods and Service Tax (GST) and other local taxes, if any, shall be payable by the Bank at actual on date of invoicing.
4. Bank will not pay any labor charges for transportation, installation of hardware items separately.
5. All deliverables and Services to be provided as per requirements for proposed solution specified in the RFP.
6. If the cost for any line item is indicated as zero then it will be assumed by the Bank that the said item is provided to the Bank without any cost.
7. The bidder should ensure that required numbers of officials are available 24*7*365 at Bank's premises to support the Bank's Officials/customers.
8. The Bidder has to make sure all the arithmetical calculations are accurate. Bank will not be held responsible for any incorrect calculations however for the purpose of calculation Bank will take the corrected figures / cost.
9. Bank shall not pay any implementation effort both by OEM & SI. Same should be absorbed in above mentioned TCO.

10. For buy-back, the units will be offered “as is where is” basis and may not be in working condition.
11. Considering falling of prices of electronic goods every year, price discovery is made for large quantity network equipment in three slabs. First slab of price discovery is for equipment to be delivered immediately at Bank’s CO & AO for the quantity as per table A & at Bank’s branches for the quantity as per table B. Second slab of price discovery is for equipment to be delivered after 6 months of go-live for the quantity as per Table E. Third slab of price discovery is for equipment to be delivered after 1 year of go-live for the quantity as per Table F.
12. Contract period is of 5 years from the date of post go-live of SD-WAN Solution with 4500 branches/offices or 6 months from date of 1st Installation, whichever is earlier. However, location wise rental payment will commence from the date of completion of all equipments installed at Branch/office. Bidder need to submit the duly signed copy of installation report.
13. Quantity mentioned against each devices are indicative only and the requirement may increase or decrease as per the actual requirement of the Bank. The actual quantity of FMS/Hardware/Software rental charges may vary and purchase order shall be placed in phased manner based on actual requirements of the Bank from time to time during the contract period.

Authorized Signatory:

Place:

Name & Designation & mail id:

Date:

Business Address:

65. Annexure G - Declaration for ComplianceAll Terms and Conditions including scope of work except technical specifications

We hereby undertake and agree to abide by all the terms and conditions stipulated by the Bank in this RFP including all addendum, corrigendum etc. (Any deviation may result in disqualification of bids).

Signature:**Name****Date****Seal of company:**Technical Specification

We certify that the systems/services offered by us for tender confirms to the specifications stipulated by you with the following deviations

List of deviations

- 1) _____
- 2) _____
- 3) _____
- 4) _____

Signature:**Name****Date****Seal of company:**

(If left blank it will be construed that there is no deviation from the specifications given above)

66. Annexure H - Undertaking by Bidder

Place:

Date:

To:

The General Manager,
Union Bank of India,
5th floor, Technology Centre,
1/1A, Adi Shankaracharya Marg, Opp. Powai Lake,
Powai, Andheri (East),
Mumbai-400072.

Undertaking (To be submitted by all Bidders' on their letter head)

We _____ (bidder name), hereby undertake that-

- As on date of submission of tender, we are not blacklisted by the Central Government / any of the State Governments / PSUs in India or any Financial Institution in India.
- We also undertake that, we are not involved in any legal case that may affect the solvency / existence of our firm or in any other way that may affect capability to provide / continue the services to bank.

Yours faithfully,

Authorized Signatories

(Name, Designation and Seal of the Company)

Date

67. Annexure I - Process for Evaluation of Bids

Only those Bidders who fulfill the eligibility criteria for Bidder and OEMs as mentioned in eligibility criteria are eligible to submit response to this RFP.

The bidder is required to provide factually correct responses to the RFP. Adequate justification for the response (including the technical and other requirements) should be provided as part of the response. In case the bank finds any response to be inadequate, the bank has the right to ask for additional explanation/ justification. In the event of any discrepancy in the response submitted by the bidder, the bank reserves the right to disqualify/ blacklist the bidder and the OEM.

The Bank reserves the right to change or relax the eligibility criteria to ensure inclusivity.

The Bank reserves the right to verify / evaluate the claims made by the Bidder independently. Any deliberate misrepresentation will entail rejection of the offer.

In case an OEM submits a bid as a bidder, then the OEM cannot participate through other System Integrator bids.

The evaluation will be a Two stage process. The stages are:

- Eligibility, functional and technical bid evaluation
- Commercial bid evaluation

A. Eligibility & Technical Bid Evaluation

The objective of this methodology is to facilitate the selection of the most optimal solution/solutions that appropriately meets the requirements of the Bank. All bids shall be evaluated by an evaluation committee setup for this purpose by the Bank. The Bank will evaluate the technical offers of the bidders in terms of eligibility criteria and the proposals meeting the criteria will only be taken up for further technical evaluation.

The decision on the Bank in regards to evaluation would be final and binding on all the Bidders to this document. The Bank may accept or reject an offer without assigning any reason whatsoever.

The Technical offers submitted by the bidder will be evaluated only if they fulfill the eligibility criteria. The Technical offer will be evaluated based on the Evaluation Matrix Given in this Annexure. Only those bidders who obtain a minimum of 60% marks or more in Technical evaluation will be considered for further stage of evaluation i.e. Functional and Commercial Evaluation. The decision of the Bank in this regard shall be final.

The technical offer submitted by the Bidders shall be evaluated as per various components mentioned:

- Technical requirements of solution
- Past experience/Implementation Experience
- Proof of Concept Stage
- Site Visit to NSI Network Operation Center
- Reference site visit
- Vendor Presentation - Approach Methodology, Proposed Team for Implementation and Bidder Presentation

The technical bid would be rated on a total score of 150 with and the ranking of technical score would be derived for each bidder.

Functional and Commercial Evaluation Process

The Bids which are qualified in Technical would be considered for next stage of Functional and Commercial Evaluation. All the technically qualified bidder will have to supply required compliance to RFP terms & Conditions post addendum. Bidder will propose implementation, management and monitoring methodology i.e. Opening of Indicative Commercial Bids and Reverse Auction. The vendor should furnish their price for the project in their Indicative Commercial Bid to facilitate the Reverse Auction process.

The contract will be awarded to the L1 bidder having lowest TCO (Total Cost of Ownership) which is an outcome of Reverse Auction Process.

Bank reserves the right to select the next ranked Bidder if the selected Bidder withdraws his proposal after selection or at the time of finalization of the contract or disqualified on detection of wrong or misleading information in the proposal.

Indicative Commercial bids quoted in any other currency than INR will be disqualified.

Bidders should give pricing of all solution/appliance, wherever applicable. Tower models for any of the device / appliance will not be accepted. All the server/appliance quoted at central side should be rack mountable and needs to be supplied with adequate rack mounting kit. In case bidder is quoting virtualized environment (vmware/Microsoft Hyper-V or any other virtualized platform), centralized virtual machine management tool also needs to be provided by bidder along with all required licenses/software and same should be part of Bill of Material.

Bids quoting unrealistic prices for any of the solution will be rejected at the discretion of the bank.

Proof of Concept

Bank at its discretion, may ask Bidders who meet with eligibility criteria as defined in the RFP to demonstrate Integrated (wherever applicable) Proof of Concept (PoC) as part of technical evaluation. The PoC will be conducted for SD-WAN and other proposed Solutions as per discretion of Bank. PoC will be based on various use cases given by the Bank. All and any cost associated with demonstrating the Integrated PoC (including provision of Servers, technical resources, travel cost, boarding cost etc.) will be to the account of the Bidder and bank will not bear any cost. Bank reserve its right to extend / shorten the period of POC where needed. The date of the POCs, timelines and locations for testing will be shared with Bidders. Evaluation of the POC exercise will be based on Technical expertise, POC Results, and discussion on POC. It is to be noted that all expenses related to PoC will be borne by bidder.

The scope of PoC will be communicated to successful bidder after eligibility evaluation.

Scoring for approach methodology & Presentation

As part of technical bid, bidder will also submit their approach methodology covering each of the activities and the proposed implementation schedule. The Bidders may also be invited to the bank to deliver an exclusive presentation detailing the proposed architecture, implementation approach, rollout strategy, Strategy for amalgamation, facility management as Services for the solution which would for about 60-120 minutes. The presentations would be delivered to competent panel chosen appropriately by the bank. The bidders are expected

to submit the soft copy of the presentation to the bank prior to the presentation.

Site Visit

Bank shall also conduct visits to Bidder's Network Operation Center (NOC) as proposed in the RFP. Bank will assess bidder's capabilities, recourse competence, proposed monitoring solution including but not limited to Reporting, IT Service Management (ITSM), Dashboards.

Bank at its discretion may also visit any or all reference sites where bidder has implemented SD-WAN and/or providing NOC Services.

Note1: Marks provided by the Bank to the bidder shall be final. No objection/query/justification related to given marks from any bidder shall be entertained. Decision of Bank in this regard shall be final & binding.

Note 2: It is to be noted that Bank will only disclose final marks to technically qualified bidders.

The Technical offers submitted by the bidder will be evaluated only if they fulfill the eligibility criteria. Only those bidders, who meet Eligibility Criteria, will be considered for functional and Technical evaluation. The Technical offer will be evaluated based on the Evaluation Matrix Given in this Annexure. Only those bidders who obtain a minimum of 60% marks or more in Technical evaluation will be considered for further stage of evaluation i.e. Functional and Commercial Evaluation. The decision of the Bank in this regard shall be final.

The evaluation process for short listing of bidder will be based on the evaluation matrix given below.

Scoring chart for functional and Technical evaluation is as follows:

S. No.	Criteria	Max Mark	Scoring	Supporting Document
Bidder's Competence				
1	No. of years in Network Management and Support Services business as on date of issuance of RFP in India:	15	>= 10 Years - 15 Marks Less the 10 Years and more than 7 years - 10 marks Less the 7 Years and more than 4 years - 7 marks Less than 4 years - 5 Marks	Valid copy of Purchase Order clearly indicating the Date of purchase order shall be submitted by the Bidder. Experience shall be considered from the Date of purchase order
2	Turnover of the bidder of	10	<ul style="list-style-type: none"> 1000 Crore or more - 10 Marks More than 750 Crore and Less than 1000 Crore - 7.5 Marks More than 500 Crore and Less than 750 Crore - 5 Marks More than 300 Crore 	Copies of the audited balance sheet and P&L Statement of the company showing the same is to be submitted. In case the audited financials for the year 2018-19 is not available, CA Certificate should be submitted.

			and Less than 500 Crore - 3 Marks	
3	Experience of executing projects of Network Management Support Services for an organization in India spread across multiple states / regions with onsite Network Engineers deployed; each project with a value greater than INR 1000 lakh in last 5 financial years and the branch network of more than 1000.	15	4 or more references - 15 marks 3 references - 10 marks 2 references - 7.5 marks 1 Reference - 5 Marks	Proof of purchase order/work order/sign off documents showing service delivers are desired to be submitted indicating the company is providing such service for the past 5 years.
4	Experience of executing Network Management projects for a Public Sector Bank/ BFSI/ Government Organizations in last 3 financial years with a branch network of more than 1500.	15	3 references - 15 marks 2 references - 10 marks 1 Reference - 8 Marks	Proof of purchase order/work order/sign off documents showing service delivers are desired to be submitted indicating the company is providing such service for the past 5 years.
Project Experience - Proposed Technologies				
5	Proposed SD-WAN Solution should be implemented in any organization in India	15	5 or more references - 15 marks 3-4 references - 10 marks 1-2 references - 5 marks	Proof of purchase order/work order/sign off documents showing implementation of SD-WAN to be submitted.
6	Proposed IP Telephony Solution should be implemented in BFSIs/PSUs/Government organization (excluding RRBs & Co-operative Bank) in India.	15	5 or more references - 15 marks 3-4 references - 10 marks 1-2 references - 5 marks	Proof of purchase order/work order/sign off documents showing implementation of SD-WAN to be submitted.
7	Proposed network switches should be implemented in BFSIs/PSUs/Government organization (excluding RRBs & Co-operative Bank) in India.	15	5 or more references - 15 marks 3-4 references - 10 marks 1-2 references - 5 marks	Proof of purchase order/work order/sign off documents showing implementation of SD-WAN to be submitted.
Approach & Methodology				
8	Presentation Solution Methodology, Solution Design, Support and Training Model. Score will be awarded based on details of overall Solution including methodology detailing implementation / takeover plan.	10		Based on Documentation and Presentation
NOC Visit - Evaluation of Bidders NOC services				

9	Methods followed by NOC team for handling the incidents, troubleshooting and resolution of the issues in line with SLA.	10		Evaluated by the Bank's Technical Evaluation Committee during visiting the NOC.
10	Tools and Dashboards for live monitoring of links and devices	10		Evaluated by the Bank's Technical Evaluation Committee during visiting the NOC.
11	Internal Escalation process for open incidents with timelines for resolution	5		Evaluated by the Bank's Technical Evaluation Committee during visiting the NOC.
Reference Site Feedback				
12	Feedback obtained during Reference site visits	15		Evaluated by the Bank's Technical Evaluation Committee reference site visit.
Total Marks		150		

In addition to this, Bank will also conduct Proof of Concept (PoC). The PoC will be conducted for SD-WAN and other proposed Solutions as per discretion of Bank. PoC will be based on various use cases given by the Bank. All and any cost associated with demonstrating the Integrated PoC (including provision of Servers, technical resources, travel cost, boarding cost etc.) will be to the account of the Bidder and bank will not bear any cost. Bank reserve its right to extend / shorten the period of POC where needed. The date of the POCs, timelines and locations for testing will be shared with Bidders. Evaluation of the POC exercise will be based on Technical expertise, POC Results, and discussion on POC. It is to be noted that all expenses related to PoC will be borne by bidder.

Further is to be noted that in case, bidder/OEM fails to demonstrate successfully any use case as prescribed by Bank (in line with RFP requirement and technical compliance), Bank has right to disqualify bidder and/or OEM on account of technical non-compliance. Bank's decision in this regard shall be final and binding.

68. Annexure J - Confidentiality / Non-Disclosure Agreement

This CONFIDENTIALITY AGREEMENT (the “Agreement”) entered into on this _ day of 2020, and shall be deemed to have become in full force and effect from (the “Effective Date”).

BY and between M/s. _____ a company incorporated under the provisions of the Companies Act, _____ in force in India, having its registered office at _____ (hereinafter referred to as “-----” or “Vendor” which expression shall, unless it be repugnant or contrary to the context or meaning thereof, mean and include its, successors and permitted assigns) of the ONE PART

AND

Union Bank of India, a corresponding new bank constituted under section 3 of Banking Companies (Acquisition & Transfer of Undertakings) Act 1970 having its Head office at Union Bank Bhavan, Vidhan Bhavan Marg, Nariman Point, Mumbai - 400021 (hereinafter referred to as “Union Bank” or “Bank” which expression shall, unless it be repugnant to the context or meaning thereof, mean and include its successors and permitted assigns), of the OTHER PART:

----- and the Bank shall hereinafter jointly be referred to as “Parties” and individually as a “Party”.

In this Agreement, “Affiliate” means any entity which from time to time Controls, is Controlled by or is under common Control with the relevant party or entity, where “Control” means having the ability (including, without limitation, by means of a majority of voting rights or the right to appoint or remove a majority of the board of directors) to control the management and policies of an entity.

WHEREAS: -

- i. Vendor inter-alia is engaged in the business of providing IT related solutions & services to various business entities in India & abroad.
- ii. Union Bank has agreed to disclose, transmit, receive, and/or exchange certain “confidential information” to cover the business transaction between parties for the provision of services related to _____ (“the Purpose”) as more particularly described in Purchase Order no _____, issued by Union Bank in favor of M/s. -----.

NOW THIS AGREEMENT WITNESS:

1. Interpretation

In this Agreement “Confidential Information” means all information belonging to a Party that is or has been disclosed to one Party (the “Receiving Party”) by the other Party (the “Disclosing Party”) in connection with the business transacted/ to be transacted between the Parties. Confidential information shall also include any copy, abstract, extract, sample, note or module thereof. The Receiving Party may use the Confidential Information solely for and in connection with the business transacted/ to be transacted between the Parties.

Notwithstanding the foregoing, “Confidential Information” shall not include any information which the Receiving Party can show: (a) is now or subsequently becomes or is in possession of the Receiving Party, legally and publicly available without breach of this Agreement by the Receiving Party, (b) was rightfully in the possession of the Receiving Party without any

obligation of confidentiality prior to receiving it from the Disclosing Party, (c) was rightfully obtained by the Receiving Party from a source other than the Disclosing Party without any obligation of confidentiality, (d) was developed by or for the Receiving Party independently and without reference to any Confidential Information and such independent development can be shown by documentary evidence, or (e) is disclosed pursuant to an order of a court or governmental agency as so required by such order, provided that the Receiving Party shall, unless prohibited by law or regulation, promptly notify the Disclosing Party of such order and afford the Disclosing Party the opportunity to seek appropriate protective order relating to such disclosure.

2. Confidentiality:

2.1 Except to the extent as agreed herein, the Receiving Party agrees to regard, preserve and keep as secret and confidential all Confidential Information of the Disclosing Party or its clients or any member of their group disclosed under this Agreement. In maintaining confidentiality hereunder, the Receiving Party agrees and accepts that it shall not, either on its own account or jointly with or for any other person, firm, company or any other entity, without obtaining the written consent of the disclosing party.

- I. disclose, transmit, reproduce or make available any such Confidential Information to any person firm, company or any other entity other than its directors, partners, advisers, agents or employees, who need to know the same for the purpose of evaluating, preparing, considering, negotiating, advising in relation to or in furtherance of the purpose aforesaid; or
- II. use the Confidential Information for any purpose other than evaluating, preparing, considering, negotiating, advising in relation to or in furtherance of the purpose for which it is disclosed; or
- III. disclose, announce or otherwise publicize the existence of its association with the Disclosing Party or the existence of the project with the Disclosing Party or any other arrangement (existing or possible) between the disclosing party, its clients or itself in connection with any project/assignment; or
- IV. use any such Confidential Information for its own benefit or the benefit of others or do anything prejudicial to the interests of the Disclosing Party or its clients or any member of their group or their projects.

2.2 The Receiving Party also agrees and accepts that it may endeavor:

- I. use at least the same degree of care in safeguarding such Confidential Information as it uses for its own Confidential information of like importance and such degree of care shall be at least that which is reasonably calculated to prevent such inadvertent disclosure;
- II. keep the Confidential Information and any copies thereof secure and in such a way so as to prevent unauthorized access by any third party;
- III. limit access to such Confidential Information to those of its (including its Affiliates") directors, partners, advisers, agents or employees who are directly involved in the consideration/evaluation of the Confidential Information and bind each of its directors, partners, advisers, agents or employees so involved to protect the Confidential Information in the manner prescribed in this Agreement; and

- IV. upon discovery of any disclosure or suspected disclosure of Confidential Information, to take reasonable effort to as per the circumstances, to inform the Disclosing Party of such disclosure in writing and immediately return to the Disclosing Party all such Information, in whatsoever form, including any and all copies thereof.

3. Return or destruction:

The Receiving Party may, upon completion of the purpose mentioned aforesaid or at any time on receipt of a written demand from the disclosing party: i) immediately return all written Confidential Information and all copies thereof provided to, or produced by, it or its advisers, as the case may be, which is in such party's possession or under its custody and control; ii) to the extent practicable, but without prejudice to the obligations of confidentiality herein, immediately destroy all analyses, compilations, notes, studies, memoranda or other documents prepared by it or its advisers to the extent that the same contain, reflect or derive from Confidential Information relating to the other party; iii) so far as it is practicable to do so (but, in any event, without prejudice to the obligations of confidentiality contained in this Agreement), immediately expunge any Confidential Information relating to the Disclosing Party or its clients or any member of their group or their projects from any computer, word processor or other device in its possession or under its custody and control.

4. Permitted disclosure:

The provisions of paragraph 2 shall not restrict any disclosure required by law or by any court of competent jurisdiction, the rules and regulations of any recognized stock exchange or any enquiry or investigation by any governmental, official or regulatory body which is lawfully entitled to require any such disclosure provided that, so far as it is lawful and practical to do so prior to such disclosure, the Receiving Party shall promptly notify the other party of such requirement with a view to providing the opportunity for the Provider to contest such disclosure or otherwise to agree the timing and content of such disclosure.

5. Ownership of Information:

Except to the extent as agreed herein, the Confidential Information and copies thereof, in whatsoever form shall at all times remain the property of the Disclosing Party or its clients and its disclosure shall not confer on the Receiving Party any rights (including any intellectual property rights) over the Confidential Information whatsoever beyond those contained in this Agreement.

6. No Representation:

Neither the disclosure, transmission receipt or exchange of Confidential Information nor anything else in this Agreement will constitute an offer by or on behalf of the Disclosing Party or be construed as soliciting any business or organization changes or any assurance of any business commitment or an inducement to incur / undertake any obligations not specified herein and neither party will be under any obligation to accept any offer or proposal which may be made by the other or on behalf of such other party.

7. Remedies and Relief:

The parties hereto acknowledge that remedies at law may be inadequate to protect the Disclosing Party or its clients against any actual breach of this Agreement by the Receiving Party, and, without prejudice to any other right and remedies otherwise available to the

Disclosing Party or its clients, the Receiving Party agrees that Disclosing Party has a right to seek injunctive relief in its favor upon proof of actual damage and upon establishment of the fact that such actual damage has taken place due to reasons directly attributable upon the Receiving Party. Such injunctive relief shall be in addition to any other remedies available hereunder, whether at law or equity. Disclosing Party shall be entitled to recover its cost and fees, including Advocate's fees, incurred in obtaining any such relief. Further, in the event of litigation relating to this Agreement, the prevailing party shall be entitled to recover its cost and expenses including Advocate's fees.

8. No Assignment

This Agreement shall not be assigned by the successful bidder, by operation of law or otherwise, without the prior written consent of Bank. This Agreement shall inure to the benefit of and will be binding upon the parties' respective successors and permitted assigns.

9. Severability

In the event that any of the provisions contained in this Agreement is found to be invalid, illegal or unenforceable in any respect by a Court of competent jurisdiction, the validity, legality, or enforceability of the remaining provisions contained in this agreement will not be in any way affected or impaired by such a finding.

10. Delay or Waiver

No delay or failure of either Party in exercising any right hereunder and no partial or single exercise thereof shall be deemed of itself to constitute a waiver or an expectation of non-enforcement of such right or any other rights hereunder. No waiver of any provision of this Agreement shall be valid unless the same is in writing and signed by the party against whom such waiver is sought to be enforced. A waiver or consent given by either party on any one occasion is effective only in that instance and will not be construed as a bar to or waiver of any right on any other occasion.

11. Notices

Notices as required by this Agreement shall be sent to the Parties at the addresses mentioned first herein above or such other addresses as the Parties may designate from time to time, and shall be sent by certified or registered mail with acknowledgement due on receipt.

12. Term

This Agreement shall commence from the Effective Date of this Agreement and shall be valid for 6 months beyond contract period of five years. Confidentiality obligations under this Agreement shall continue to be binding and applicable without limit in point in time except and until such information enters the public domain, without breach of the agreement. Either Party may terminate this Agreement for breach, if the defaulting Party fails to rectify the breach within the one month notice period issued by the non-defaulting Party. Upon expiration or termination as contemplated herein the Receiving Party shall immediately cease any and all disclosures or uses of Confidential Information; and at the request of Disclosing Party, the Receiving Party shall promptly return or destroy all written, graphic or other tangible forms of the Confidential Information and all copies, abstracts, extracts, samples, notes or modules thereof.

13. Governing Law

The provisions of this Agreement shall be governed by the laws of India and shall be subject to the exclusive jurisdiction of courts in Mumbai.

14. Indemnity

The Receiving Party agree to indemnify and hold harmless the Disclosures against all costs, liability, losses and claims incurred by the Disclosing Party as a result of a breach of this Agreement.

15. Modification

Modification to any of the provisions of this Agreement shall be void unless it is writing and duly executed by Parties.

16. Headings

The headings given herein above are for ease of reference only and shall not attach or have any effect/ meaning whatsoever contrary to what is stated in the agreement.

17. Set off

Without prejudice to other rights and remedies available to the bank, bank shall be entitled to set off or adjust any amounts due to the bank from successful bidder/OEM against any payments due and payable by bank for the services rendered.

18. Review of Contract and performance

Bank shall have the right of periodical /yearly review of the performance of the successful bidder with regard to upgradation of processors, memory and storage space and maintenance support under the contract which would be basis of continuation or termination of the same. Bank shall also have the right to review, either itself or through another agency as it may deem fit, the financial and operating performance of the bidder in order to assess the ability of the bidder to continue to meet its outsourcing/contractual obligations.

19. Proprietary Rights:

The entire work product mentioned in this RFP shall be the sole and exclusive property of the Bank. The successful bidder hereby-irrevocably grants, assigns, transfers to the Bank all rights, title and interest of any kind, in and to the work product produced under RFP contract. All information processed, stored, or transmitted by successful Bidder belongs to the Bank. The Bidder does not acquire implicit access rights to the information or rights to redistribute the information. The Bidder understands that civil, criminal, or administrative penalties may apply for failure to protect information appropriately. Any information considered sensitive by the bank must be protected by the successful Bidder from unauthorized disclosure, modification or access. The bank's decision will be final.

The successful bidder will ensure strict compliance of all labor laws, insurance, minimum wages to the staff employed /deployed /engaged for the work assigned and the Bank will not

be liable for any such persons/personnel of successful bidder and shall not be liable for any levies / penalties etc. that may be imposed by the authorities concerned for their action/inaction. There shall be no employer employee relationship whatsoever between the bank and the successful bidder /their employees and the bidder or his employees, staff, agents will not be entitled to any employment with Bank. In the event of any demand/fines/penalty made by any of the authorities on bank in respect of the conduct/actions taken by the bidder/their employees/labourers, the Bank will be entitled to recover the said amounts from the bills / amount payable or from the performance guarantee and also take appropriate action against said persons of bidder/bidder for their misconduct, if any.

20. Counterparts

This Agreement has been signed in duplicate, each of which shall be deemed to be an original. The exchange of a fully executed Agreement (in counterparts or otherwise) by fax shall be sufficient to bind the parties to the terms and conditions of this Agreement.

IN WITNESS WHEREOF THE PARTIES HERETO HAVE CAUSED THIS AGREEMENT TO BE EXECUTED BY THEIR AUTHORIZED REPRESENTATIVES ON THIS _____ DAY OF _____ 2020

Signed and delivered by

Signed and delivered by

M/s _____

Union Bank of India

Signed by:

Signed by:

Name

Name

Title

Title

in the presence of

in the presence of

.....

.....

69. Annexure K - Reference Site Details

Please provide following information for most relevant projects and clients in India:

Use the format below to provide information for which your firm was legally contracted for carrying out consulting assignment. Please mention more than one assignment under the same client if relevant. (Use separate sheet for each client)

Name of the Bank / Financial Institution/Company (Client Name)	
Address of Bank / Financial Institution/Company (Client Name)	
Brief description of the nature of business / process handled.	
Contact Details (At least two contacts details of senior staff of the client are to be provided for each reference).	
Contact1	
Name:	
Designation:	
Landline No.:	
Mobile No.:	
E-mail id:	
Contact2	
Name:	
Designation:	
Landline No.:	
Mobile No.:	
E-mail id:	
Description of the services provided	
Duration of assignment including start date and end date.	
Approximate value of service	

Certificate of experience/ work done/ satisfactory work completion from Senior Executive of the client to be attached regarding the successful completion. Please include client references/ commendation letters, if any.

Place:

Date:

Signature:

Name & Designation:

Business Address:

70. Annexure L - Business Rules for Reverse Auction

RFP for Bank's "Request for Proposal (RFP) for Network Management support services for Wide Area Network of the Bank"

Reverse Auction through E-Procurement

The detailed procedure for Reverse Auction to be followed in the "Request for Proposal (RFP) for Network Management support services for Wide Area Network of the Bank:

The response to the present tender will be submitted by way of submitting the Technical offer & Indicative Commercial offers separately through online. The technical details with the relevant information /documents/acceptance of all terms and conditions strictly as described in this tender document will have to be submitted by the Bidders. The Indicative commercial bids submitted by the Bidders who are short listed in the technical bid evaluation process will be opened and those Bidders will be invited to participate in the online Reverse Auction to be conducted by the company selected by the Bank. Bidders who are short listed from Technical evaluation will be trained by the Reverse Auction Company for this purpose, and they will have to abide by the E-business rules framed by the Bank in consultation with Reverse Auction Service provider. The e-business rules are furnished hereunder in this document.

Further, please note that the Bidder(s) who do not qualify in the technical bid processes will not be considered for participation in Reverse Auction. For participating in reverse auction digital signature is a pre-requisite.

BUSINESS RULES FOR REVERSE AUCTION

1. APPLICABILITY

- 1.1. Reverse Auctions are carried out under the framework of rules that are called Business Rules.
- 1.2. All bidders participating in Reverse Auction shall understand/accept and give an undertaking for compliance with the same to the Bank in the prescribed format Exhibit-A.
- 1.3. Any bidder not willing to submit such an undertaking shall be disqualified for further participation respecting the procurement in question.

2. ELIGIBILITY:

- 2.1. Bidders need to sign integrity pact as per Bank's prescribed format & covers under integrity pact in advance or at the time of submission of integrity pact by authorized signatory on or before last date & time of submission of bid with RFP fee & EMD cost. In case bidder fails to submit integrity pact on or before last date & time of submission of bid, bid will be liable for rejection.
- 2.2. Only vendors who have submitted integrity pact and prescribed undertaking to the Bank and who are technically qualified can participate in Reverse Auction relevant to the procurement for which RFP is floated.

3. COMPLIANCE/CONFIRMATION FROM BIDDERS:

- 3.1. The bidders participating in Reverse Auction shall submit the following duly signed by the same Competent Authority who signs the offer documents in response to the RFP:
 - 3.1.1. Acceptance of Business Rules for Reverse Auction and undertaking as per format in Exhibit-A.
 - 3.1.2. Agreement between service provider and bidder. (This format will be given by the service provider prior to announcement of Reverse Auction.)
 - 3.1.3. Letter of authority authorizing the name/s of official/s to take part in Reverse Auction as per format in Exhibit-B.
 - 3.1.4. Undertaking of Process Compliance Statement for RA as per Exhibit C

4. TRAINING

- 4.1. The Bank will facilitate training for participation in Reverse Auction either on its own or through the service provider for the Reverse Auction.
- 4.2. Where necessary, the Bank/service provider may also conduct a 'mock reverse auction' to familiarize the bidders with Reverse Auction process.
- 4.3. Any bidder/bidder not participating in training and/or 'mock reverse auction' shall do so at his own risk and it shall not be open for him to make any complaint/grievance later.

5. TOTAL COST OF OWNERSHIP (TCO)

- 5.1. TCO refers to the aggregate amount payable by the Bank for transfer of ownership.
 - 5.2. TCO shall encompass but not be limited to the following:
 - 5.2.1 Cost of the equipment/product or services.
 - 5.2.2 License fee (Corporate or user specific as defined in RFP) including OS/Data Base/Application licenses).
 - 5.2.3 Excluding of GST/CGST/SGST/IGST.
 - 5.2.4 Installation and commissioning charges, if any
 - 5.2.5 The prices should include the comprehensive onsite warranty maintenance of the equipments covering all components, services, and visits to the concerned offices as specified in the RFP.
 - 5.2.6 Annual Maintenance Charges for the period as specified in the RFP.
 - 5.2.7 Transportation and Forwarding charges to respective sites.
 - 5.2.8 Training costs for the product/service/equipment if and as defined in RFP.
 - 5.2.9 Service Level Agreement (SLA) costs as defined in RFP for applicable period.
 - 5.2.10 Facility Management/infrastructure support costs as defined in RFP.
 - 5.2.11 Insurance to cover the equipment for and from transit period till installation.
 - 5.3. The TCO shall be arrived at after deducting 'buy back' costs involved and if/as defined in the RFP.
 - 5.4. TCO, however, shall not include variables of octroi and entry tax. These shall be paid as per actuals and on production of receipts. However, no penalties respecting octroi or entry tax shall be paid by the Bank and the vendor shall bear such expenses.
- #### 6. DATE/TIME FOR TRAINING
- 6.1. The Venue, Date, Time etc. for training in Reverse Auction shall be advised at the appropriate time.
 - 6.2. The Bank shall Endeavour to fix such Date/Time at mutual convenience to the bidder/s, service provider and the Bank.

- 6.3. No request for postponement/fixing of Training Date/Time shall be entertained which in the sole view and discretion of the Bank might result in any avoidable delay to either the Reverse Auction or the whole process of selection of bidder.

7. DATE/TIME OF REVERSE AUCTION

- 7.1. The Date and Time of commencement of Reverse Auction as also Duration of 'Reverse Auction Time' shall be communicated at least 3 working Days prior to such auction Date.
- 7.2. Any force majeure or other condition leading to postponement of auction shall entitle the Bank to postponement of auction even after communication, but, the Bank shall be obliged to communicate to all participating bidders the 'postponement' prior to commencement of such 'Reverse Auction'.

8. CONDUCT OF REVERSE AUCTION

- 8.1. The Reverse Auction shall be conducted on a specific web portal meant for this purpose.
- 8.2. The Reverse Auction may be conducted by the Bank itself or through a service provider specifically identified/appointed/empanelled by the Bank.

9. SERVICE PROVIDER'S ROLE & RESPONSIBILITIES

- 9.1. In all Reverse Auctions conducted by the Bank through a Service Provider, the Bank shall enter into a separate agreement clearly detailing the role and responsibilities of the service provider hosting the web portal for the Reverse Auction.
- 9.2. For creating necessary obligations and rights, the service provider will also enter into an agreement with each bidder as per a format designed by him for this purpose. The Bank shall resolve any points/issues concerning such agreement of bidder and service provider.
- 9.3. While a Service Level Agreement (SLA) by the bank with the service provider is an arrangement for smooth and fair conduct of the Reverse Auction, the Bank shall be directly responsible to bidders for fair and transparent conduct of Reverse Auction.
- 9.4. The service provider at the end of each Reverse Auction shall provide the bank with all details of the bids and reports of reverse auction.
- 9.5. The service provider shall also archive the data pertaining to the Reverse Auction for a minimum period of 3 years.

9.6. TRAINING AND AUCTION

- 9.6.1. Service provider / auctioneer are responsible for conduct of adequate training to all technically qualified bidders representing the reverse auction and bidding process.
- 9.6.2. Each bidder / bidder shall participate in the training at his / their own cost.
- 9.6.3. Wherever it is considered necessary and asked by the bidders or as decided by the auctioneer or by Bank a mock auction may also be conducted for the benefit of all concerned.
- 9.6.4. Authorized representatives of the bidders named in the authorization letter given by the bidder (Exhibit-B) shall be given unique user name, password by the service provider /

auctioneer.

- 9.6.5. Each bidder shall change the password and edit the information in the registration page after receipt of initial password.
- 9.6.6. All the bids made from the login ID given to bidder shall ipso-facto be considered bid made by the bidder / bidder to whom login ID and password were assigned by the service provider / auctioneer.
- 9.6.7. Any bid once made through registered login ID / password by the bidder / bidder cannot be cancelled. The bidder, in other words, is bound to sell the “Offering” as per the RFP at the bid price of TCO.
- 9.6.8. Every successive bid by the bidder / bidder being decremented bidding shall replace the earlier bid automatically and the final bid as per the time and log-in ID shall prevail over the earlier bids.
- 9.6.9. The Bank shall conduct the reverse auction as per the Standard English reverse auction, that is, no two bids can have identical price from two different bidders. In other words, there shall never be a “Tie” in bids.

10. PROXY BID

- 10.1. A proxy bid is one where bidder can submit the lowest bid amount by him in strict confidence to the system directly. This obviates the need for him participating in the bidding process until the proxy bid amount is decrementally reached by other bidders.
- 10.2. When proxy bid amount is reached, the bidder has an option to revise the proxy bid amount or he can prefer to start participating in bidding process.
- 10.3. Since it is an English auction with no ties, two bidders submitting identical proxy bid amount and succeeding in auction simultaneously does not arise.
- 10.4. During training, the issue of proxy bidding will be clarified in detail by the service provider.

11. TRANSPARENCY IN BIDS

- 11.1. All bidders will be able to view during the auction time the current lowest price in portal. Bidder shall be able to view not only the lowest bid but also the last bid made by him at any point of time during the auction time.

12. MASKING OF NAMES

- 12.1. Names of bidders/ bidders shall be anonymously masked in the Reverse Auction process and bidders will be given suitable dummy names.
- 12.2. After completion of Reverse Auction, the service provider / auctioneer shall submit a report to the Bank with all details of bid and the original names of the bidders as also the L1 bidder with his / their original names.

13. START PRICE

- 13.1. Bank shall determine the start price either on its own or through asking for information of price band on TCO from each bidder at appropriate time during or at the conclusion of technical evaluation. Based on the price band so informed by bidders, Bank would determine the start price for reverse auction.

14. DECREMENTAL BID VALUE

- 14.1. The bidders shall be able to bid only at a specified decrement value and not at any other fractions. The Bid decrement value shall be Rs. 7500/- or 0.25% of the Start price of the Reverse Auction, whichever is higher.
- 14.2. The bid decrement value shall be rounded off to the nearest thousands of rupees.
- 14.3. For the sake of convenience of bidders, the web portal shall display the next possible decremented value of bid. It is not, however, obligatory on the part of bidders to bid at the next immediate lower level only. (That is, bids can be even at 2 or 3 lower levels than the immediate lower level and should not exceed 2% of start bid price at a time)

15. COPY OF BUSINESS RULES

- 15.1. The Bank shall supply copy of the Business rules to any bidders / bidders, wishing to participate in the reverse auction. Such request shall be made in writing to the Bank by an authorized representative of the bidder.
- 15.2. The Bank shall also handover a copy of the Business Rules with a covering letter duly signed by an authorized signatory of the Bank.
- 15.3. For any dispute concerning the Business Rules, the hard copy of Business Rules supplied by the Bank for the reference of reverse auction process will alone be considered final and bidding.

16. SPLITTING OF ORDERS

- 16.1. If any RFP specifically authorizes splitting of orders for the sake of reducing dependency on single source of supply or provision of service, Bank is entitled to split the order in the order and as provided in RFP.
- 16.2. While splitting the order, Bank shall specify the maximum quantum for L1, L2 etc. in RFP.
- 16.3. In case L2 bidder is not willing to supply at L1 price, Bank shall call L3, L4 etc. in order to arrive at the split quantum to be awarded.

17. REVERSE AUCTION PROCESS

- 17.1. In order to reduce the time involved in the procurement process, Bank shall be entitled to complete the entire procurement process through a single Reverse Auction. For this purpose, Bank shall do all it can to award the contract to L1 bidder or in the circumstances where awarding of contract may have to be done to the L2, L3 bidder as provided for in the RFP.
- 17.2. The Bank shall however, be entitled to cancel the procurement of Reverse Auction, if in its view procurement or reverse auction process cannot be conducted in a fair manner and / or in the interest of the Bank.
- 17.3. The successful bidder shall be obliged to provide a Bill of Material at the last bid price at the close of auction.

18. EXPENDITURE ON REVERSE AUCTION

- 18.1. All expenses of reverse auction shall be borne by the Bank.

18.2. Bidders, however, shall attend the training or mock auction at their own cost.

19. CHANGES IN BUSINESS RULES

19.1. Any change in Business Rules as may become emergent and based on the experience gained shall be made only by a Committee of senior / top executives of the Bank.

19.2. Any / all changes made in Business Rules shall be uploaded in the Website immediately.

19.3. If any reverse auction process has commenced and a change is made in Business Rules, it shall be informed immediately to each bidder/ bidder and his concurrence to / acceptance of the change shall be obtained in writing by the Bank.

20. DON'TS APPLICABLE TO THE BIDDER/BIDDER

20.1. No bidder shall involve himself / itself or any of his / its representatives in any price manipulation directly or indirectly with other bidders. If any such practice comes to the notice, Bank shall disqualify the bidder / bidders concerned from the reverse auction process.

20.2. Bidder shall not disclose details of his bids or any other details concerning Reverse Auction process of the Bank to any other third party without specific permission in writing from the Bank.

20.3. Neither Bank nor service provider / auctioneer can be held responsible for consequential damages such as no power supply, system problem, inability to use the system, loss of electronic information, power interruptions, UPS failure, etc. (Bank shall, however, entertain any such issues of interruptions, problems with open mind and fair degree of transparency in the process before deciding to stop or extend the auction.)

21. GRIEVANCES REDRESSAL

21.1. Any aggrieved bidder / bidder through Reverse Auction process can make complaint in writing within 48 hours of the Reverse Auction to the Chief Compliance Officer of the Bank.

21.2. The Chief Compliance Officer along with the Chief Law Officer of the bank and Chief of Audit Dept. shall give personal hearing to the aggrieved bidder / bidder and decide upon the complaint / grievance.

21.3. Decision of the Grievance Redressal Committee shall be binding on the Bank as well as on all bidders participating in the Reverse Auction.

21.4. Any aggrieved vendor / bidder through Reverse Auction process can make representation in writing within 48 hours of the Reverse Auction to the IEM (Independent External Monitor) of the Bank.

22. ERRORS AND OMISSIONS

22.1. On any issue or area of material concern respecting Reverse Auction not specifically dealt with in these Business Rules, the decision of the bank shall be final and binding on all concerned.

Place:

Date:

Signature:

Name & Designation:

Business Address:

71. Annexure L (A) - Compliance Statement - Reverse Auction
(To be submitted by all the bidders participating in Reverse Auction)**Exhibit -A**

To,
Union Bank of India
Department of Information Technology
Powai, Mumbai

DECLARATION

- 1 We _____ (name of the company) hereby confirm having submitted our bid for participating in Bank's RFP dated _____ for procurement of _____.
- 2 We also confirm having read the terms of RFP as well as the Business Rules relating to the Reverse Auction for this RFP process.
- 3 We hereby undertake and agree to abide by all the terms and conditions stipulated by Union Bank of India in the RFP document including all annexure and the Business Rules for Reverse Auction.
- 4 We shall participate in the on-line auction conducted by _____ Ltd. (Auction Company) and submit our commercial bid. We shall also abide by the procedures prescribed for online auction by the auction company.
- 5 We, hereby confirm that we will honor the Bids placed by us during the auction process, failing which we shall forfeit the EMD. We also understand that the bank may debar us from participating in future tenders.
- 6 We confirm having nominated Mr _____, designated as _____ of our company to participate in the Reverse Auction on behalf of the company. We undertake that the company shall be bound by the bids made by him in Reverse Auction.
- 7 We undertake to submit the confirmation of last bid price by us to the auction company/Bank within 48 working hours of the completion of event. We also undertake to submit the Bill of Materials for the TCO (Total Cost of Ownership) in terms of RFP.

Signature with company seal

Name:

Company / Organization:

Designation within Company / Organization:

Address of Company / Organization:

Date:

Name of Authorized Representative: _____

Signature of Authorized Representative: _____

Verified above signature

Competent Authority Signature: _____

Date: _____

72. Annexure L (B) - Letter of Authority for Participation in Reverse Auction**Exhibit -B**

To,
Union Bank of India
Department of Information Technology
Powai, Mumbai

- 1 We _____ (name of the company) have submitted our bid for participating in Bank's RFP dated _____ for procurement of _____.
- 2 We also confirm having read and understood the terms of RFP as well as the Business Rules relating to the Reverse Auction for this RFP process.
- 3 As per the terms of RFP and Business rules, we nominate Mr. _____, designated as _____ of our company to participate in the Reverse Auction.
- 4 We accordingly authorize Bank and / or the Auction Company to issue user ID and password to the above named official of the company.
- 5 Both Bank and the auction company shall contact the above named official for any and all matters relating to the Reverse Auction.
- 6 We, hereby confirm that we will honor the Bids placed by Mr. _____ on behalf Of the company in the auction process, failing which we will forfeit the EMD. We agree and understand that the bank may debar us from participating in future tenders for any such failure on our part.

Signature with company seal

Name -

Company/ Organization

Designation within Company / Organization

Address of Company / Organization

Date:

Name of Authorized Representative: _____

Signature of Authorized Representative: _____

Verified above signature

Signature of Competent Authority: _____

Date: _____

73. Annexure L (C) - Undertaking of Process Compliance Statement for R A

(This letter should be on the letterhead of the bidder duly signed by an authorized signatory)

Exhibit -C

Place:

Date:

To,

The General Manager,
Union Bank of India,
Technology Centre,
1/1A, Adi Shankaracharya Marg, Opp. Powai Lake,
Powai, Andheri (East),
Mumbai-400072.

Sir,

Subject: Agreement to the process related Terms and Conditions for the online Reverse Auction for Network Management support services for Wide Area Network of the Bank

This letter is to confirm that:

1. The undersigned is authorized representative of the company.
2. We have studied the Commercial Terms and the Business Rules governing the Reverse Auction as mentioned in the RFP and confirm our agreement to them.
3. We confirm that Union Bank of India and Auction Service Provider shall not be liable & responsible in any manner whatsoever for my/our failure to access & bid on the e-auction platform due to loss of internet connectivity, electricity failure, virus attack, problems with the PC, any other unforeseen circumstances etc before or during the auction event.
4. We also confirm that we have a valid digital signature certificate issued by a valid Certifying Authority.
5. We also confirm that we will mail the price confirmation & break up of our quoted price as per [Annexure F](#) within 24 hours of the completion of the reverse auction.
6. We, hereby confirm that we will honour the bids placed by us during the auction process.

Signature with company seal

Name -

Company/ Organisation

Designation within Company / Organisation

Address of Company / Organisation

Date:

Name of Authorized Representative: _____
Signature of Authorized Representative: _____
Verified above signature
Signature of Competent Authority: _____
Date: _____

74. Annexure M - Pre Contract Integrity Pact

Tender Ref. No:....

INTEGRITY PACT

Whereas Union Bank of India having its registered office at Union Bank Bhavan, 239, Vidhan Bhavan Marg, Nariman Point, Mumbai, India -400 021 acting through its Department, represented by General Manager / Dy. General Manager hereinafter referred to as the Buyer and the first party, proposes to procure (Name or category of the Equipment, services, etc.) hereinafter referred to as Stores and / or Services.

And

M/s_____ represented by_____ Chief Executive Officer, (which term, unless expressly indicated by the contract, shall be deemed to include its successors and its assignee), hereinafter referred to as the bidder/seller and the second party, is willing to offer/has offered the Stores and / or Services.

2. Whereas the Bidder/Seller is a private company/public company/ /partnership/registered export agency, constituted in accordance with the relevant law in the matter and the BUYER is a Public Sector Undertaking and registered under Companies Act 1956. Buyer and Bidder/Seller shall hereinafter be individually referred to as “Party” or collectively as the “parties”, as the context may require.

3. Preamble

Buyer has called for tenders under laid down organizational procedures intending to enter into contract /s for supply / purchase / etc. of _____ and the Bidder /Seller is one amongst several bidders /Proprietary Vendor /Customer Nominated Source/Licenser who has indicated a desire to bid/supply in such tendering process. The Buyer values and takes primary responsibility for values full compliance with all relevant laws of the land, rules, regulations, economic use of resources and of fairness / transparency in its relations with its Bidder (s) and / or Seller(s).

In order to achieve these goals, the Buyer will appoint Independent External Monitor(s) (IEM) in consultation with Central Vigilance Commission, who will monitor the tender process and the execution of the contract for compliance with the principles mentioned above.

4. Commitments of the Buyer

4. 1 The Buyer commits itself to take all measures necessary to prevent corruption and fraudulent practices and to observe the following principles: -

- (i) No employee of the Buyer, personally or through family members, will in connection with the tender, or the execution of a contract demand, take a promise for or accept, for self or third person, any material or immaterial benefit which the person is not legally entitled to.
- (ii) The Buyer will during the tender process treat all Bidder(s) /Seller(s) with equity and reason. The Buyer will in particular, before and during the tender process, provide to

all Bidder (s) /Seller(s) the same information and will not provide to any Bidders(s) /Seller(s) confidential /additional information through which the Bidder(s) / Seller(s) could obtain an advantage in relation to the process or the contract execution.

(iii) The Buyer will exclude from the process all known prejudiced persons.

4.2 If the Buyer obtains information on the conduct of any of its employees which is a criminal offence under the Indian Legislation Prevention of Corruption Act 1988 as amended from time to time or if there be a substantive suspicion in this regard, the Buyer will inform to its Chief Vigilance Officer and in addition can initiate disciplinary action.

5 Commitments of the Bidder(s) /Seller(s):

5.1 The Bidder(s)/ Seller(s) commit itself to take necessary measures to prevent corruption. He commits himself to observe the following principles during his participation in the tender process and during the contract execution.

- (i) The Bidder(s) /Seller(s) will not directly or through any other persons or firm, offer promise or give to any of the Buyer's employees involved in the tender process or the execution of the contract or to any third person any material or other benefit which he / she is not legally entitled to, in order to obtain in exchange any advantage during the tendering or qualification process or during the execution of the contract.
- (ii) The Bidder(s) /Seller(s) will not enter with other Bidders / Sellers into any undisclosed agreement or understanding, whether formal or informal. This applies in particular to prices, specifications, certifications, subsidiary contracts, submission or non submission of bids or any other actions to restrict competitiveness or to introduce cartelization in the bidding process.
- (iii) The bidder(s) /Seller(s) will not commit any offence under the Indian legislation, Prevention of Corruption Act, 1988 as amended from time to time. Further, the Bidder(s) /Seller(s) will not use improperly, for purposes of competition or personal gain, or pass on to others, any information or document provided by the Buyer as part of the business relationship, regarding plans, technical proposals and business details, including information constrained or transmitted electronically.
- (iv) The Bidder(s) /Seller(s) shall ensure compliance of the provisions of this Integrity Pact by its sub-supplier(s) / sub-contractor(s), if any, Further, the Bidder /Seller shall be held responsible for any violation/breach of the provisions by its sub-supplier(s) /Sub-contractor(s).

5.2 The Bidder(s) /Seller(s) shall ensure compliance of the provisions of this Integrity Pact by its sub-supplier(s) / sub-contractor(s), if any, Further, the Bidder /Seller shall be held responsible for any violation /breach of the provisions by its sub-supplier(s) /sub-contractor(s).

5.3 The Bidder(s) /Seller(s) will not instigate third persons to commit offences outlined above or be an accessory to such offences.

5.4 Agents / Agency Commission

The Bidder /Seller confirms and declares to the Buyer that the bidder/Seller is the original manufacturer/authorized distributor / stockiest of original manufacturer or Govt. Sponsored /Designated Export Agencies (applicable in case of countries where domestic laws do not permit direct export by OEMS of the stores and /or Services referred to in this tender / Offer / contract / Purchase Order and has not engaged any individual or firm, whether Indian or Foreign whatsoever, to intercede, facilitate or in any way to recommend to Buyer or any of its functionaries, whether officially or unofficially, to the award of the tender / contract / Purchase order to the Seller/Bidder; nor has any amount been paid, promised or intended to be paid to any such individual or firm in respect of any such intercession, facilitation or recommendation. The Seller / Bidder agrees that if it is established at any time to the satisfaction of the Buyer that the present declaration is in anyway incorrect or if at a later stage it is discovered by the Buyer that the Seller incorrect or if at a later stage it is discovered by the Buyer that the Seller/Bidder has engaged any such individual /firm, and paid or intended to pay any amount, gift, reward, fees, commission or consideration to such person, party, firm or institution, whether before or after the signing of this contract /Purchase order, the Seller /Bidder will be liable to refund that amount to the Buyer. The Seller will also be debarred from participating in any RFP / Tender for new projects / program with Buyer for a minimum period of five years. The Buyer will also have a right to consider cancellation of the Contract / Purchase order either wholly or in part, without any entitlement of compensation to the Seller /Bidder who shall in such event be liable to refund agents / agency commission payments to the buyer made by the Seller /Bidder along with interest at the rate of 2% per annum above LIBOR (London Inter Bank Offer Rate) (for foreign vendors) and Base Rate of SBI (State Bank of India) plus 2% (for Indian vendors). The Buyer will also have the right to recover any such amount from any contracts / Purchase order concluded earlier or later with Buyer.

6. Previous Transgression

6.1 The Bidder /Seller declares that no previous transgressions have occurred in the last three years from the date of signing of this Integrity Pact with any other company in any country conforming to the anti corruption approach or with any other Public Sector Enterprise in India that could justify Bidder's /Seller's exclusion from the tender process.

6.2 If the Bidder /Seller makes incorrect statement on this subject, Bidder /Seller can be disqualified from the tender process or the contract, if already awarded, can be terminated for such reason without any liability whatsoever on the Buyer.

7. Company Code of Conduct

Bidders /Sellers are also advised to have a company code of conduct (clearly rejecting the use of bribes and other unethical behavior) and a compliance program for the implementation of the code of conduct throughout the company.

8. Sanctions for Violation

8.1 If the Bidder(s) /Seller(s), before award or during execution has committed a transgression through a violation of Clause 5, above or in any other form such as to put his reliability or

credibility in question, the Buyer is entitled to disqualify the Bidder(s) /Seller (s) from the tender process or take action as per the procedure mentioned herein below:

- (i) To disqualify the Bidder /Seller with the tender process and exclusion from future contracts.
- (ii) To debar the Bidder /Seller from entering into any bid from Buyer for a period of two years.
- (iii) To immediately cancel the contract, if already signed /awarded without any liability on the Buyer to compensate the Bidder /Seller for damages, if any. Subject to Clause 5, any lawful payment due to the Bidder/Seller for supplies effected till date of termination would be made in normal course.
- (iv) To encash EMD /Advance Bank Guarantees / Performance Bonds / Warranty Bonds, etc. which may have been furnished by the Bidder /Seller to the extent of the undelivered Stores and / or Services.

8.2 If the Buyer obtains Knowledge of conduct of Bidder /Seller or of an employee or representative or an associate of Bidder /Seller which constitutes corruption, or if the Buyer has substantive suspicion in this regard, the Buyer will inform to its Chief Vigilance Officer.

9. Compensation for Damages

9.1 If the Buyer has disqualified the Bidder(s) /Seller(s) from the tender process prior to the award according to Clause 8, the Buyer is entitled to demand and recover the damages equivalent to Earnest Money Deposit in case of open tendering.

9.2 If the Buyer has terminated the contract according to Clause 8, or if the Buyer is entitled to terminate the contract according to Clause 8, the Buyer shall be entitled to encash the advance bank guarantee and performance bond / warranty bond, if furnished by the Bidder / Seller, in order to recover the payments, already made by the Buyer for undelivered Stores and / or Services.

10. Price Fall Clause

The Bidder undertakes that it has not supplied /is not supplying same or similar product/systems or subsystems at a price lower than that offered in the present Bid in respect of any other Ministry /Department of the Government of India or PSU or Coal India Ltd and its subsidiaries during the currency of the contract and if it is found at any stage that same or similar product /Systems or Subsystems was supplied by the Bidder to any other Ministry /Department of the Government of India or a PSU or any Public Sector Bank at a lower price during the currency of the contract, then that very price will be applicable to the present case and the difference in the cost would be refunded by the Bidder to the Buyer, if the contract has already been concluded”.

11. Independent External Monitor(s)

11.1 The Buyer has appointed independent External Monitors for this Integrity Pact in consultation with the Central Vigilance Commission (Names and Addresses of the Monitors are given in RFP).

11.2 As soon as the integrity Pact is signed, the Buyer shall provide a copy thereof, along with a brief background of the case to the independent External Monitors.

11.3 The Bidder(s) / Seller(s) if they deem it necessary, may furnish any information as relevant to their bid to the Independent External Monitors.

11.4 If any complaint with regard to violation of the IP is received by the buyer in a procurement case, the buyer shall refer the complaint to the Independent External Monitors for their comments / enquiry.

11.5 If the Independent External Monitors need to peruse the records of the buyer in connection with the complaint sent to them by the buyer, the buyer shall make arrangement for such perusal of records by the independent External Monitors.

11.6 The report of enquiry, if any, made by the Independent External Monitors shall be submitted to MD & CEO, Union Bank of India, Union Bank Bhavan, Vidhan Bhavan Marg, Nariman Point, Mumbai -21 within 2 weeks, for a final and appropriate decision in the matter keeping in view the provision of this Integrity Pact.

12. Law and Place of Jurisdiction

This Integrity Pact is subject to Indian Laws, and exclusive Jurisdiction of Courts at Mumbai, India.

13. Other Legal Actions

The actions stipulated in this Integrity Pact are without prejudice to any other legal action that may follow in accordance with the provision of the extant law in force relating to any civil or criminal proceedings.

14. Integrity Pact Duration.

14.1 This Integrity Pact begins when both parties have legally signed it. It expires for the successful Bidder / Seller 10 months after the last payment under the contract, and for all other Bidders / Sellers within 6 months form date of placement of order / finalization of contract.

14.2 If any claim is made/ lodged during this time, the same shall be binding and continue to be valid despite the lapse of this Integrity Pact as specified above, unless it is discharged / determined by MD & CEO, Union Bank of India.

14.3 Should one or several provisions of this Integrity Pact turn out to be invalid, the reminder of this Integrity Pact remains valid. In this case, the parties will strive to come to an agreement to their original intentions.

15 Other Provisions

15.1 Changes and supplements need to be made in writing. Side agreements have not been

made.

15.2 The Bidders (s)/ Sellers (s) signing this IP shall not initiate any Legal action or approach any court of law during the examination of any allegations/complaint by IEM and until the IEM delivers its report.

15.3 In view of nature of this Integrity Pact, this Integrity Pact shall not be terminated by any party and will subsist throughout its stated period.

15.4 Nothing contained in this Integrity Pact shall be deemed to assure the bidder / Seller of any success or otherwise in the tendering process.

16. This Integrity Pact is signed with Union Bank of India exclusively and hence shall not be treated as precedence for signing of IP with MoD or any other Organization.

17. The Parties here by sign this Integrity Pact at _____ on _____
(Seller/Bidder) and _____ on _____ (Buyer)

BUYER

BIDDER * /SELLER*

Signature:

Signature:

General Manager/Dy G M,
Union Bank of India,
..... Division

Authorized Signatory (*)

Date:
Stamp:

Date:
Stamp:

Witness

Witness

1. _____

2. _____

1. _____

2. _____

(*) - Authorized signatory of the company who has also signed and submitted the main bid.

75. Annexure N - Letter for Refund of EMD

LETTER FOR REFUND OF EMD
(To be submitted by the unsuccessful bidders)

Date:

The General Manager,
Union Bank of India,
Technology Centre,
1/1A, Adi Shankaracharya Marg, Opp. Powai Lake,
Powai, Andheri (East),
Mumbai-400072.

We _____ (Company Name) had participated in the Request for Proposal (RFP) for Network Management support services for Wide Area Network of the Bank and we are an unsuccessful bidder.

Kindly refund the EMD submitted for participation. Details of EMD submitted are as follows

Sr. No.	Bidder Name	DD/EMD Number	Drawn on (Bank Name)	Amount (Rs)

Bank details to which the money needs to be credited via NEFT are as follows

1. Name of the Bank with Branch
2. Account Type
3. Account Title
4. Account Number
5. IFSC Code

Sign

Name of the signatory

Designation

Company Seal.

76. Annexure O - Bid Query Format

Bidders have to provide their queries on eligibility criteria, scope of work, terms & conditions etc. in excel format as mentioned below. Bidders are requested to categorize their queries under appropriate headings. Bidders are requested to provide a reference of the page number, state the clarification point and the queries/suggestion/deviation that they propose as shown below (all the queries will be entertained only in Microsoft Excel in the following format by e-mail):

Queries will not be accepted in any other format other than Microsoft Excel.

Sl. No.	Clause no.	Page no.	Clause	Query	Bank Response

Place:

Date:

Signature:

Name & Designation:

Business Address:

77. Annexure P - Bank Guarantee for EMD

Date:

To

Union Bank of India,
Department of Information Technology,
1/1A, Adi Shankaracharya Marg, JVLR,
Opp. Powai Lake (Andheri East),
Powai (Andheri East), Mumbai 400072.

Dear Sir,

M/s _____ having their registered office at _____ (hereinafter called the 'Bidder') wish to respond to the Request for Proposal (RFP) for Network Management support services for Wide Area Network of the Bank, self and other associated Bidders and submit the proposal for the same as listed in the RFP document.

Whereas the 'Bidder' has submitted the proposal in response to RFP, we, the _____ Bank having our head office _____ hereby irrevocably guarantee an amount of Rs.1,50,00,000.00 (Rupees One Crore fifty lac Only) as bid security as required to be submitted by the 'Bidder' as a condition for participation in the said process of RFP.

The Bid security for which this guarantee is given is liable to be enforced/ invoked:

1. Withdraws its bid during bid validity period
2. Refuses to honor commercial bid. Bank reserves the right to place order onto Bidder based on prices quoted by them.
3. Refuses to accept purchase order or having accepted the purchase order, fails to carry out his obligations mentioned therein

We undertake to pay immediately on demand, to Union Bank of India, the said amount of Rs.1,50,00,000.00 (Rupees One Crore Fifty Lac Only) without any reservation, protest, demur, or recourse. The said guarantee is liable to be invoked/ enforced on the happening of the contingencies as mentioned above and also in the RFP document and we shall pay the amount on any Demand made by Union Bank of India which shall be conclusive and binding on us irrespective of any dispute or difference raised by the Bidder.

Notwithstanding anything contained herein:

- 1) Our liability under this Bank guarantee shall not exceed Rs. 1,50,00,000.00 (Rupees One Crore fifty lac Only).
- 2) This Bank guarantee will be valid up to _____; with a claim period of 45 days thereafter and
- 3) We are liable to pay the guarantee amount or any part thereof under this Bank guarantee only upon service of a written claim or demand by you on or before _____.

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

Signature

Name

(In Block letters)

Designation

(Staff Code No.)

Official address:

(Bank's Common Seal)

Attorney as per power of Attorney No.

Date:

WITNESS:

1..... (Signature with Name, Designation & Address)

2..... (Signature with Name, Designation & Address)

78. Annexure Q - Format of Performance Bank Guarantee (Covering Delivery obligations)

NOTE:

1. This guarantee should be furnished by a Nationalized Bank / Scheduled Bank, other than Union Bank of India, as per the following format.
2. This bank guarantee should be furnished on stamp paper value as per Stamp Act. (not less than Rs.500/-).
3. The stamp paper should be purchased either in the Name of the Bank executing the Guarantee or in the name of Union Bank of India.
4. This Bank Guarantee should be furnished within 30 days from the date of purchase order or the delivery period prescribed in the purchase order whichever is earlier.
5. This Bank Guarantee should be directly sent to the Bank by the Issuing Bank under Registered Post with Acknowledge Due.

To
Union Bank of India,
5th floor, Technology Centre, Union Bank of India,
Adi Shankaracharya Marg, Opp. Powai Lake,
Powai, Andheri (East),
Mumbai-400072.

Dear Sir,

In consideration of Union Bank of India, Technology Centre, Adi Shankaracharya Marg, Opp. Powai Lake, Powai, Andheri (East), Mumbai-400072, placing an order for Implementation of & on _____ having registered office at _____ (hereinafter called the vendor) as per the purchase contract entered into by the vendor vide purchase contract no _____ dated _____ (hereinafter called the said contract), we _____ (Name of the Guarantor Bank), a 'schedule bank', issuing this guarantee through its branch at _____ presently located at _____ (hereinafter called the bank), do hereby irrevocably and unconditionally guarantee the due performance of the vendor as to the) for Network Management support services for Wide Area Network of the Bank as per the said contract entered into by the vendor with you.

If the said vendor fails to implement or maintain the system or any part thereof as per the contract and on or before the schedule dates mentioned therein, we _____ (Name of the Guarantor Bank), do hereby unconditionally and irrevocably agree to pay the amounts due and payable under this guarantee without any demur and merely on demand in writing from you during the currency stating that the amount claimed is due by way of failure on the part of the vendor or loss or damage caused to or suffered / or would be caused to or suffered by you by reason of any breach by the said vendor of any of the terms and conditions of the said contract, in part or in full. Any such demand made on us shall be conclusive as regards the amount due and payable under this guarantee.

We _____ (Name of the Guarantor Bank), further agree that this guarantee shall continue to be valid will you unless you certify that the vendor has fully performed all the terms and conditions of the said contract and accordingly discharge this guarantee, or until _____, whichever is earlier. Unless a claim or demand is made on us in writing under this guarantee on or before _____, we shall be discharged from all our obligations under this guarantee. If you extend the schedule dates of performance under the said contract, as per the terms of the said contract, the vendor shall get the validity period of this guarantee extended suitably and we agree to extend the guarantee accordingly at the request of the vendor and at our discretion, provided such request is served on the bank on or before _____. Failure on part of the vendor in this respect shall be treated as a breach committed by the vendor

and accordingly the amount under this guarantee shall at once become payable on the date of receipt of demand made by you for payment during the validity of this guarantee or extension of the validity period.

You will have fullest liberty without affecting this guarantee to postpone for any time or from time to time any of your rights or powers against the vendor and either to enforce or forebear to enforce any or all of the terms and conditions of the said contract. We shall not be released from our liability under this guarantee by the exercise of your liberty with reference to matters aforesaid or by reason of any time being given to the vendor or any other forbearance act or omission on your part or any indulgence by you to the vendor or by any variation or modification of the said contract or any other act, matter or thing whatsoever which under the law relating to sureties would but for the provisions hereof have the effect of so releasing us from our liability hereunder.

In order to give full effect to the guarantee herein contained you shall be entitled to act as if we are your principal debtors in respect of all your claims against the vendor hereby guaranteed by us as aforesaid and we hereby expressly waive all our rights of surety ship and other rights if any which are in any way inconsistent with the above or any other provision of this guarantee.

The words the vendor, the beneficiary of this guarantees i.e. Yourself, and ourselves i.e. _____ (Name of the Guarantor Bank), unless repugnant to the context or otherwise shall include their assigns, successors, agents, legal representatives. This guarantee shall not be effected by any change in the constitution of any of these parties and will ensure for and be available to and enforceable by any absorbing or amalgamating or reconstituted company or concern, in the event of your undergoing any such absorption, amalgamation or reconstitution.

This guarantee shall not be revocable during its currency except with your prior consent in writing. This guarantee is non-assignable and non-transferrable.

Notwithstanding anything contained herein above:

- I) Our liability under this bank guarantee shall not exceed 10% of the TCO.
- II) This bank guarantee shall be valid up to _____.
- III) We are liable to pay the guaranteed amount or any part thereof under this bank guarantee only if you serve upon us a written claim or demand (and which should be received by us), on or before _____ before 12:00 hours (Indian standard time) where after it ceases to be in effect in all respects whether or not the original bank guarantee is returned to us.

This guarantee deed must be returned to us upon expiration of the period of guarantee.

Signature

Name

(In Block letters)

Designation

(Staff Code No.)

Official address:

(Bank's Common Seal)

Attorney as per power of Attorney No.

Date:

WITNESS:

1..... (Signature with Name, Designation & Address)

2..... (Signature with Name, Designation & Address)

79. Annexure R - Know Your Employee (KYE) Clause

(Bidder has to submit Undertaking on company letter head as per format given below).

1. We _____ (name of the company) hereby confirm that all the Resource (both on-site and off-site) deployed/to be deployed on Bank's project for _____ (Name of the RFP) have undergone KYE (Know Your Employee) process and requisite checks have been performed prior to employment of said employees as per our policy.
2. We undertake and agree to save defend and keep harmless and indemnified the Bank against all loss, cost, damages, claim penalties expenses, legal liability because of non compliance of KYE and of misconduct of the employee deployed by us to the Bank.
3. We further agree to submit the required supporting documents (Process of screening, Background verification report, police verification report, character certificate, ID card copy, Educational document, etc) to Bank before deploying officials in Bank premises for _____ (Name of the RFP)."

Signature of Competent Authority with company seal _____
Name of Competent Authority _____
Company / Organization _____
Designation within Company / Organization _____
Date _____

Name of Authorized Representative _____
Designation of Authorized Representative _____
Signature of Authorized Representative _____
Verified above signature _____
Signature of Competent Authority _____
Date _____

80. Annexure S - Existing Infrastructure to be Managed by the selected NSI

The list given here is the tentative and exhaustive:

Asset Details

Sl. No.	Assets	Location	Count
1.	Juniper QFX 10002 Spine switch	DC	2
2.	Juniper QFX 5100 Leaf Switch	DC	14
3.	Cisco Nexus 9K Switches	DC	12
4.	Cisco Nexus 9K Switches	NDC	4
5.	Cisco Nexus 9K Switches	DR	12
6.	Cisco Nexus 3K Switches	DC	2
7.	Cisco Nexus 3K Switches	DR	2
8.	Huawei Router	DC	3
9.	Huawei Router	NDC	2
10.	Huawei Router	DR	3
11.	Huawei Switches	DC	2
12.	Cisco L2 switches	DC, DR & NDC	Multiple
13.	Cisco L3 switches	DC, DR & NDC	Multiple

Configuration and other required details shall be shared with finally selected bidder.

81. Annexure T - Resource Details of NSI

(To be submitted on the letter head of the vendor company signed by the Authorized person)

Sl No.	Name of the Engineer	Designation	Qualification	No. of Years in the organization
1				
.				
.				
.				
100				

Place:

Date:

Seal & Signature

Note: NSI has to identify and inform the minimum 10 engineers with their qualification and experience who are proposed to be deployed for the implementation of this project.

82. Annexure U - Undertaking of Information Security

(This letter should be on the letterhead of the bidder as well as the OEM/ Manufacturer duly signed by an authorized signatory on Information security as per regulatory requirement)

Place:

Date:

To:

The General Manager,
Union Bank of India,
5th floor, Technology Centre,
1/1A, Adi Shankaracharya Marg, Opp. Powai Lake,
Powai, Andheri (East),
Mumbai-400072.

Sir,

Subject: Request for Proposal (RFP) for Network Management support services for Wide Area Network of the Bank.

We hereby undertake that the proposed solution / software to be supplied will be free of malware, free of any obvious bugs and free of any covert channels in the code (of the version of the application being delivered as well as any subsequent versions/modifications done)

Yours faithfully,

Authorized Signatory

Name:

Designation:

Vendor's Corporate Name

Address

Email and Phone #

83. Annexure V - List of Regional Offices

Sr. No.	Regional Offices
1	RO, Agra
2	RO, Ahmedabad
3	RO, Allahabad
4	RO, Azamgarh
5	RO, Bengaluru
6	RO, Baroda
7	RO, Belgaum
8	RO, Bhopal
9	RO, Bhubaneshwar
10	RO, Chandigarh
11	RO, Chennai
12	RO, Coimbatore
13	RO, Dehradun
14	RO, Delhi (North)
15	RO, Delhi (South)
16	RO, Durgapur
17	RO, Ernakulam
18	RO, Ghazipur
19	RO, Goa
20	RO, Gorakhpur
21	RO, Guwahati
22	RO, Gwalior
23	RO, Howrah
24	RO, Hyderabad
25	RO, Indore
26	RO, Jabalpur
27	RO, Jaipur
28	Ro, Jalandhar
29	Ro, Jaunpur
30	Ro, Kanpur
31	Ro, Karnal
32	RO, Kolhapur
33	RO, Kolkata
34	RO, Kottayam
35	RO, Kozhikode
36	RO, Lucknow
37	RO, Ludhiana
38	RO, Madurai
39	RO, Mangalore
40	RO, Meerut
41	RO, Mehsana

Sr. No.	Regional Offices
42	RO, Mumbai (North)
43	RO, Mumbai (South)
44	RO, Mumbai (West)
45	RO, Nagpur
46	RO, Nashik
47	RO, Nellore
48	RO, Patna
49	RO, Pune
50	RO, Raipur
51	RO, Rajkot
52	RO, Ranchi
53	RO, Rewa
54	RO, Salem
55	RO, Samastipur
56	RO, Sambalpur
57	RO, Siliguri
58	RO, Surat
59	RO, Trivandrum
60	RO, Udaipur
61	RO, Varanasi
62	RO, Vijayawada
63	RO, Visakhapatnam

84. Annexure W - Certificate of Local Content

(Certificate from the statutory auditor or cost auditor of the company (in case of companies) or from a practicing cost accountant or practicing chartered accountant (in respect of suppliers other than companies) giving the percentage of local content, on their letter head with Registration Number with seal.)

Date:

To,

Dear Sir,

Ref.: RFP No.: _____ Dated: _____

1. This is to certify that proposed _____ <product details> is having the local content of _____ % as defined in the above-mentioned RFP.
2. This certificate is submitted in reference to the Public Procurement (Preference to Make in India), Order 2017 - Revision vide Order No. P-45021/2/2017-PP (BE-II) dated May 28, 2018.

**Signature of Statutory Auditor/
Cost Auditor**
Registration Number:
Seal

Counter-signed:**Bidder****OEM**

85. Annexure X - Standard Terms and Conditions for Outsourcing

Introduction

- A. The purpose of these standard terms and condition for Outsourcing Contracts (hereinafter referred to as the "standard Terms and conditions") is to set forth the terms and conditions applicable to the, outsourcing agreement executed between the Service Provider and the Bank.
- B. If any provisions of the standard terms and conditions is inconsistent with any provision of the outsourcing agreement, of which the Standard terms and conditions constitute an integral part, the provision of standard terms and conditions shall prevail,

1. Representations and Warranties:

The following representation and warranties shall be deemed to have been given by the Service Provider in relation to outsourcing contracts upon the contracts being executed.

In order to induce UBI to enter into the Contract / Agreement, the Service Provider hereby represents and warrants as of the date hereof, which representations and warranties shall survive the term and termination hereof, the following:

- 1.1 That the Service Provider is a company/firm which has the requisite qualifications, skills, experience and expertise in providing all such services as are necessary to perform its obligation under the contract/agreement and the financial wherewithal, the power and the authority to enter into the Contract / Agreement and provide the *Service(s)/Systems* sought by UBI.
- 1.2 That the service Provider is not owned or controlled by any director or officer I employee of the UBI or by related party having the same meaning as assigned under sec 2(76) of the Companies Act or their relatives having the same meaning as assigned under' section 2(77) of the Companies Act 2013 read with rule 4 of the companies (specification of definition details) Rules 2014.
- 1.3 That the Service provider is not involved in any major litigation, potential, threatened and existing, that may have an impact of affecting or compromising the performance and delivery of *Service(s) / Systems* under the Contract / Agreement.
- 1.4 That the Service provider shall use such assets of UBI as the UBI may permit for the sole purpose of execution of its obligations under the terms of the bid, Tender or the Contract / Agreement. The Service provider shall however, have no claim to any right, title, lien or other interest in any such property, and any possession of property for any duration whatsoever shall net create any right in equity or otherwise, merely by fact of such use or possession during or after the term hereof.
- 1.5 That the Service provider shall procure all the necessary permissions and adequate approvals and licenses for use of various software and any copyrighted process/product free from all claims, titles, interests and liens thereon and shall keep UBI, its directors, officers, employees, representatives, consultants and agents indemnified in relation thereto.
- 1.6 That the execution of the *Service(s)* herein is and shall be in accordance and in compliance with all applicable laws as amended from time to time.

- 1.7 That there are - (a) no legal proceedings pending or threatened against Service provider or its team which adversely affect/may affect performance under this Contract / Agreement; and (b) no inquiries or investigations have been threatened, commenced or pending against the Service provider or any sub-Service provider / third part or its team members by any statutory or regulatory or investigative agencies.
- 1.8 That neither the execution and delivery by the Service provider of the Contract / Agreement nor the Contractor's compliance with or performance of the terms and provisions of the Contract / Agreement (i) will contravene any provision of any applicable law or any order, writ, injunction or decree of any court or governmental authority binding on the Service provider (ii) will conflict or be inconsistent with or result in any breach of any or the terms, covenants, conditions or provisions of, or constitute a default under any agreement, contract or instrument to which the Service provider is a party or by which it or any of its property or assets is bound or to which it may be subject or (iii) will violate any provision of the Memorandum and Articles of Association of the Contractor.
- 1.9 The Service provider shall not charge any fees to the customers of the UBI directly for the services rendered by them on behalf of the UBI.
- 1.10 The service provider shall not sell/ compel the customers of the UBI to buy third party products along with the UBI's product.

2. Compliance Requirements

The service provider by executing the outsourcing agreement shall be deemed to have unconditionally agreed as under:

- 2.1. The entire activity and Services would be guided by and conform to policies and guidelines of the UBI, Reserve Bank of India, IDRBT, State and Central Governments, legal provisions etc.
- 2.2. Information Security standards for end-to-end solution would conform to ISO 27001, CERT-In guidelines, IT Act 2000, The information Technology (Reasonable Security Practices and Procedures and Sensitive personal data or Information) Rules, 2011 ("IT SPD Rules), RBI, Government, IDRBT and UBI's policies.
- 2.3. The business practices, processes adopted for rendering services, maintenance of records, accounting norms & procedures etc for Banking and financial services shall conform to regulatory, legal and UBI's policies and guidelines.

3. Subcontracting

The service provider by executing the outsourcing agreement shall be deemed to have unconditionally agreed as under:

It is agreed between the parties that service provider shall not procure services either through subcontract without the prior written permission of the UBI. If subcontracting is permitted by the UBI then;

Service provider shall be responsible for all the services provided to the UBI regardless of which entity is conducting the operations on behalf of contractor. The Service provider shall be responsible for managing the activities of its personnel and/or the personnel of subservice provider and under no circumstances and at no, point of time the subservice provider of the Service provider will be considered employees, subservice provider or agent of UBI. The Service provider shall be responsible for ensuring that the Sub-Contractor comply with all security & confidentiality requirement of the UBI set out in this agreement and the UBI can obtain independent report for the same.

4. Human Resource Requirement

The service provider by executing the outsourcing agreement shall be deemed to have unconditionally agreed as under:

- 4.1. The Service provider shall provide a contingent of well trained personnel and extend necessary mentoring and operational support to the intermediary network of agents, etc. as part of the solution/service.
- 4.2. The Service provider shall confirm that every person deployed by them on the project has been vetted through a third-party background check prior to their engagement. The Service provider shall manage the activities of its personnel or others engaged in the project, etc and shall be accountable for all the personnel deployed/engaged in the project.
- 4.3. In case the performance of the Business Correspondents/their CSPI agent/ employees engaged in the project is not satisfactory or is detrimental to the interests of the UBI, The Service provider shall have to replace the said person within the time limits stipulated by the UBI. Where the Service provider fails to comply with the UBI's request, UBI may replace the said person, Business Correspondent or their agents/employees on its own.
- 4.4. No right to employment in the UBI shall accrue or arise to the employees or agents of the Service provider, by virtue of engagement of employees, agents, etc. of The Service provider for any assignment under this project. It is further clarified that the arrangement herein with the Service provider is a contract for service.
- 4.5. The Service provider shall exercise due diligence and only engage persons having established identity, integrity, requisite qualifications and skills and deployment experience for all critical activities.
- 4.6. The Service provider shall extend all of the outsourced Banking and financial services by deploying such personal that have high integrity and meet the qualifications and other criteria stipulated by the Reserve UBI of India, Government or the UBI from time to time and agrees and undertake that during the subsistence of this agreement they will not employ any personnel/individual below the Minimum Wages fixed by appropriate Government on this behalf from time to time, as per the provisions of Minimum Wages Act 1948.

5. Service Levels

The service provider by executing the outsourcing agreement shall be deemed to have unconditionally agreed as under:

- 5.1. The Service provider shall proceed to carry out the Service(s) with diligence and care in accordance with any stipulation as to the time, manner, mode, and method of execution contained in the Contract / Agreement and shall meet the standards of good industry practice.
- 5.2. Notwithstanding generality of the foregoing, the Service provider shall achieve the service levels and key performance matrixes stipulated by UBI under the contract.
- 5.3. Standard of Performance

The Service provider shall perform the Service(s) and carry out its obligations under the Contract with due diligence, efficiency and economy, in accordance with generally accepted techniques and practices used in industry and with professional engineering standards recognized by the international professional bodies and shall observe sound management, technical and engineering

practices. It shall employ appropriate advanced technology, procedures and methods. The Service provider shall always act, in respect of any matter relating to the Contract, as faithful advisors to UBI and shall, at all times, support and safeguard UBI's legitimate interests in any dealing with third parties.

5.4. Key Performance Measurements

Unless specified by UBI to the contrary, the Service provider shall perform the Service(s) and carry out the Service(s) under and in accordance with the terms of the Contract / Agreement and as per the good industry practice.

5.5. Reporting Progress

The Service provider shall monitor progress of all the activities specified in the program of work! Service(s) and submit free of cost weekly progress report about various aspect of the work/Service(s) to UBI. UBI on mutual agreement between both Parties may change the periodicity of such reports.

6. Intellectual Property Rights and Patent Rights, Information Security and confidentiality

The service provider by executing the outsourcing agreement shall be deemed to have unconditionally agreed as under:

- 6.1. Purchaser/UBI shall own and have a right in perpetuity to use all Intellectual Property Rights which have arisen out of or in connection with the Implementation of the Contract, if any, including all processes products and Services which have been developed by the Service provider during the Performance of Service(s) and for the purposes of inter-alia, use or sublicense of such service(s) under the Contract. The Service provider undertakes to disclose all Intellectual Property Rights arising out of or in connection with the performance of the service(s) to UBI and execute all such agreements /documents and file all relevant applications, effect transfers and obtain all permits, approvals consents and no objections that may be necessary in this regard to effectively transfer and conserve the Intellectual Property Rights of UBI.
 - 6.1.1. Further the service provider shall be obliged to ensure that all approvals, consents, no objections, registrations, licenses, permits and rights which are inter-alia necessary for use of the information technology system installed by the contractor, shall be acquired in the name of UBI, prior to termination of the Contract and which shall be assigned by UBI if necessary under the applicable laws or otherwise to the Service provider for the purpose of execution of any of its obligations under the terms of the bid, or the Contract. However, Subsequent to the term of the Contract, such approvals, consents, no objections, registrations, licenses, permits and rights etc., shall ensure to the exclusive benefit of UBI.
 - 6.1.2. The Service provider shall ensure that while it uses any software, hardware, Processes or material in the course of performing the service(s), it does not infringe the Intellectual Property Rights of any person and the Service provider shall keep the UBI, its directors, employees, agents and representatives indemnified against all costs, charges, expenses, liabilities, claims, damages, litigations, suits, judgments and / or otherwise howsoever, arising out of any illegal or unauthorized use (piracy) or in connection with any claim or proceedings relating to any breach or violation of any permission/license terms or infringement of any Intellectual Property Rights by the Service provider or any sub-Service provider during the course of performance of the service(s).

6.2. Information Security

- 6.2.1. The Service provider and its personnel shall not carry any written material, layout, diagrams, floppy diskettes, hard disk, storage tapes or any other media out of UBI's premises without written permission from UBI.
- 6.2.2. The Service provider personnel shall follow UBI's information security policy and instructions in this behalf.
- 6.2.3. The Service provider acknowledges that UBI's business data and other proprietary information or materials, whether developed by UBI or being used by UBI pursuant to a license agreement with a third party (the foregoing collectively referred to herein as "proprietary information") are confidential and proprietary to UBI; and the Service provider agrees to use reasonable care to safeguard the proprietary information and to prevent the unauthorized use or disclosure thereof, which care shall not be less than that used by Service provider to protect its own proprietary information. Service provider recognizes that the goodwill of UBI depends, among other things, upon Service provider keeping such proprietary information confidential and that unauthorized disclosure of the same by Service provider could damage UBI. By reason of Contractor's duties and obligations hereunder, Service provider may come into possession of such proprietary information, even though the Service provider does not take any direct part in or furnish the Service(s) performed for the creation of said proprietary information and shall limit access thereto to employees with a need to such access to perform the Services required by the Contract / Agreement. Service provider shall use such information only for the purpose of performing the Service(s).
- 6.2.4. Service provider shall upon termination of the Contract / Agreement for any reason, or upon demand by UBI / Purchaser, whichever is earlier, return any and all information provided to Service provider by UBI, including any copies or reproductions, both hardcopy and electronic.

6.3. Ownership and Retention of Documents

- 6.3.1. UBI shall own the documents, prepared by or for the Service provider arising out of or in connection with the Contract / Agreement. The services provider shall preserve the documents and data in accordance with the legal/regulatory obligation of the UBI.
- 6.3.2. Forthwith upon expiry or earlier termination of the Contract / Agreement and at any other time on demand by UBI, the Service provider shall deliver to UBI all documents provided by or originating from UBI and all documents produced by or from or for the Service provider in the course of performing the Service(s), unless otherwise directed in writing, by UBI at no additional cost. The Service providers shall not, without the prior written consent of UBI store, copy, distribute or retain any such Documents.

6.4. Data Ownership

By virtue of the Contract / Agreement, the Contractor's team may have access to personal and business information of UBI and / or a third party. UBI have the sole ownership of and the right to use, all such data in perpetuity including any data or other information pertaining to the subscriber that may be in the possession of the Service provider or Contractor's team in the course of performing the Service(s) under the Contract / Agreement.

a. Confidentiality

The service provider hereby represents and warrants that they shall ensure the preservation and protection of the security and confidentiality of the beneficiary/customer information or data which are in the custody or possession of the service provider. They further represent and warrants

that they shall ensure the preservation and protection of the sensitive personal data or information as defined/laid down in "The information Technology (Reasonable Security Practices and Procedures and Sensitive Personal data or information) Rules, 2011" ("IT SPD Rules).

The Parties agree that they shall hold in trust any Confidential Information received by either Party, under the Contract / Agreement, and the strictest of confidence shall be maintained in respect of such Confidential Information. The Parties also agree:

- a) to maintain and use the Confidential Information only for the purposes of the Contract / Agreement and only as permitted herein;
- b) to only make copies of such documents / papers as specifically authorized by the prior written consent of the other party and with the same confidential or proprietary notices as may be printed or displayed on the original;
- c) to restrict access and disclosure of Confidential information to such of their employees, agents, service providers, and Service providers strictly on a "need to know" basis, to maintain confidentiality of the Confidential Information disclosed to them in accordance with this Clause and d) In the event of earlier termination of the Contract I Agreement, the Parties hereby agree to maintain the confidentiality of the Confidentiality obligation shall survive the termination of this agreement.

Confidential Information does not include information which:

- i. the recipient knew or had in its possession, prior to disclosure, without limitation on its confidentiality;
- ii. information in the public domain as a matter of law;
- iii. is received from a third party not subject to the obligation of confidentiality with respect to such information;
- iv. is released from confidentiality with the written consent of the other Party.

The recipient shall have the burden of proving that Clauses (i) or (ii) above are applicable to the information in the possession of the recipient. Notwithstanding the foregoing, the Parties acknowledge that the nature of the Service(s) to be performed under this Contract / Agreement may require the Service provider's personnel to be present on premises of UBI or may require the Service provider's personnel to have access to computer networks and databases of UBI while on or off premises of UBI. It is understood that it would be impractical for UBI to monitor all information made available to the Service provider under such circumstances and to provide notice to the Service provider / Service provider of the confidentiality of all such information. Therefore, the Service provider agrees that any technical or business or other information of the other party that the Contractor's personnel, sub Service providers, or agents acquire while on the UBI's premises, or through access to UBI's computer systems or databases while on or off UBI's premises, shall be deemed Confidential Information. Confidential Information shall at all times remain the sole and exclusive property of the Disclosing Party. Upon termination of the Contract / Agreement, Confidential Information shall be returned to the disclosing Party or destroyed, if incapable of return. The destruction shall be witnessed and so recorded, in writing, by an authorized representative of each of the Parties. Nothing contained herein shall in any manner impair rights of UBI in respect of the Systems, Service(s), and Documents etc.

In the event that any of the Parties hereto becomes legally compelled to disclose any Confidential Information, such Party shall give sufficient notice to the other Party to enable the other Party to prevent or minimize to the extent possible, such disclosure. Neither party shall disclose to a third party any Confidential Information or the contents of the Contract / Agreement without the prior

written consent of the other Party. The obligations of this Clause shall be satisfied by handling Confidential Information with the same degree of care, which the receiving Party applies to its own similar confidential information but in no event less than reasonable care. The obligations of this Clause shall survive the expiration, cancellation or termination of this Contract / Agreement. The provision of this clause shall survive termination of the Contract / Agreement till such Confidential Information enters public domain and as stated above.

7. UBI's/Reserve Bank of India's Right of Inspection and Periodic Audit

The service provider by executing the outsourcing agreement shall be deemed to have unconditionally agreed as under:

- 7.1. UBI/Reserve Bank of India reserves the right to inspect and monitor/assess the progress of the Services at any time during the course of the Contract / Agreement. UBI may demand and upon such demand being made, UBI shall be provided with any document, data, material or any other information, which it may require, to enable it to assess the progress of the Services.
- 7.2. The project shall confirm to UBI/Reserve Bank of India's policies and would be subject to Internal and External audits or agents appointed to act on its behalf and to obtain copies of any audit or review reports and findings made on the service provider in conjunction with the services performed for the UBI.
- 7.3. The Service provider shall allow the Reserve Bank of India or persons authorized by them to access the UBI/service provider's documents; records & service providers' transactions and other necessary information given to or stored or processed by the service provider within a reasonable time. In the event these are not made accessible to Reserve Bank of India within a reasonable time, the service provider will reimburse the UBI which they may be liable to pay supervisory fees to Reserve Bank of India.
- 7.4. The Service provider is required to extend all necessary co-operations to facilitate audit process.
- 7.5. The Service provider shall have adequate audit controls and track normal and exception transactions.
- 7.6. UBI shall utilize the services of internal or external auditors for ensuring proper operations by the Service provider.
- 7.7. UBI/Reserve Bank of India shall also arrange for a random verification for better control and shall have the right to review and monitor the security practices and control processes of the service provider on regular basis and require the service provider to disclose security breaches if any.
- 7.8. The UBI/Reserve Bank of India reserve its right to inspect and monitor/access the progress/activities of the services and Complaint Register and other related documents at any time during the course of the contract / agreement. UBI / Reserve Bank of India may demand and upon such demand being made, UBI / Reserve Bank of India shall be provided with any document, data, material, Complaint Register or any other information, which it may require, to enable it to access the activity, details of compliant redressals and progress of the services.

8. Review of Contract and Performance

The service provider by executing the outsourcing agreement shall be deemed to have unconditionally agreed as under;

- 8.1. UBI shall have the right of periodic review of the performance of the Service provider under the contract which would be basis of continuation or termination of the same. UBI on mutual agreement between both Parties may change the periodicity of such review.
- 8.2. UBI shall also have the right to review, either itself or through another Agency as it may deem fit, the financial and operating performance of the service provider in order to assess the ability of the Service provider to continue to meet its outsourcing/contractual obligations.

9. Delay in the Contractor's Performance

The service provider by executing the outsourcing agreement shall be deemed to have unconditionally agreed as under:

- 9.1. Time is the essence of contract. Time period for delivery, installation and Implementation will be drawn up by the UBI or as given in the contract and service provider should adhere to the schedule and complete the project within given time. Performance of the Contract shall be made by the Service provider in accordance with the time schedule specified by UBI. UBI will impose following penalties apart from the liquidated damages termination of contract etc and will be recovered from the Service provider from his payment.
- 9.2. A delay by the Service provider in the performance of its Contract obligations shall render the Service provider liable to any or all the following sanctions:
- a) Forfeiture of its performance Bank guarantee if any,
 - b) Imposition of liquidated damages and penalties, and /or
 - c) Termination of the Contract for default.

10. User Acceptance Test and Quality Check

The service provider by executing the outsourcing agreement shall be deemed to have unconditionally agreed as under:

- 10.1. UBI or its representative shall have the right to inspect and/or to test the goods and Services to check their conformity to the Contract specifications at no extra cost to the UBI.
- 10.2. The inspections and test may be conducted on the premises of the Contractor, at point of delivery and / or at the final destination. If conducted on the premises Of the Contractor, all reasonable facilities and assistance, including access to drawings and production data, shall be furnished to the inspectors at no charge to the UBI.
- 10.3. Should any inspected or tested goods fail to conform to the specifications, UBI may reject the goods, and the Service provider shall either replace the rejected goods or make alterations necessary to meet specification requirements free of cost to UBI.
- 10.4. Pre-delivery /acceptance Inspection will be carried out by the UBI through its staff / consultant at Contractor's factory / warehouse or at any of the UBI's site / Location depending on the exigencies of UBI. The Service provider shall keep ready the equipment for inspection if the inspection is carried out at UBI's Site, the Service provider should provide all assistance including manpower. There shall not be any additional charges for such inspection. However, UBI will have the discretion to recover the costs related to travel and stay of its staff / consultants.

11. Business Continuity Plan

The service provider by executing the outsourcing agreement shall be deemed to have unconditionally agreed as under:

- 11.1. The parties shall comply with the provisions of the Business Continuity Plan and the Service provider shall ensure that it is able to implement the Business Continuity Plan at any time in accordance with its terms.
- 11.2. The Service provider shall test the Business Continuity Plan on a regular basis (and in any event not less than once in every [12 month] period) jointly with the UBI. The UBI may require the Service provider to conduct additional tests of the Business Continuity Plan where the UBI considers it necessary, including where there has been any change to the Services or any underlying business processes, or on the occurrence of any event which may increase the likelihood of the need to implement the Business Continuity Plan. The Authority reserves the right to attend any Business Continuity Plan test undertaken by the Contractor.
- 11.3. If the UBI requires an additional test of the Business Continuity Plan it shall give the Service provider written notice and the Service provider shall conduct the test in accordance with the UBI's requirements and the relevant provisions of the Business Continuity Plan. The Contractor's costs of the additional test shall be borne by the UBI unless the Business Continuity Plan fails the additional test in which case the Contractor's costs of that failed test shall be borne by the Contractor.
- 11.4. Following each test, the Service provider shall send to the Authority a written report summarising the results of the test and shall promptly implement any actions or remedial measures which the UBI considers to be necessary as a result of those tests.
- 11.5. The service provider shall undertake regular risk assessments and/or business impact analysis in relation to the provision of the Services not less than once every six months and shall provide the results of, and any recommendations in relation to those risk assessments or business impact analysis to the Authority promptly in writing following each review.

12. Indemnity

The service provider by executing the outsourcing agreement shall be deemed to have unconditionally agreed as under:

- 12.1. The Service provider agrees to indemnify and keep indemnified, defend and hold harmless Purchaser and its directors, employees, agents and representatives from and against any, loss, damages, liabilities, claims, litigations, suits, actions, judgments, and or otherwise including but not limited to those from third parties or liabilities of any kind howsoever suffered, arising out of or incurred inter alia during and after the Contract period including but not limited to third-party claims due to infringement of patent, trademark, Intellectual Property Rights, copyrights or industrial drawings and designs arising from use of the services or any part thereof and / or otherwise.
- 12.2. Further, the said indemnity shall also be available for any of actions arising out of or in connection with the Contractor's breach of the representations and warranties specified in the Contracts/ Agreement; acts or omissions of negligence or misconduct by the Service provider or its professionals, representatives, agents, subcontractor, security analysts, consultants and advisors; For the purpose of the Agreement/Contract, the Service provider shall mean and include the Contractor, its personnel, employees, consultants, advisors, agents, representatives and / or other authorized persons.
- 12.3. The responsibility to indemnify shall survive the termination of the Agreement / Contract for any reason with regard to any indemnity claims arising in relation to performance thereof. Service Provider shall ensure that in addition to security features deployed in the technology, controls and operational procedures should ensure protection of the UBI from loss, disclosure or frauds.

- 12.4. The Service provider shall indemnify the UBI from transaction risk (from system error, human error, negligence and mismanagement) and fraud risk (loss to earnings or capital due to intentional deception by employees, customers, agents, external entities, etc).
- 12.5. The Service Provider shall indemnify the UBI and provide a system free from risks arising out of data becoming outdated, lost or overwritten due to inappropriate update procedures and the potential for frauds.
- 12.6. The Service Provider shall indemnify the UBI and hold the UBI harmless against loss or liability, claims actions or proceedings due to wrong debit/credit of any account of any beneficiary/customer that may arise through the action of its employees, agents, contractors, etc. or otherwise.
- 12.7. The Service Provider shall assist the UBI in identifying potential risks in the solution, remedy any of the identified risks, develop strategies to measure, monitor and mitigate those risks and implement new controls.
- 12.8. The Service Provider shall maintain adequate documentation, records, audit trails, etc and cooperate with the UBI's internal audit teams, regulatory authorities and third-party external auditors for conducting periodical audit and arrange for necessary access to relevant information / assets under the control of the Service provider.
- 12.9. The Service Provider shall take Fidelity Insurance to cover any loss arising out of the outsourced activity.

13. Force Majeure

The service provider by executing the outsourcing agreement shall be deemed to have unconditionally agreed as under:

- 13.1. Notwithstanding the provisions of this RFP the Service provider shall not be liable for forfeiture of its Performance Bank Guarantee, liquidated damages or termination for default, if and to the extent that, its delay in performance or other failure to perform its obligations under the Contract / Agreement is the result of an event of Force Majeure.
- 13.2. For purpose of this Clause "Force Majeure" means an event beyond the control of the Service provider and not involving the Contractor's fault or negligence and not foreseeable. Such events may include war or revolution, terrorist act, fire, flood, earthquake, epidemic and quarantine restriction.
- 13.3. If a Force Majeure situation arises, the Service provider shall promptly notify UBI in writing of such conditions and the cause thereof. Unless otherwise directed by UBI in writing, the Service provider shall continue to perform its obligations under the Contract as far as is reasonably practical and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event. UBI may terminate the Contract I Agreement, by giving a written notice of minimum 30 (thirty) days to the Contractor, if as a result of Force Majeure the Service provider is unable to perform a material portion of the Service(s) for a period of more than 60 (sixty) days.

14. Relationships between the Parties

The service provider by executing the outsourcing agreement shall be deemed to have unconditionally agreed as under:

- (a) The Service(s) of the Service provider herein shall not be construed as any 'agency of U3f and there shall be no principal and agent relationship between UBI and the Service provider in this regard.
- (b) Nothing in the Contract / Agreement constitutes any fiduciary relationship between UBI and Contractor/Contractor's Team or any relationship of employer - employee, principal and agent, or partnership, between UBI and Contractor.
- (c) No Party has any authority to bind the other Party in any manner whatsoever except as agreed under the terms of the Contract / Agreement.
- (d) UBI has no obligations to the Contractor's/Contractor's team except as agreed under the terms of the Contract / Agreement.

15. No Assignment

The service provider by executing the outsourcing agreement shall be deemed to have unconditionally agreed as under:

The Contract / Agreement cannot be transferred or assigned by the Service provider without the prior written approval of UBI.

16. Term

The agreement shall valid up to the term/period as mentioned in the agreement unless otherwise terminated by the parties in accordance with terms of the agreement. The Agreement may be renewed upon such terms and conditions, which the parties may mutually agrees in writing.

17. Termination

The service provider by executing the outsourcing agreement shall be deemed to have unconditionally agreed as under:

17.1. UBI may, terminate the Contract / Agreement by giving the Service provider a prior and written notice of 30 days indicating its intention to terminate the Contract / Agreement under the following circumstances:

- (a) Where it comes to UBI's attention that the Service provider is in a position of actual conflict of interest with the interests of UBI, in relation to any of terms of the Contractor's bid or the Contract / Agreement.
- (b) Where the Contractor's ability to survive as an independent corporate entity is threatened or is lost owing to any reason whatsoever, including inter-alia the filing of any UBI Bankruptcy proceedings against the Contractor, any failure by the Service provider to pay any of its dues to its creditors, the institution of any winding up proceedings against the Service provider or the happening of any such events that are adverse to the commercial viability of the Contractor.

17.2. In the event of the happening of any events of the above nature, UBI shall reserve the right to take any steps as are necessary, to ensure the effective transition of the Service(s) to the next successor Service provider, and to ensure business continuity.

17.3. Termination for Insolvency:

UBI may at any time terminate the Contract / Agreement by giving written notice to the Contractor, without compensation to the Contractor, if the Service provider becomes Bankrupt or otherwise

insolvent, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to UBI.

17.4. Termination for Default:

UBI, without prejudice to any other right or remedy for breach of Contract, by a written notice of default sent to the Contractor, may terminate the Contract / Agreement in whole or in part.

18. Consequences of Termination

The service provider by executing the outsourcing agreement shall be deemed to have unconditionally agreed as under:

- 18.1. In the event of termination of the Contract / Agreement due to any cause whatsoever, [whether consequent to the stipulated term of the Contract / Agreement or otherwise], UBI shall be entitled to impose any such obligations and conditions and issue any clarifications as may be necessary to ensure an efficient transition and effective business continuity of the Service(s) which the Service provider shall be obliged to comply with and take all available steps to minimize loss resulting from that termination/breach, and further allow the next successor Service provider to take over the obligations of the erstwhile Service provider in relation to the execution / continued execution of the scope of the Contract / Agreement. Termination process will be initiated only after the service provider has been provided with a written curing period of 30 (thirty) days.
- 18.2. In the event that the termination of the Contract / Agreement is due to the expiry of the term of the Contract / Agreement, a decision not to grant any (further) extension by UBI, the Service provider herein shall be obliged to provide all such assistance to the next successor Service provider or any other person as may be required and as UBI may specify including training, where the successor(s) is a representative / personnel of UBI to enable the successor to adequately provide the Service(s) hereunder, even where such assistance is required to be rendered for a reasonable period that may extend beyond the term/earner termination hereof.
- 18.3. Where the termination of the Contract / Agreement is prior to its stipulated term on account of a default on part of the Service provider or due to the fact that the survival of the Service provider as an independent corporate entity is threatened/has ceased, UBI shall pay the Service provider for that part of the Service(s) which have been authorized by UBI and satisfactorily performed by the Service provider up to the date of termination, without prejudice to any other rights, UBI may retain such amounts from the payment due and payable by UBI to the Service provider/Service provider as may be required to offset any losses caused to UBI as a result of any act/ omissions of the Service provider / Service provider. In case of any loss or damage due to default on the part of the Service provider / Service provider in performing any of its obligations with' regard to executing the Service(s) under the Contract / Agreement. The Service provider / Service provider shall compensate UBI for any such loss, damages or other costs, incurred by UBI. Additionally, the sub Service provider / Service provider / other members of its team shall continue to perform all its obligations and responsibilities under the Contract / Agreement in an identical manner as were being performed hitherto before in order to execute an effective transition and to maintain business continuity. All third parties shall continue to perform all / any functions as stipulated by UBI and as may be proper and necessary to execute the service(s) under the Contract / Agreement in terms of the Service provider's / Service provider's bid and the Contract / Agreement.
- 18.4. Nothing herein shall restrict the right of UBI to invoke the Performance Bank Guarantee and other guarantees, securities furnished, enforce the Deed of Indemnity and pursue such other rights and / or remedies that may be available to UBI under law or otherwise.

- 18.5. The termination hereof shall not affect any accrued right or liability of either Party nor affect the operation of the provisions of the Contract / Agreement that are expressly or by implication intended to come into or continue in force on or after such termination.
- 18.6. Termination survives the Contract / Agreement.
- 18.7. In the event of termination of this Agreement for any reason, UBI shall have the right to publicize such termination to caution the customers / public from dealing with the Contractor.

Yours faithfully,

Authorized Signatory

Name:

Designation:

Vendor's Corporate Name

Address

Email and Phone #

86. Annexure Y - Undertaking of Authenticity for Networking Hardware

To

Date:

Union Bank of India,
Department of Information Technology,
1/1A, Adi Shankaracharya Marg, JVLR,
Opp. Powai Lake (Andheri East),
Powai (Andheri East), Mumbai 400072.

Sub: RFP for Network Management support services for Wide Area Network of the Bank

Ref: 1. Your Purchase Order No.-----dated -----

1. Our invoice no. /Quotation no. -----dated-----

Dear Sir,

With reference to the Computer Hardware being supplied / quoted to you vide our invoice no. / quotation no. / order no. cited above-----

We hereby undertake that all the components/parts/assembly/software used in the Networking Hardware shall be original new components / parts / assembly / software only, from respective OEMs of the products and that no refurbished / duplicate / second hand components / Parts / Assembly / Software are being used or shall be used.

Should you require, we hereby undertake to produce the certificate from our OEM supplier in support of above undertaking at the time of delivery / installation. It will be our responsibility to produce such letters from our OEM Supplier's at the time of delivery or within a reasonable time.

In case of default and we are unable to comply with above at the time of delivery or during installation for networking Hardware / Software already billed, we agree to take back the Networking Hardware without demur, if already supplied and return the money if any paid to us by you in this regard.

We (system OEM name) also take full responsibility of both Parts & Service SLA as per the content even if there is any defect by our authorized Service Centre / Reseller / SI etc.

Authorized Signatory

Name:

Designation: