भारतीय लघु उद्योग विकास बैंक

Small Industries Development Bank of India

नेटवर्क स्वीचेस, की खरीद के लिए

प्रस्ताव के लिए अनुरोध

Request for Proposal
for
Procurement and Implementation of Network switches, Security Equipment at Data Center and DR Site

टेंडर सं. / Tender No.	400/2016/1152/BYO/ITV
टेंडर जारी करने की तिथि / Tender Issue Date	24 फरवरी, 2016 / February 24, 2016
पूर्व-बोली बैठक की तिथि / Date of Pre-bid meeting	01 मार्च, 2016 / March 01, 2016, 1130hrs
बोली जमा करनी की अंतिम तिथि / Last date for bid submission	15 मार्च, 2016 / March 15, 2016, 1630hrs
तकनीकी बोलियां खोलने की तिथि / Date of opening of Technical Bids	16 मार्च, 2016 / March 16, 2016, 1130hrs
बयाना जमा राशि / Earnest Money Deposit	Rs.3,00,000/- (Rupees Three lakh only)
टेंडर मूल्य /Tender Cost	Rs.1,000/- (Rupees one thousand only)

भारतीय लघु उद्योग विकास बैंक
एमएसएमई विकास केन्द्र, सी-11, जी ब्लाक,
बांद्रा कुर्ला काम्प्लेक्स, बांद्रा (पू.), **मुम्बई – 400051**

SMALL INDUSTRIES DEVELOPMENT BANK OF INDIA
MSME Development Center, C-11, 'G' Block,
Bandra Kurla Complex, Bandra (E), **Mumbai - 400 051**

Table of Contents

1. Critical Information/ महत्वपूर्ण सूचना

S.N. क्र.सं.	Events / कार्यक्रम	Date/ तिथि	Time/ समय
1	Last date for seeking clarifications for pre-bid meeting/ पूर्व-बोली बैठक के लिए स्पष्टीकरण की मांग की अंतिम तिथि	29 फरवरी, 2016 / February 29, 2016	1600 hrs
	Clarifications mail to be sent to **crprasad@sidbi.in and ssadagopan@sidbi.in.**		
2	Pre Bid meeting / पूर्व-बोली बैठक *No clarifications would be given after pre-bid meeting* / पूर्व बोली बैठक के बाद कोई भी स्पष्टीकरण नहीं दिया जायेगा।	01 मार्च 2016 / March 01, 2016	1130hrs
3	Last date for submission of bids/ बोली जमा करने की अंतिम तिथि	15 मार्च , 2016 / March 15, 2016	1630hrs
4	Date & Time of Opening of Minimum Eligibility bid & Technical bid/ न्यूनतम व तकनीकी बोली खोलने की तिथि व समय	16 मार्च , 2016 / March 16, 2016	1130 hrs
5	बयाना जमा राशि / Earnest Money Deposit	Rs.3,00,000/- (Rupees Three Lakh Only)	
6	टेंडर मूल्य /Tender Cost	Rs.1,000/- (Rupees One Thousand Only)	
7	Bid Validity/ बोली के वैद्यता	**180 days** from the last date of bid submission / बोली जमा करने की अंतिम तिथि से **180 दिन** तक।	
8	**Address for Bid Submission/ बोली जमा और पूर्व-बोली बैठक करने का पता**		
	General Manager (Systems) Small Industries Development Bank of India, 3rd Floor, Information Technology Vertical , MSME Development Centre Plot No. C-11, G Block, Bandra Kurla Complex , Bandra (E), **Mumbai - 400 051** Phone: 022-67531100 / 67531228 Fax: 022-67531236	**महाप्रबन्धक (सिस्टम्स)** भारतीय लघु उद्योग विकास बैंक, तीसरा तल, इन्फॉर्मेशन टेक्नालजी वेरतिकाल, एमएसएमई विकास केंद्र, प्लाट सं. सी-11, जी ब्लाक, बांद्रा कुर्ला काम्प्लेक्स, बांद्रा(पू.), **मुम्बई** दूरभाष: 022-67531100 / 67531228 फैक्स: 022-67531236	
9	Date and time of opening of commercial bids / वाणिज्यिक बोली खोलने की तिथि व समय	To be intimated at a later date बाद में सूचित किया जायेगा	
10	**Contact details of SIDBI officials / सिडबी अधिकारियों के संपर्क विवरण**		
	C R Prasad, AGM (Systems) / Phone: 022-67531238, Mail id : crprasad@sidbi.in	C R Sadagopan, DGM (Systems) Phone: 022-67531229 Mail id: sadagopan@sidbi.in	

2. Abbreviations

RFP	Request For Proposal
EMD	Earnest Money Deposit
TCO	Total Cost of Ownership
PBG	Performance Bank Guarantee
BG	Bank Guarantee
NAC	Network Admission Control
IPv6	Internet Protocol Version 6
IPv4	Internet Protocol Version 4
SFP	Small Form-factor Pluggable
OEM	Original Equipment Manufacturer
MSE	Micro and Small Enterprises
TOR	Top Of Rack
L3	Layer 3
L2	Layer 2
IPS	Intrusion Prevention System

3. Introduction and Disclaimers

3.1. Purpose of RfP

a) The purpose of RfP is to shortlist vendor for supply, installation, configuration and support of Network switches, firewalls for Data Center, Mumbai and DR Site, Chennai and Intrusion Prevention System at Data Center, Mumbai.

b) The contract duration is six years i.e., three years Warranty and three years AMC.

c) Since, SIDBI is going to deploy switches, Firewalls and IPS at Data Center and DR Site, the participating bidders are required to ensure uptime, timely replacement, support. Preventive maintenance etc. as defined in the RfP.

d) Details of the equipment under procurement, Scope of Work and other terms and conditions are given in the subsequent sections of this tender document.

3.2. Information Provided

The Request for Proposal document contains statements derived from information that is believed to be relevant at the date 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 SIDBI. Neither SIDBI 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 document. Neither SIDBI nor any of its employees, agents, contractors, or advisers has carried out or will carry out an independent audit or verification exercise in relation to the contents of any part of the document.

3.3. Disclaimer

Subject to any law to the contrary, and to the maximum extent permitted by law, SIDBI and its officers, employees, contractors, agents, and advisers disclaim all liability from any loss or damage (whether foreseeable or not) suffered by any person acting on or refraining from acting because of any information including forecasts, statements, estimates, or projections contained in this RfP document or conduct ancillary to it whether or not the loss or damage arises in connection with any negligence, omission, default, lack of care or misrepresentation on the part of SIDBI or any of its officers, employees, contractors, agents, or advisers.

3.4. Costs to be borne by Respondents

All costs and expenses incurred by Respondents in any way associated with the development, preparation, and submission of responses, including but not limited to; the attendance at meetings, discussions, demonstrations, POC etc. and providing any additional information required by SIDBI, will be borne entirely and exclusively by the Respondent.

3.5. No Legal Relationship

No binding legal relationship will exist between any of the Respondents and SIDBI until execution of a contractual agreement.

3.6. Recipient Obligation to Inform Itself

The Recipient must conduct its own investigation and analysis regarding any information contained in the RfP document and the meaning and impact of that information.

3.7. Evaluation of Offers

The issuance of RFP document is merely an invitation to offer and must not be construed as any agreement or contract or arrangement nor would it be construed as any investigation or review carried out by a Recipient. The Recipient unconditionally acknowledges by submitting its response to this RFP document that it has not relied on any idea, information, statement, representation, or warranty given in this RFP document.

3.8. Acceptance of Selection Process

Each Recipient / Respondent having responded to this RfP acknowledges to have read, understood and accepts the selection & evaluation process mentioned in this RfP document. The Recipient / Respondent ceases to have any option to object against any of these processes at any stage subsequent to submission of its responses to this RfP.

3.9. Errors and Omissions

Each Recipient should notify SIDBI of any error, omission, or discrepancy found in this RfP document.

3.10. Acceptance of Terms

A Recipient will, by responding to SIDBI for RfP, be deemed to have accepted the terms of this Introduction and Disclaimer.

3.11. Requests for Proposal

1. Recipients are required to direct all communications (**including pre-bid queries**) related to this RfP, through the Nominated Point of Contact person:

Contact Person	A V SyamSundar	C R Prasad	C R Sadagopan
Position	Manager(Systems)	AGM (Systems)	DGM (Systems)
Email Id	avsyam@sidbi.in	crprasad@sidbi.in	sadagopan@sidbi.in
Telephone	+91 - 22 –67531201	+91 - 22 –67531238	+91 - 22 –67531229

2. SIDBI may, in its absolute discretion, seek additional information or material from any of the Respondents after the RfP closes and all such information and material provided must be taken to form part of that Respondent's response.
3. Respondents should provide details of their contact person, telephone, fax, email and full address(s) to ensure that replies to RfP could be conveyed promptly.
4. If SIDBI, in its absolute discretion, deems that the originator of the question will gain an advantage by a response to a question, then SIDBI reserves the right to communicate such response to all Respondents.
5. SIDBI may, in its absolute discretion, engage in discussion or negotiation with any Respondent (or simultaneously with more than one Respondent) after the RfP closes to improve or clarify any response.

3.12. Notification

SIDBI will notify all short-listed Respondents in writing or by mail as soon as practicable about the outcome of their RfP. SIDBI is not obliged to provide any reasons for any such acceptance or rejection.

3.13. Proposal Ownership

The proposal and all supporting documentation submitted by the vendors shall become the property of SIDBI unless the bank agrees to the vendor‟s specific request in writing, that the proposal and documentation be returned or destroyed.

****

4. Background

4.1. Introduction

Small Industries Development Bank of India (SIDBI), set up on April 2, 1990 under an Act of Indian Parliament, acts as the Principal Financial Institution for the Promotion, Financing and Development of the Micro, Small and Medium Enterprise (MSME) sector and for Co-ordination of the functions of the institutions engaged in similar activities.

4.2. Financial Support

Financial support to MSMEs is provided by way of (a) indirect finance / refinance to eligible Primary Lending Institutions (PLIs), such as, banks, State Financial Corporations (SFCs), etc. for onward lending to MSMEs and (b) direct assistance in the niche areas like risk capital/equity, sustainable finance, receivable financing, service sector financing, cluster specific financial products, schemes and processes, funding for MSME infrastructure and funding for marketing activities. The cumulative disbursement till March 31, 2015 by SIDBI to the MSME sector since inception stood over ₹3.90 lakh crore, benefitting around 346 lakh persons / units.

1. **Indirect Finance**

- **Refinance:** The Bank provides refinance support to primary lending institutions (PLIs) comprising mainly banks together having a network of more than 1 lakh branches. Refinance constitutes around 80% of the Bank's portfolio as on March 31, 2015. Refinance is extended for (i) Setting up of new projects and for technology upgradation / modernisation, diversification, expansion, rehabilitation, energy efficiency, adoption of clean production technologies, etc. of existing MSMEs, (ii) Service sector entities and (iii) Infrastructure development and up-gradation.
- **Micro Finance:** SIDBI's micro finance serves as a potent tool of inclusive growth and attainment of Millennium Development Goals by catering to the bottom-of-the-pyramid sections of the society. As a part of its responsible finance initiative, SIDBI has created a Lenders' Forum comprising key MFI Funders with a view to promote cooperation among MFI lenders for leveraging support to MFIs. Besides, SIDBI has developed a Code of Conduct Assessment (COCA) Tool, which applies to providing credit services, recovery of credit, collection of thrift, etc. undertaken by MFIs. Cumulatively, the assistance under microfinance through SIDBI has benefited around 332 lakh (approx.) disadvantaged people, most of them being women.

2. **Direct Finance**

SIDBI provides direct credit to MSMEs mainly to supplement and complement the efforts of banks and FIs in providing credit to the MSME sector. Focus of direct lending is mainly on the areas, where gaps exist or in clusters or in niche areas through product and process innovations. Some of the major financing schemes of SIDBI are as under:

- **Equity Assistance:** With a view to ameliorating the problems faced by the MSMEs in accessing growth capital, SIDBI had started the risk capital operations to support the growth requirements of a number of MSMEs including leveraging of senior loans, marketing / brand building, technical knowhow, etc. where bank loans are generally not available as such investments are non-asset creating. SIDBI offers the quasi-equity support which is collateral free, having higher moratorium on repayment and a flexible structuring.
- **Sustainable Finance:** As a part of its Green initiative, SIDBI has developed specialized loan schemes to promote energy efficiency (EE), cleaner production (CP)

and environment protection in the MSME sector. These loans are under bilateral lines of credit from international agencies such as JICA, Japan; AFD, France; and KfW, Germany. These focused schemes have two pronged approach, i.e. concessional lending to encourage investment in green energy efficient investments and information dissemination to various MSME sectors. SIDBI's strategic partnership with World Bank (WB) and Bureau of Energy Efficiency (BEE), Ministry of Power, Govt. of India for financing energy efficiency in MSMEs has provided an impetus to EE based investments.

- **Service Sector Financing:** In view of the growing share and importance of service sector to national income, employment and entrepreneurial opportunities, SIDBI has focused on increasing the share of service sector portfolio in its business. SIDBI has negotiated new lines of credit for service sector with international funding agencies like World Bank and JICA, Japan.
- **Addressing Delayed Payments:** In order to help the MSMEs for quicker realization of their receivables, SIDBI fixes limits to well-performing purchaser companies and discounts usance bills of MSMEs / eligible service sector units supplying components, parts, sub-assemblies, services, etc. so that the MSME / service sector units realise their sale proceeds quickly. SIDBI also offers invoice discounting facilities to the MSME suppliers of purchaser companies.

3. Recent Initiatives

- **SIDBI Make in India Loan for Enterprises [SMILE] Scheme** to make available soft loan, in the nature of quasi-equity to meet the required debt-equity ratio and term loan on relatively soft terms for establishment of new MSMEs, as also for pursuing opportunities for growth for existing MSMEs.
- **India Aspiration Fund** to boost the start-up Venture Capital ecosystem in the country. It will act as a Fund of Funds managed by SIDBI and will be contributing to MSME focused VCFs, which will enable them to raise private capital, thus enhancing the flow of equity to start-ups and growth stage MSMEs in the country.
- **Make in India Fund** to make our MSMEs world class manufacturing hub. Under the fund, concessional finance are provided to identified MSME sectors.
- **Micro Units Development & Refinance Agency (MUDRA)** to funding the unfunded by way of providing access to institutional finance to the small units.
- SIDBI has also set up various subsidiaries / associates to create an enabling ecosystem for MSME growth.

• **MUDRA**	• Micro Units Development and Refinance Agency • **(www. mudra.org.in)**
• **CGTMSE**	• Credit Guarantee Fund Trust for Micro and Small Enterprises • **(www. cgtmse.in)**
• **ISARC**	• India SME Asset Reconstruction Company Ltd • **(www. isarc.in)**
• **SVCL**	• SIDBI Venture Capital Limited • **(www. sidbiventure.co.in)**
• **NCGTC**	• National Credit Guarantee Trustee Company

4.3. Promotional and Developmental (P & D) Support

- **Promoting Youth Entrepreneurship** through a website www.smallB.in to provide handholding guidance information on how to set up new units and how to expand the existing ones.
- **MSME Advisory services** like guiding new / existing entrepreneurs regarding availability of credit from banks, government subsidies, debt counselling.
- **Loan Facilitation** to MSMEs to help them avail credit from banks/FIs.
- **Capacity building** of smaller banks like Regional Rural Banks (RRBs) / Urban Cooperative Banks (UCBs) / District Central Cooperative Banks (DCCBs) banks to purvey credit to micro enterprises.
- **Micro Enterprises Creation** which aims at promoting viable rural enterprises leading to employment generation in rural areas.
- **Entrepreneurship and Skill development** through reputed institutions throughout the country, with special emphasis on women, weaker section, specific industry groups / service sector.
- **Cluster Development** to provide various Business Development Services (BDS), such as, new technologies, use of IT, skill development, energy efficiency, marketing, etc.

4.4. Operational functions

Overall operational functions of SIDBI are distributed among various verticals and cells. Broad functions in SIDBI are:

S.N.	Broad areas
A.	**Financing and Allied Activities**
1	Direct Risk Capital assistance
2	Managing Fund of Funds, India Venture Board, National Innovation Finance Programme (NIFP)
3	Infrastructure financing,
4	Merchant Banking for MSMEs
5	Receivable Finance, Trade Financing and Factoring Services
6	Service Sector Financing
7	Indirect Finance, Assignment, Securitisation
8	Sustainable finance including EE funding and funding of cleaner technologies
9	Stressed Assets and NPA Management,
10	Direct Credit Operations (CCG),
11	Working Capital related products (CC/LC/BG etc.)
12	Coordination Cell for Product Review & New Products
13	Refinance-SFCs & Banks
14	Indirect finance to NBFCs
15	Micro Credit operations (Funding of MFIs)
16	Treasury
17	Loan syndication Services, Credit Advisory Centres
18	Risk Management,
19	Economic Planning, Research & Publications (including MSME research), Annual Report
20	Internal Audit
21	Strategic Planning / Budgeting

22	Resource Management
B.	**Promotion Activities/Development etc**
23	Government Schemes Cell
24	Associate Institution Cell
25	Corporate Social Responsibility
26	International Consultancy, Project Management Division
27	Cluster development, Technical assistance
28	Central Coordination, Government Liaison and Parliamentary Committees/ Questions
29	Promotion and Development, capacity building of RRBs and UCBs
30	Customer Service Cell including Lead Management, MSE-CDP
31	SmallB and SIDBI Website
32	Insurance Marketing Cell
33	Energy Efficiency cell
34	Poorer States Inclusive Growth (PSIG) Project
C.	**Administration /HR/ Planning / others etc**
35	Business Process reengineering Cell
36	Premises Vertical
37	Administration, PF & Pension
38	HR & Training
39	Corporate Accounts, Taxation, Compliances
40	RBI Co-ordination
41	SIDBI MSME International Training Centre, e-learning modules
42	Management Information
43	Corporate Image Enhancement Cell
44	Information Technology
45	Implementation of Rajbhasha (Hindi) policy
46	Legal & RTI
47	Board Division
48	Staff Accountability / Disciplinary cases
49	Vigilance cell

4.5. Current IT Setup

1. **Data Centre and DR Site**

   SIDBI has its Data centre at Mumbai and DR Site at Chennai. All the applications, Internet, Video Conferencing core Infrastructure etc are hosted at Data centre and the same are accessed over MPLS VPN based WAN by all locations and offices. In the event of failure of Data centre, DR Site is activated.

2. **Present IT Infrastructure**

Infrastructure Type	Details of Components
Hardware	Servers (Tower, Rack & Blades with majority on Intel and few on RISC architecture), Routers, Switches, Backup Tape library, Security devices, Video Conferencing core infrastructure & End points, biometric attendance systems, SSL VPNetc
Operating Systems	IBM AIX 6.1, HP-UX 11. 31 v3, Windows 2003/2008 etc, Linux, Citrix XenServer Enterprise Edition for virtualization.
Database Servers	Oracle 10g in RAC (Real Application Cluster), Oracle Data guard for

Infrastructure Type	Details of Components
	DR replication of archive logs.
Application Servers	Citrix XenApp 5.0, IBM Websphere and MQ-Series, Oracle Application Server.
Web Server	JBoss, Apache Tomcat, IIS, IBM HTTP
Development Tools	Oracle Developer Suite ver 6, Java/JSP, Lotus Domino, IBM Rational
Groupware	IBM Domino 9
Office automation	Microsoft Office 2003 and above, Unicode
Antivirus	Symantec Enterprise Edition Version 12
Enterprise Backup Solution	LAN based backup using Veritas Netbackup DataCenter 7.0
EMS Tools	HP OpenView - Operations Manager, Network Node Manager (NNM), Client Configuration Manager (CCM), SM7, SPIs for Database, Lotus Notes and Citrix, Business Crystal Reports.
Security	• Data Center Core Firewall (Fortigate 3600 in failover mode), Perimeter Firewall (Fortigate 800 in failover mode) and NIPS (Cisco 4240) • DR Site Checkpoint (4800) firewall
Web Gateway Security	Cisco Ironport S370 Series web gateway security appliance with proxy and caching, web content filtering, antimalware and antivirus.
Video Conferencing	The core infrastructure consists of Polycom DMA, RSS, MCU, RPAD, PRI gateway, Resource manager with software clients and Radvision Scopia Elite MCU. Endpoints are mix of hardware and software and of Polycom (HDX 8000/7000/Group 500/desktop clients).
Access Gateway (SSL VPN)	Citrix Netscaler
WAN	Complete managed IP MPLS VPN from three service providers connecting all the locations. Primary link on wired or wireless with backup on CDMA/RF/3G (excluding Regional offices where dual service provider network is present). The entire WAN architecture is HUB and Spoke with HUB locations being Data Center and DR Site. All routers installed are of Cisco 1900/2900/3900/3800 series and are from service providers.
LAN	• Data Center and DR Site – Cisco L3 / L2 based LAN • Other Locations – L2 based LAN with switches of heterogeneous make (Cisco/Dlink/HP). • SIDBI also issued tender for replacement of L2 switches at various locations/offices and addition of L3 switches at Lucknow and New Delhi.
Business Applications	Website, Intranet portal, Business Application with details as given in subsequent paragraph of this document.

3. **Details of Present Network and Security Architecture at DC and DR**

A. Connectivity

i. **Wide Area Network**

SIDBI has implemented complete managed IP MPLS VPN based WAN at all locations/offices. Complete managed services include supply of all network hardware

(router, MUX, Modem etc) on lease, configuration, troubleshooting, monitoring, maintenance etc.

The primary connectivity is wired or wireless with backup on 3G, CDMA, RF etc based on feasibility of service provider at the location.

The MPLS VPN network architecture is HUB and spoke, with HUB locations being Data center and DR Site. QoS is enabled on the WAN network for prioritization of video and business traffic. Further, the last mile is encrypted (IPSec). All locations can reach DC and DR simultaneously.

Further, three service providers are contracted to build the network. The bandwidth at the locations varies from 256Kbps to 4Mbps and at aggregation points (DC and DR) the bandwidth available is 4/32/64Mbps. Bandwidths at the locations are upgraded based on operational requirement.

SIDBI also carries out additional monitoring, configuration and management of WAN, which is currently carried out by outsourced partner USING HPOV, NNM deployed by the Bank.

ii. **LAN**

SIDBI has implemented IP based, wired LAN at DC and DR with L3 and L2 switching. The L3 switches at DC and DR are of Cisco make and L2 switches are of Cisco/HP make.

iii. **Point to Point Link**

For online log shipment / replication from DC to DR, Bank has deployed point to point links of requisite bandwidth taken from two service providers. The links are terminated on L3 switches at DC and at Firewall in DR.

iv. **External Networks**

SIDBI also has connectivity with third party networks like Infinet, Reuters, SWIFT etc at both DC and DR.

These networks are currently connected as separate LAN. However, SIDBI proposes to integrate the same with DC network through proper security during this contract.

v. **Network Hardware Details**

The detail of network hardware at DC and DR is as given below:

S.N.	Hardware Description	Make/Model
A.	**DataCentre**	
1	Core Routers	Cisco 3900/3800/2900/1900 series
2	Core Switches (L3)	Cisco 6509E in HA
4	Access Switches	Cisco 2950 / 2960 / HP
B.	**DR Site**	
1	Router	Cisco 1900/2900 series
2	Core Switch	Cisco 3750X
3	Access Switches	Cisco 2950/HP/Dlink

B. Internet

- Internet at SIDBI is centralized with gateway at Data center and DR Site and all locations access Internet over WAN with proxy authentication.

- Bank has procured Internet bandwidth from two service providers at Mumbai and single service provider at Chennai.
- Link load balancers are deployed at Mumbai for load sharing between the Internet links.
- Web Gateway Security (WGS) appliance is installed at Datacenter which acts as proxy server with content filtering and antimalware software loaded on it. The WGS is integrated with AD.
- Currently, Bank does not have WGS and link load balancers at DR Site, the same along with dual internet links would be added in due course.

C. Mail

- SIDBI is currently using Lotus Domino for mailing. Outbound mails are sent from domino to internal SMTP and then transferred directly over Internet. SIDBI has its external mail box hosted with third party. All inbound internet mails from external domains, are first received at hosted mail box, gets scanned for antispam, thereafter they are pushed to SMTP server of the Bank.
- SIDBI has also enabled employees to access internal mails while on move through handheld & laptops for which lotus traveler is installed.

D. SMS facility

SIDBI also subscribed to SMS facility wherein information is sent to the customers.

E. Server

The servers deployed at DC and DR are mix of rack mountable and blade servers. Further, SIDBI is using Citrix Xen Server for virtualization. The operating system used is Windows (2003, 2008 etc), HP Unix, Linux (multiple flavours).

F. Video Conferencing

SIDBI has deployed video conferencing solution at all locations/offices. The solution is a mix of hardware/software based. The core infrastructure installed at Datacenter, consists of:

S.N.	Description	Make	Model	Remarks
1	MCU	Polycom	RMX 1500	15 port, full HD
		Polycom	RMX 1500	5 Port with PRI card
		Radvision	Elite	10 Port, full HD
2	Recording	Polycom	RSS 4000	5 port
3	Real Presence Distributed Media Application	Polycom	DMA 7000	50 concurrent calls.
4	Real Presence Resource manager	Polycom	RM	With 100 desktop clients
5	Real Presence Access Director.	Polycom	RPAD	To enables users within and beyond the firewall, to securely access video services.

The endpoints deployed at the locations are mix of Polycom (HDX 8000/7000/4500/Group 500 series).

The video conferencing is carried over existing WAN (no separate network for VC is implemented), Internet and PRI lines.

G. Security

i. Data Center

The Security architecture deployed at DC is two layer firewall architecture i.e. core and perimeter, with core firewall being Fortigate 3600C and perimeter being Fortigate 800. Further, Network Intrusion Prevention System (Cisco 4240 NIPS) is implemented at the perimeter and Antivirus loaded on all servers.

Zoning is created on the core and perimeter firewall and details of which are as follows:

- **Core firewall:** five zones are created on it for hosting various applications. The details of each zone are:
  - ✓ Zone-1: database servers, middleware servers, applications servers, citrix servers, VC core infrastructure, web gateway security appliances etc.
  - ✓ Zone-2: database servers for core banking software
  - ✓ Zone-3: UAT servers.
  - ✓ Zone-4:Test environment servers
  - ✓ Zone-5: WAN/LAN (Mumbai Office)
- **Perimeter firewall:** only one zone is created and all the web servers, lotus notes traveler, mail server, SSL VPN, RPAD etc are hosted.

ii. DR Site

At DR Site, Bank has deployed single firewall on which three zones are created. The details of each zone are:

- ✓ Zone-1: all applications, middleware, citrix servers, databases etc
- ✓ Zone-2: web servers, SSL VPN etc
- ✓ Zone-3: WAN/LAN (Chennai office)

iii. SSL VPN

To enable staff and customers access applications over Internet, SIDBI has deployed SSL VPN appliance at both Data Center and DR Site.

iv. Antivirus and Operating System Patches

Enterprise edition Antivirus is deployed at datacenter and clients loaded on all the servers and end computing devices. The antivirus definitions are updated periodically from the antivirus server hosted at datacenter.

Further, WSUS server is installed in the datacenter and windows patches are periodically updated from the same to the servers and end computing devices.

v. Branch/Office

All the branches are connected over MPLS VPN to DataCenter and DR Site. The local LAN is connected directly to the router. There is no security device/appliance installed in the branches.

vi. Authentication

Currently, Bank has two factor password and biometric authentication.

vii. **Syslog Server**

Bank has deployed syslog server to gather the logs of key network and security devices.

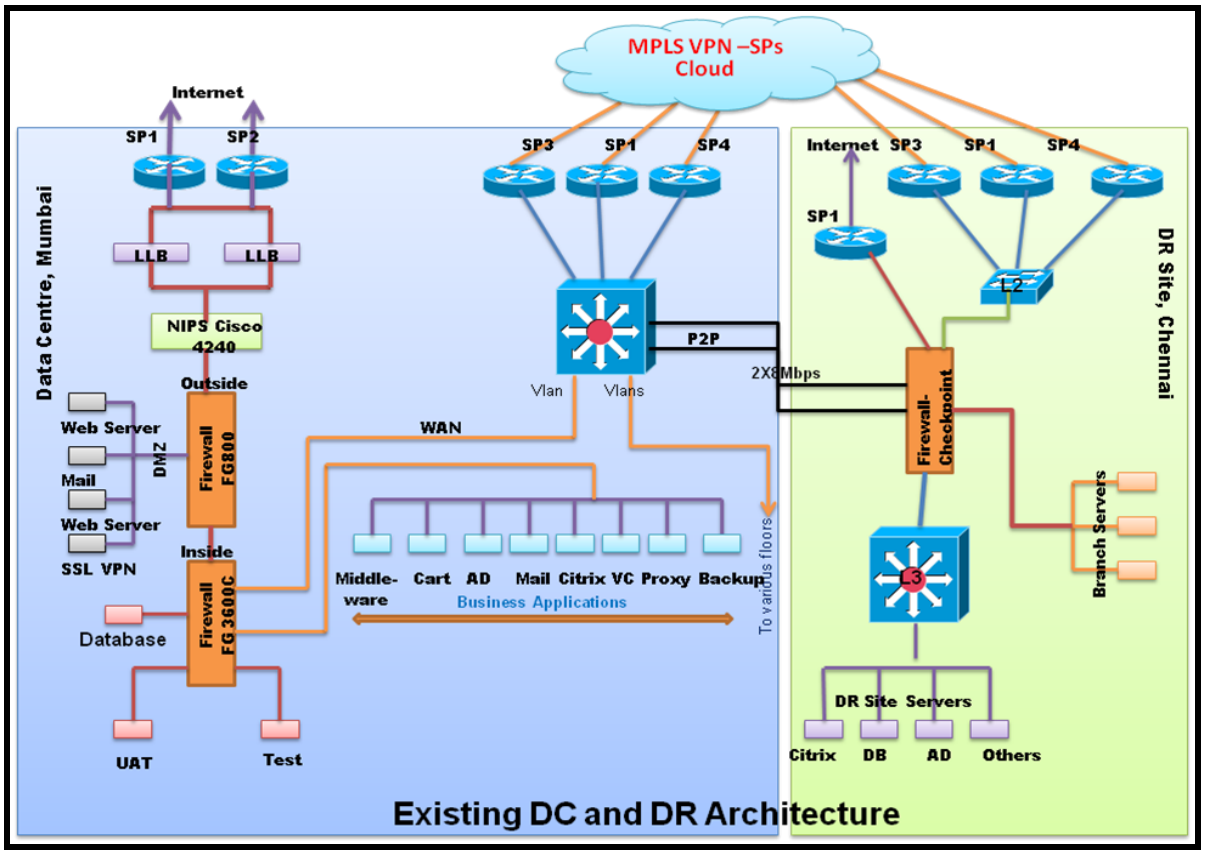
viii. **Security Hardware Details**

The detail of security hardware is as given below:

S.N.	Hardware Description	Make/Model
A.	**DataCentre**	
1	Firewall - Perimeter	Fortigate 800 in failover. (In process of replacement in this tender.)
2	Firewall - Core	Fortigate 3600 in failover (Core)
3	NIPS	Cisco 4240 (In process of replacement in this tender)
B.	**DR Site**	
1	Firewall	Checkpoint 4800

H. The Network and Security Architecture Diagram

The network and security architecture diagram at DC and DR is given below:

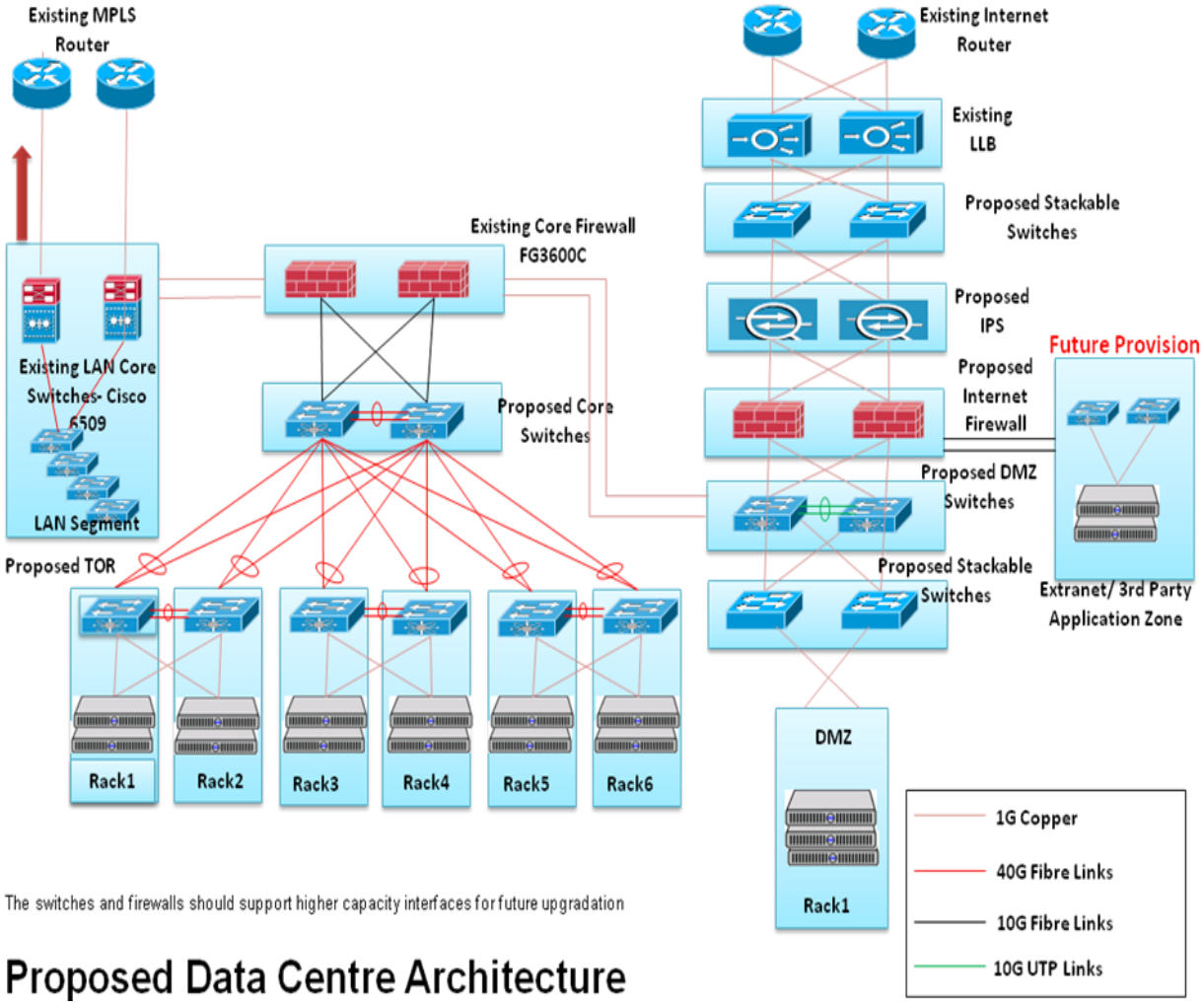


4.6. Tender Objective and Requirement

1. SIDBI intends to strengthen the switching and security at data center and DR site.
2. <u>At DC SIDBI proposes to</u>:
   - Replace the existing perimeter firewalls and Intrusion Prevention System and add new firewalls and IPS. **The new firewalls should not be of Fortigate**.

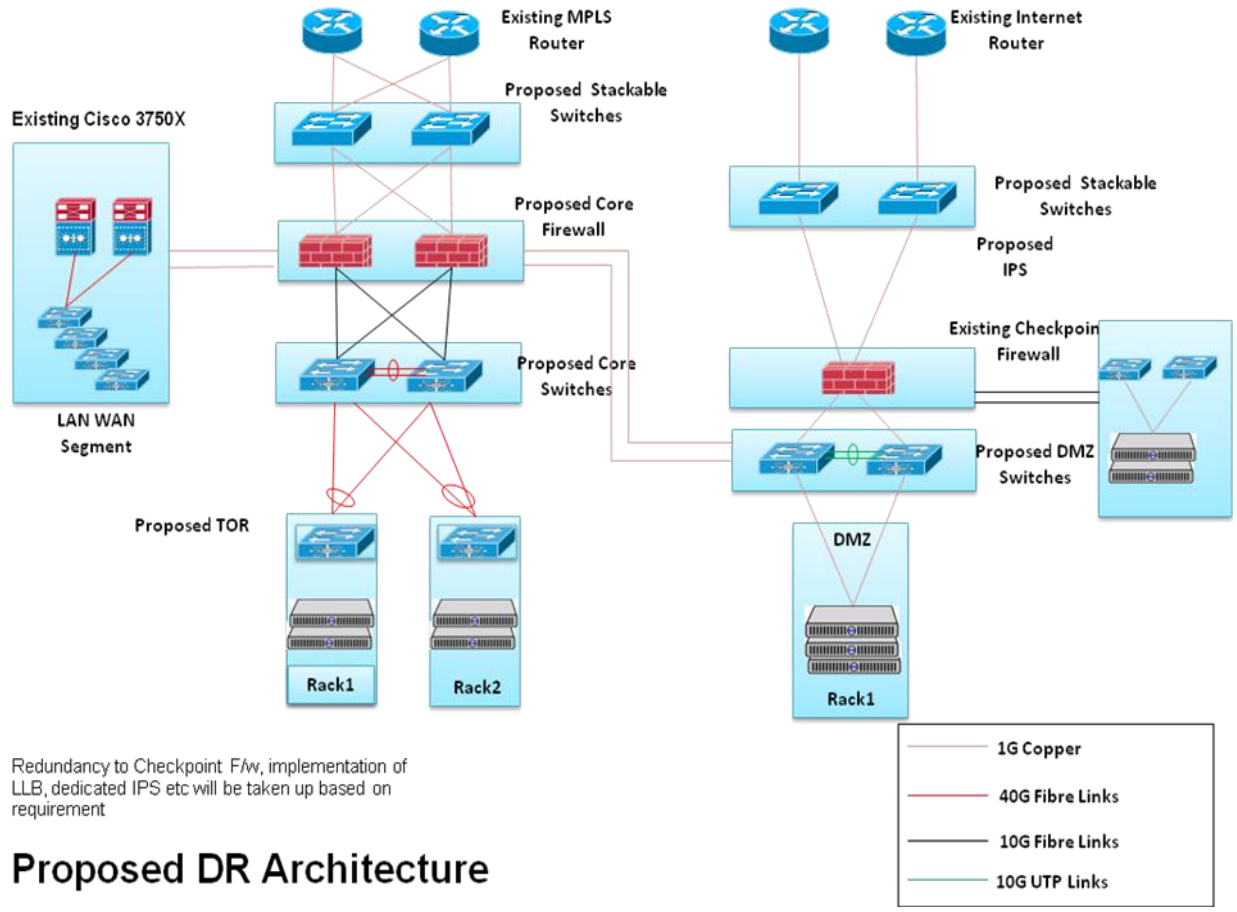
- Add Core, TOR and DMZ switches
- Add L2 stackable switches at perimeter and DMZ

3. At DR SIDBI proposes to:
   - Shift the existing firewall (Checkpoint) to the perimeter and add core firewalls in HA. **The core firewalls should not be of Checkpoint**.
   - Add Core, TOR and DMZ switches
   - Add L2 stackable switches at perimeter and on WAN side.
4. The Salient features of the DC & DR architecture are:
   - Two layer firewall architecture
   - Creation of zones/VLANs on Core firewall and switches for segregation of application servers, databases, UAT environment, Video conferencing infrastructure etc.
   - Creating zones on perimeter firewall / DMZ switches for hosting web servers, mail server, Polycom RPAD, Citrix netscaler etc.
5. The architecture proposed at DC and DR is as follows:
   a) **Data Center Proposed Architecture Diagram**



Proposed Data Centre Architecture

b) **DR Site, Proposed Architecture Diagram**



6. The following existing firewalls and switches at DC and DR would be used in the proposed architecture:

S.N.	Item Description	Quantity
1	Fortigate 3600C core firewall at DC	02
2	Checkpoint 4800 firewall at DR	01
3	Cisco 6509E core switches at DC	02
4	Cisco 3750X core switch at DR	01

7. The bidder to note that **Fortigate firewall** should not be proposed at Data Centre and **Checkpoint firewall** at DR Site.

8. The consolidated requirement of network switches, firewalls and IPS at Data Center, Mumbai and DR Site, Chennai are as given below:

S.N.	Item Description	Qty.
A.	**Data Centre**	
1.	Top of Rack Switches	06
2.	Core Switches	02
3.	DMZ Switches	02
4.	Stackable switches	04
5.	Perimeter Firewall	02
6.	Dedicated IPS	02
B.	**DR Site**	
1.	Top of Rack Switches	02

S.N.	Item Description	Qty.
2.	Core Switches	02
3.	DMZ Switches	02
4.	Stackable switches	04
5.	Core Firewall	02

9. All the switches, firewall and IPS should be rack mountable and rack mount kit to be included. Further, Indian power cords to be provided with the equipment.
10. Backplane of the Core and TOR switches should support Non-blocking Architecture.
11. Bank has deployed Cisco router and switches at its data centre so proposed switches should be Interoperable with Cisco Router and Switches.
12. Bidder should quote all the switches at DC and DR from the **SAME OEM**. Mix and match of OEMs are not allowed.
13. All the equipment should be with three years warranty and three years AMC which should be back to back with OEM and should be on-site and comprehensive.
14. Bank will initially place order for all the equipment with 3 years warranty, 3 years AMC and support. However, payment towards AMC will be made in respective years.
15. SIDBI is in the process of implementing NAC and IPv6 and also setting up Security Operating Center. Hence, the hardware proposed by the bidder should be capable of integration with **ANY NAC** solution without any upgradation of switch hardware/software.
16. **IPv6** –SIDBI is in the process of deploying IPv6 and hence all equipment should be IPv4 and IPv6 ready from day one. The equipment proposed should have IPv6 Forum Phase 2 - Core protocols, SNMP, IPSec, DHCPv6 certification.
17. All Configuration changes to be made on the existing and proposed switches and security devices to implement the proposed architecture is under the current scope of this RfP.
18. The purpose behind issuing this RfP is to invite pre-qualification, technical and commercial bids from the eligible bidders and selection of bidder(s).
19. The selection process consists of three phases viz., 1) Pre-Qualification / Minimum Eligibility Criteria 2) Technical Evaluation and 3) Commercial Evaluation.

****

5. Scope of Work

The Scope of Work involves:

1. Bidder will be responsible for end-to-end implementation of the network and security devices, including but not limited to covering aspects like – supplying, installing (including rack mounting), customizing, integrating, migrating, testing, troubleshooting, creating different zones/VLANs on the firewall and switches, redesigning IP Addresses, arranging for training etc.
2. The bidder should study the **CURRENT** network and security architecture at Data Centre and DR Site, which should include the:
    - Existing security and network hardware deployed, including Video conferencing infrastructure, AD etc.
    - WAN / LAN architecture and QoS implemented on the WAN links
    - IP address schema
    - Zoning of applications, databases, UAT environment, storage, citrix servers, WGS etc
    - VLANs configured
    - Application access over Internet and Intranet etc
    - Policies added on the firewalls
3. The bidder should prepare and submit comprehensive implementation strategy/plan for implementing the end to end proposed Network /Security Architecture solution etc at DC and DR. On approval of the plan by the Bank, implementation to be carried out. The bidder is required to carry out the exercise immediately after issue of purchase order. The plan should include:
    - IP address re-designing
    - Zoning on core for application servers, citrix servers, databases, UAT environment, Storage, video conferencing equipment, web gateway security appliances, WAN/LAN (considering QoS deployed) etc.
    - Zoning on perimeter for web servers, external networks, mail etc

      Zoning to be carried out through VLANs on switches / DMZs on the firewall as per Industry best practices.
    - Configuring policies on the firewalls and IPS.
    - Positioning and configuring of the IPS
    - Any configuration changes to be carried out on the existing firewalls, network switches etc would be under the scope of the bidder.
    - Cabling / rack requirement to be intimated. Cabling and supply of racks is not under the current scope of this RfP.
    - Submission of low level diagram of the entire implementation at DC and DR and relevant documents / reports.
4. The bidder should supply the switches, firewalls, IPS at respective locations as per the specifications given in technical bid.

5. The bidder should rack mount the hardware after removal of the existing hardware items, if any from the racks.
6. The bidder should carry out configuration / implementation of the proposed architecture. The implementation should be carried out on holidays or after office hours with minimum downtime to avoid disruption in datacenter services.
7. **Affixing Asset Tags on HW Equipments:** It will be the responsibility of the successful bidder to affix the Asset tags on each equipment being supplied to the Bank. Our office will provide the asset tag details to the successful bidder.
8. **Warranty and AMC**
   a) On-site, comprehensive and BACK-TO-BACK warranty from OEM for a period of three (3) years from the date of acceptance.
   b) On-site, comprehensive BACK-TO-BACK AMC from OEM for a period of three (3) years from the date of expiry of warranty.
   c) The warranty and AMC also includes all software subscriptions (critical hot fixes, service packs, firmware upgrades and all upgrades & updates) of all components supplied as part of solution without any additional cost to the Bank.
   d) Replacement of failed hardware should be **next business day (NBD)**.
   e) Detailed scope of warranty and AMC is given in **Section 9.3** of this tender.
9. **Support**
   a) L1 support should be from the bidder and L2 and above support from OEM.
   b) Comprehensive on-site 24X7X365 support by the bidder and OEM during Warranty and AMC.
   c) The Bank will log call to the bidder central help desk only. The call logging from Bank side would be from central location.
   d) Any coordination required with OEM, it would be the responsibility of bidder engineer.
   e) SIDBI should also be able to raise Tag with the OEM and the tag support should be 24X7X365. Bidder has to provide credentials for the same.
   f) The bidder by themselves should ensure that all critical/security patches / upgrades / updates etc are applied, as and when released by the OEM.
   g) **Return Material Authorization (RMA)**
      i. The replacement unit (during warranty and AMC) has to be shipped by OEM to the location and the bidder should install, configure and integrate the same. Once confirmed on the successful working of the device, the faulty unit has to be collected by the bidder and delivered to OEM.
      ii. All charges towards replacement has to be borne by the bidder. No charges whatsoever would be paid by the Bank.
   h) **Onsite engineer**

   The bidder to deploy on-site engineer for a period of two weeks from the date of acceptance for resolving initial day to day problems until the solution is stabilized.
10. **Preventive Maintenance**
    a) Preventive maintenance shall be compulsory carried out by the bidder during Warranty and AMC period. Preventive maintenance activity should be completed every **half year** and report should be submitted to the bank.

b) Preventive maintenance activity should take care of physical verification, device configuration verification, device health checkup, fine-tuning the configuration, security checkup, verification of bugs/patches, upgradation of firmware/operating system to the latest version (if available from OEM) etc.

c) The preventive maintenance report format shall be prepared by bank; the bidder shall strictly follow the format of bank and submit the same for each location wise during Warranty/AMC period.

d) The bidder is required to prepare PM schedule for all the locations and forward the same at least one week in advance to the Bank.

e) Non performance of PM will attract penalty as specified in **Section 9.7** of RfP.

11. At present IPv6 is not implemented in the Bank Network, however Bank is in the process of implementation. Bidder need to implement IPv6 without any additional cost whenever Bank decided to implement during the contract period.

12. The bidder to note that, the Bank reserves the right to modify/update the parameter files/**configuration** with required awareness of its consequences and any such modification/updation will be recorded for information of the selected bidder.

13. Any corruption in the software or media shall be rectified during the full period of the contract including Warranty and AMC at no extra cost to the Bank.

14. The bidder to note that, the Bank reserves the right to upgrade the equipment during the contract period by enabling license or addition of module/card. The upgradation may be carried out with the shortlisted vendor by calling for proposal or if desired, Bank would issue RfP and shortlist vendor for supply of components.

15. The hardware supplied as part of this contract should be maintained by the bidder and OEM for at least 6 years (i.e. three years warranty and three years AMC) from the date of acceptance of the hardware/solution by the Bank.

16. The system spare parts/services as and when required, and complete maintenance of the Systems during warranty period and AMC, shall be supported for a period not less than 6 years (Warranty and AMC) from the date of acceptance of the System by the Bank.

17. Submission of relevant documents / reports.

18. SIDBI conducts periodic Information Security audit by third party as per regulatory requirements. In case of any observation by the auditor for upgradation of software / firmware to mitigate the risk or any changes in configuration, the same will be conveyed to the bidder. The bidder is required to upgrade the software/firmware of all the equipment supplied by them, subject to availability from OEM.

19. **Site Inspection**

a) The bidder has to inspect the Data Center, Mumbai and DR Site, Chennai within 7 working days after placing the order for site requirement analysis i.e. space, cabling, electrical power requirement along with number of sockets and their capacity etc required for installation of hardware.

b) The bidder should submit site inspection report indicating the details of requirement i.e. type of backbone fiber cable, fiber patch panels, fiber/UTP patch chords, UTP

cable etc along with detailed specifications, make/model etc to the officer at the site and also forward scanned copy of same to Network Management Team at SIDBI, Mumbai and Chennai.

c) Passive components viz., laying of cables, patch panels/patch chords etc **not** under the scope of this RfP.

20. **Training and Knowledge Transfer**

a) The selected Bidder will ensure knowledge transfer to the Bank at every stageof the project to enable the Bank to carry out the work as specified in this RFP in future after completion of this assignment.

a) The vendor will be required to demonstrate features / functionalities and administration of the commissioned hardware / software to the Bank.

b) The selected bidder shall arrange for OEM training on complete administration of proposed network switches, firewalls, IPS to two officials of Bank. The training should be hands-on with complete configuration, management, troubleshooting etc. The training should be at Mumbai.

21. **Shifting**

a) The Bank may, during the currency of the project (6 years) may shift the equipment to other locations (i.e. co-locate data center and DR site to other location(s)) within the Country and in such case the bidder undertakes to continue to provide warranty/AMC and maintain/support the equipments at the new location.

b) The charges towards physical shifting and cabling would be borne by the Bank.

c) Bidder will be informed about old and new location/office details as and when the Bank decides to shift the Data Centre and DR Site. The bidder should carry out de-commissioning, dismantling, un-mounting of hardware from the old location and commissioning, rack mounting and configuration of hardware etc at the new location.

d) The vendor is required to update their database and provide support, Warranty/AMC etc, for the shifted devices at the new location.

e) No additional cost whatsoever would be paid by the Bank. Transportation, transit insurance would be taken by the Bank.

22. Any additional requirement regarding hardware, software, connectors, cables (except patch chords, fiber/UTP backbone cabling, Patch panels) etc after awarding the contract will not be entertained by the Bank. The Bidder shall be responsible for the same.

23. All claims for functional / technical delivery made by the Bidders in their responses to the RfP shall be assumed as deliverable, within the quoted financials.

24. In case of any damage to Bank property during equipment delivery and installation attributable to the bidder, bidder has to replace the damaged property at its own cost.

25. **Responsibility of SIDBI**

a) Make available the details of existing servers, applications, other infrastructure etc.

b) SIDBI or its outsourced partner from central location would be logging all calls with the vendor central help desk and coordinating for call closure.

c) Make available site for installation with power, rack space, earthing, internal cabling (fiber / UTP) and patch chords/panels (fiber, UTP).

d) Provide details of contact person at the location/office who would be coordinating during installation. Network Management Team at Mumbai would be coordinating along with local contact person during configuration.

e) Providing downtime for installation / preventive maintenance of equipment. The vendor should communicate at least one week in advance, the proposed date for preventive maintenance etc, based on which downtime would be obtained from the locations/offices.

****

6. Information to Bidders

The Bidders are expected to examine all instructions, forms, terms and specifications in the bidding documents. Failure to furnish all information required by the bidding documents may result in the rejection of its bid and will be at the bidder's own risk.

6.1. Pre-bid Meeting

1. The Bank shall hold a pre-bid meeting on the date and time mentioned in 'Critical Information' section above. Purpose of the meeting is to bring utmost clarity on the scope of work and terms of the RFP being floated. The Bidders are expected to use the platform to have all their queries answered. No query will be entertained after the pre-bid meeting.
2. It would be the responsibility of the Bidders representatives (only one person per bidder) to be present at the venue of the meeting.
3. Clarification sought by bidder should be made in writing (Letter/E-mail/FAX etc) and submitted on or before the date as indicated in the Critical Information sheet. Bank has discretion to consider any other queries raised by the bidder's representative during the pre-bid meeting.
4. The text of the clarifications asked (without identifying the source of enquiry) and the response given by the Bank, together with amendment / corrigendum to the bidding document, if any, will be posted on the Bank (www.sidbi.in) website and CPP Portal after the pre-bid meeting. It would be responsibility of the bidder to check the websites before final submission of bids.
5. If SIDBI, in its absolute discretion, deems that the originator of the question will gain an advantage by a response to a question, then SIDBI reserves the right to communicate such response to all Respondents.

6.2. Amendment to the bidding document

1. At any time prior to the date of submission of Bids, the Bank, for any reason, may modify the Bidding Document, by amendment.
2. 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 the submission of Bids.
3. The amendment will be posted on Banks website (www.sidbi.in) and CPP portal (http://eprocure.gov.in).
4. All Bidders must ensure that such clarifications/amendments have been considered by them before submitting the bid. Bank will not have any responsibility in case some omission is done by any bidder.

6.3. Language of Bid

The bid prepared by the Bidders as well as all correspondence and documents relating to the Bid exchanged by the Bidder and the Bank and supporting documents and printed literature shall be written in English.

6.4. Documents Comprising the Bid

The bid shall consist of Pre-qualification/ minimum eligibility criteria, Technical bid and Commercial bid.

6.5. Bid Currency

Bids should be quoted in Indian Rupee only.

6.6. Tender Form Cost

Non-refundable Bid Price of Rs.1,000/- (Rupees One Thousand only) by way of Banker's Cheque/ Demand Draft/ Pay Order drawn on a scheduled bank, favouring 'Small Industries Development Bank of India', payable at Mumbai must be submitted separately along with RFP response.

6.7. Earnest Money Deposit (EMD)

1. All the responses must be accompanied by a refundable INTEREST FREE security deposit of amount of Rs.3,00,000/-.
2. EMD should be in the form of:
   a) Demand Draft / Banker's Cheque in favour of "Small Industries Development Bank of India" payable at Mumbai **OR**
   b) Bank guarantee (BG) from a Scheduled Commercial Bank valid for a period of 6 months from the last date of submission of bid and strictly in the format as prescribed in **Annexure - IX**.
3. Any bid received without EMD in proper form and manner shall be considered unresponsive and rejected.
4. Request for exemption from EMD (Security Deposit) will not be entertained.
5. The EMD amount / BG of all unsuccessful bidders would be refunded immediately upon happening of any the following events:
   a) Issue of LoI / purchase order to the successful bidder **OR**
   b) The end of the bid validity period, including extended period (if any) **OR**
   c) Receipt of the signed contract from the selected Bidder; **whichever is earlier.**
6. Successful Bidder will be refunded the EMD amount / BG only after acceptance of the solution by SIDBI and submission of Performance Bank Guarantee by the bidder.
7. In case the acceptance of equipment is delayed due any reasons beyond the bank's purview, successful bidder shall have the BG towards EMD, validity extended for a period of three months till the equipment is accepted by the bank.
8. The bid security (EMD) may be forfeited:
   a) If a Bidder withdraws its bids during the period of bid validity.
   b) If a Bidder makes any statement or encloses any form which turns out to be false/ incorrect at any time prior to signing of the contract.
   c) In case of successful Bidder, if the Bidder fails to accept the LOI / Purchase order or sign the contract or fails to furnish performance guarantee.
   d) In all the above cases, the bidder would also be banned for a period of 3 years from subsequent bidding in any of the Bank's (SIDBI) tenders.

6.8. Period of Validity of Bids

1. Prices and other terms offered by Bidders must be firm for an acceptance period of 180 days from date of closure of this RfP.

2. In exceptional circumstances the Bank may solicit the Bidders consent to an extension of the period of validity. The request and response thereto shall be made in writing. The Bid security provided shall also be extended.
3. Bank, however, reserves the right to call for fresh quotes at any time during the period, if considered necessary.

6.9. Deadline for submission of Bids

1. The bids must be received by the Bank at the specified address not later than the date specified in "Critical Information" section.
2. In the event of the specified date for the submission of bids, being declared a holiday for the Bank, the bids will be received up to the appointed time on the next working day.
3. The Bank may, at its discretion, extend the deadline for submission of Bids by amending the Bid Documents, in which case, all rights and obligations of the Bank and Bidders previously subject to the deadline will thereafter be subject to the deadline as extended.

6.10. Late Bids

Any bid received by the Bank after the deadline for submission of bids prescribed by the Bank will be rejected and returned unopened to the bidder.

6.11. Modification And/ Or Withdrawal of Bids

1. The Bidder may modify or withdraw its bid after the bid's submission, provided that written notice of the modification including substitution or withdrawal of the bids is received by the Bank, prior to the deadline prescribed for submission of bids.
2. The Bidder modification or withdrawal notice shall be prepared, sealed, marked and dispatched. A withdrawal notice may also be sent by Fax and followed by a signed confirmation copy received by the Bank not later than the deadline for submission of bids.
3. No bid may be modified or withdrawn after the deadline for submission of bids.
4. Bank has the right to reject any or all bids received without assigning any reason whatsoever. Bank shall not be responsible for non-receipt / non-delivery of the bid documents due to any reason whatsoever.

6.12. Quotation of Price for all Items

1. The Bidder should quote for list of all the items proposed / listed in this Bid.
2. In case, prices are not quoted by any bidder for any specific item / product / service for the purpose of evaluation the highest of the prices quoted by other bidders, participating in the bidding process, will be reckoned as the notional price for that item/product / service, for that bidder and commercial evaluation would be carried out.
3. However, if selected, at the time of award of Contract, the lowest of the price(s) quoted by other bidders (whose Price Bids are also opened) for that new item/ product / service and highest price for buyback items will be reckoned. This shall be binding on all the bidders.
4. However, the Bank reserves the right to reject all such incomplete bids

6.13. Opening of Bids by the Bank

1. On the scheduled date and time, bids will be opened by the Bank Committee in presence of Bidder representatives. It is the responsibility of the bidder's representative to be

present at the time, on the date and at the place specified in the tender document. The bidders' representatives who are present shall sign a document evidencing their attendance.

2. If any of the bidders or all bidders who have submitted the tender and are not present during the specified date and time of opening it will be deemed that such bidder is not interested to participate in the opening of the Bid/s and the bank at its discretion will proceed further with opening of the technical bids in their absence.
3. The Bidder name and presence or absence of requisite EMD, RfP cost (if any) and such other details as the Bank, at its discretion may consider appropriate will be announced at the time of technical bid opening. No bid shall be rejected at the time of bid opening, except for late bids which shall be returned unopened to the Bidder.
4. Bids that are not opened at Bid opening shall not be considered for further evaluation, irrespective of the circumstances. Withdrawn bids will be returned unopened to the Bidders.

6.14. Pre Contract Integrity Pact

1. Pre Contract Integrity Pact is an agreement between the prospective vendors / bidders and the buyer committing the persons / officials of both the parties not to exercise any corrupt influence on any aspect of the contract.
2. The bidder has to submit signed Pre Contract Integrity Pact as per the format at **Annexure-XI** on the letterhead of the Company. However, the successful bidder has to submit the same in non-judicial stamp paper of requisite value (to be borne by the bidder) applicable at the place of its first execution after the issue of Purchase Order.

6.15. Erasures or Alterations

The offers containing erasures or alterations will not be considered until it is duly signed and stamped by the authorized signatory. There should be no hand-written material, corrections or alterations in the offer. Technical details must be completely filled in. Correct technical information of the product being offered must be filled in. Filling up of the information using terms such as "OK", "accepted", "noted", "complied", "as given in brochure / manual is not acceptable. The Bank may treat such offers as not adhering to the tender guidelines and as unacceptable.

6.16. Documents to be submitted

1. Bidders are required to submit their responses in **THREE envelopes**, with contents of each as under:

Envelope #	Bid Contents	No. of Copies	Label of Envelope
	Pre-Qualification / Minimum Eligibility a) DD/ Pay Order / BG for Rs.3,00,000/- towards EMD. The BG should be as per format given in **Annexure – IX.** b) DD/ Pay Order for **Rs.1,000/-** towards cost of tender form. c) Bid Forwarding Letter as per	**01** Editable soft copy	**"Minimum Eligibility"** RfP for Procurement of Network Switches, Security Appliances and Implementation– Tender No. 400/2016/ 1152/BYO/ITV dated 24/02/2016"

Envelope #	Bid Contents	No. of Copies	Label of Envelope
1	**Annexure – I**. d) Documentary evidence establishing that the Bidder is eligible to Bid and is qualified to perform the contract i.e., Pre-Qualification Criteria / minimum eligibility criteria as per **Annexure – II**. e) Masked Price Bid without indicating the price as per **Annexure –IV** should be submitted. f) Manufacturer Authorization Form (MAF) as per **Annexure – V**. g) Undertaking of authenticity – **Annexure – VI**. h) Power of Attorney for authorized signatory – **Annexure – VII**. i) Non Blacklisting – **Annexure –VIII**. j) Non-disclosure agreement - **Annexure –X**. k) Pre contract integrity pact – **Annexure – XI.** l) Statement of deviation as per **Annexure -XII**. m) Bank Mandate Form – **Annexure –XIII**.		
2	**Technical Bid** Technical Bid as per **Annexure - III**. Data sheets/printed literature of all the components being quoted.	01 Editable soft copy	"**Technical Bid** - RfP for Procurement of Network Switches, Security Appliances and Implementation – Tender No. 400/2016/ 1152/BYO/ITV dated 24/02/2016"
3	**Commercial Bid** Commercial Bid as per **Annexure –IV**.	01	**"Commercial Bid -** RfP for Procurement of Network Switches, Security Appliances and Implementation – Tender No. 400/2016/

Envelope #	Bid Contents	No. of Copies	Label of Envelope
			1152/BYO/ITV dated 24/02/2016"

2. The Bid shall be typed or written in indelible ink, all pages numbered and shall be signed by the Bidder representative on whose favour Power of Attorney is issued to bind the Bidder to the Contract.
3. Power of Attorney as per format given in **Annexure - VII** is to be submitted along with pre-qualification/minimum eligibility bid.
4. Relevant documents must be submitted as proof wherever necessary. Technical specification sheets of all the items to be submitted.
5. Faxed copies of any submission are not acceptable and will be rejected by the Bank.
6. Responses should be concise and to the point. Submission of irrelevant documents must be avoided.
7. If the bids do not contain all the information required or is incomplete, the proposal is liable to be rejected.
8. The Bidder shall seal the bids in non-window envelopes, superscribing the nature of bid (i.e. pre-qualification/minimum eligibility, Technical or Commercial). All the individual envelopes must be super-scribed with the following information as well:
   - Name of the bidder, Contact Name, Contact Number and e-mail id.
9. If the envelop(s) are not sealed and marked as indicated above, the Bank will assume no responsibility for the Bid's misplacement or its premature opening.
10. The bidder to note that, under no circumstances the Commercial Bid should be kept in Technical Bid Covers. The placement of Commercial Bid in Pre-qualification / Technical Bid covers will make bid liable for rejection.
11. The RfP is hosted on SIDBI website http://www.sidbi.in and also on Central Public Procurement Portal (CPPP). SIDBI reserves the right to change the dates mentioned above. Changes and clarification, if any, related to RfP will be posted on Bank web site and CPPP. Bidders must have close watch on the website and CPPP during the intervening period before submitting response to RfP.
12. Each of the envelope(s) shall be addressed to the Bank at the address given below:

    The General Manager (Systems)
    Small Industries Development Bank of India
    MSME Development Center, 3rd Floor,
    Information Technology Vertical [ITV],
    Plot No.C-11, 'G' Block
    Bandra Kurla Complex
    Bandra (East)
    Mumbai 400 051

****

7. Pre-Qualification / Minimum Eligibility Criteria

1. Proposals not complying with the 'Eligibility criteria' are liable to be rejected and will not be considered for further evaluation. The proposal should adhere to the following minimum eligibility criteria.

S. N.	Criteria	Supporting Documents Required
1.	The Bidder should be either a Government Organization/ PSU/ PSE/ partnership firm or a limited Company under Indian Laws or /and an autonomous Institution approved by GOI/RBI promoted.	a) Partnership firm: Certified copy of Partnership Deed OR b) Limited Company: Certified copy of Certificate of Incorporation and Certificate of Commencement of Business. c) Reference of Act/Notification d) For other eligible entities: Applicable documents.
2	The Bidder should have been in existence in India and must be engaged in the business of supply, maintenance and support of network and Security solutions in India for at least five (5) years as on date of RfP. (In case of mergers / acquisition / restructuring or name change, the date of establishment of the earlier / original partnership firm/limited company will be taken into account).	a. Partnership firm: Certified copy of Partnership Deed. OR Limited Company: Certified copy of Certificate of Incorporation and Certificate of Commencement of Business. b. Reference of Act/Notification c. For other eligible entities: Applicable documents. d. Copy of Work order / agreement / completion certificate for completed projects.
3	The bidder should have minimum average annual turnover of INR 25 Crore out of Indian Operations over the last three (3) Financial years.	Supporting the fact the bidder should furnish CA certificate for last three financial years ending in 2015.
4	The bidder should have positive net-worth and cash profit (i.e. no cash loss) in 2 years out of last 3 years.	
5	The bidder must have a currently valid Sales Tax / VAT / Service tax registration certificate and PAN number.	Copies of Sales Tax / VAT / Service tax / PAN to be enclosed.
6	The OEM(s) should authorize the bidder to quote their product(s) in the present tender of SIDBI.	MAF from respective OEMs (for each category of hardware – switches, firewalls and IPS) as per format given in **Annexure –V** enclosed.

S. N.	Criteria	Supporting Documents Required
7	The equipments offered should not be 'End of Support' for a minimum period of 6 years.	Certificate from respective OEM on Non-End of Support for a minimum period of 6 years to be enclosed.
8	The bidder should have executed at least one order of **Rs.100 lakh** for supply, installation and support of Network and Security solutions for Data Centre in at least one organization in BFSI sector / PSU / Government Organization in India during last 5 years.	Copy of PO issued
9	The bidder should have at least one certified engineer at Mumbai on OEM technology for network switches as proposed in the responses to the RfP.	Details of the engineer along with copy of certification of engineer to be attached.
10	The bidder should have trained and experienced engineers on the proposed firewalls and IPS at Mumbai.	Details of the engineer.
11	The OEM of proposed firewalls and dedicated IPS should feature in the Gartner's Magic Quadrant under the "leaders" or "challengers" quadrant as per latest Gartner report. **Note:** In case of firewall it should feature in Enterprise Network Firewall and for IPS in Intrusion Prevention System.	Proof of same to be attached.
12	The OEM of proposed network switches for Data Centre and DR Site, should have supplied and installed the same series/category of switches in at least 3 data centers in BFSI sector / PSU/ Government Organizations in India.	Declaration by the OEM on their letter head along with contact details of the customers to be submitted.
13	The bidder should have their own support arrangement at Mumbai and Chennai.	Details of support location along with address and contact details to be submitted.
14	The bidder should not have been black-listed by any Public Financial Institutions, Public Sector Bank, RBI or IBA or any other Government agencies during the last 3 years. Bidder	Self declaration to this effect on company's letter head signed by company's authorized signatory as per **Annexure-VIII**.

S. N.	Criteria	Supporting Documents Required
	must certify to that effect.	

2. In this tender, either the bidder on behalf of the Principal/ OEM or Principal/ OEM itself can bid but both cannot bid simultaneously for the same model/product.
3. If a bidder submits bid on behalf of the Principal/ OEM, the same bidder shall not submit a bid on behalf of another Principal/ OEM for the same item/ product.
4. Bank reserve the right to place the order with respective bidder(s) at the contracted price for all the items in single or multiple lots within the bid validity period.
5. The Bank reserves the right to alter the quantities or locations specified in the offer in the event of changes in plans of the Bank. The same shall be advised at the time of placing the order with shortlisted bidder(s).
6. The bidder to submit documentary evidence for all the above points along with **Annexure-III – Pre-Qualification / Minimum Eligibility Criteria**.
7. Proposals of bidders who do not fulfill the above criteria or who fail to submit the required data along with documentary evidence thereon would be rejected.
8. Last five years would be counted backward from the date of issue of RfP.

****

8. Evaluation Methodology

8.1. Clarification of bids

1. During evaluation of Bids, the Bank, at its discretion, may ask the Bidders for clarifications of their Bids. The request for clarification and the response shall be in writing (Courier/Fax/e-Mail), and no change in the price of substance of the Bid shall be sought, offered or permitted.
2. Bidder to submit point by point compliance to the technical compliance and it should be included in the Bid.
3. Any deviations from the specifications should be clearly brought out in the bid.
4. Bidder to quote for entire package on a single responsibility basis for the goods and services it proposes to supply under the contract.

8.2. Preliminary Examinations

1. The Bank will examine the Bids to determine whether they are complete, the documents have been properly signed, supporting papers/ documents attached and the bids are generally in order.
2. The Bank may, at its sole discretion, waive any minor infirmity, nonconformity or irregularity in a Bid which does not constitute a material deviation, provided such a waiver does not prejudice or affect the relative ranking of any Bidder.
3. Prior to the detailed evaluation, the Bank will determine the substantial responsiveness of each Bid to the Bidding document. For purposes of these Clauses, a substantially responsive Bid is one, which conforms to all the terms and conditions of the Bidding Document without material deviations. Deviations from or objections or reservations to critical provisions, such as those concerning Bid security, performance security, qualification criteria, insurance, Force Majeure etc will be deemed to be a material deviation. The Bank's determination of a Bid's responsiveness is to be based on the contents of the Bid itself, without recourse to extrinsic evidence.
4. If a Bid is not substantially responsive, it will be rejected by the Bank and may not subsequently be made responsive by the Bidder by correction of the nonconformity.
5. Bids without EMD / Bid security in the proper form and manner will be considered non-responsive and rejected**.**
6. The Bidder is expected to examine all instructions, forms, terms and specification in the Bidding Document. Failure to furnish all information required by the Bidding Document or to submit a Bid not substantially responsive to the Bidding Document in every respect will be at the Bidder's risk and may result in the rejection of its Bid.
7. The Bank would also evaluate the Bids on technical and functional parameters including possible visit to inspect live site(s) of the bidder, witness demos, bidders presentation, verify functionalities / response times etc.

8.3. Technical Evaluation

1. Pursuant to the evaluation of pre-qualification/ minimum eligibility criterion mentioned above, bidders will be short-listed for technical evaluation. Technical evaluation will be carried out only for the bidders who succeed the pre-qualification criterion.
2. SIDBI will review the technical bids of the short-listed bidders [who qualify the minimum eligibility criteria] to determine whether the technical bids are substantially responsive

and meeting the technical specifications given in the tender. Bids that are not substantially responsive are liable to be disqualified at SIDBI's discretion.

3. The bidder's disqualification during technical evaluation in any one item would result in disqualification of the tender as a whole.
4. During Technical evaluation the Bank at its discretion can ask the bidders for the demonstration / POC of all or some components/ features and components of the hardware items quoted by them.

   However, SIDBI will not pay/ reimburse any expenditure incurred by the vendor for arranging the demonstration / POC.
5. Bank may waive off any minor infirmity or nonconformity or irregularity in a bid, which does not constitute a material deviation, provided such a waiving, does not prejudice or effect the relative ranking of any bidder
6. Technical evaluation would be carried out and all bidders who qualify the technical evaluation will be short listed for commercial evaluation.

8.4. Commercial Evaluation

1. All the bidders who qualify in Technical evaluation as per the criteria mentioned above would be short listed for commercial evaluation.
2. Bidders who do not qualify the technical evaluation will NOT be invited for opening of commercials.
3. Lowest Cost bid would arrived as **(Cost of New Hardware with three years Warranty/support and inclusive of all taxes) + (AMC cost of each year inclusive of all taxes calculated at Present Value) + (Installation and Training Charges) + (Optional Items Cost).**

   The details of calculation are as given below:

   a) **W =** Cost of equipment inclusive of all taxes and back to back warranty and support for three years from OEM.

   b) **X =** AMC of all the equipments inclusive of all taxes and back to back alignment with OEM and support and for a period of three years, at Present Values (PV).

   The PV for the AMC component per year will be calculated as per the following formula:

$$\frac{C}{(1+r)^{n}}$$

Where:

- 'C' is the annual AMC amount of each year.
- 'r' is discount rate for calculation purpose will be taken as 8.32%.
- 'n' is number of years, i.e. 'n' is 4 for 1st year, 5 for 2nd year and 6 for 3rd year of AMC.

   c) **Y =** Cost towards Installation and training

   d) **Z =** Optional Item Cost

   e) **T = W+X+Y+Z**

4. Based on the above calculations the lowest quoted price (**T above**) will be termed as L1 bid and the rest of the bids shall be ranked in ascending order of price quoted, as L2, L3, L4 and so on.

8.5. Arithmetic errors correction

Arithmetic errors, if any, in the price break-up format will be rectified on the following basis:

1. If there is discrepancy between the unit price and the total price, which is obtained by multiplying the unit price with quantity, the unit price shall prevail and the total price shall be corrected unless it is a lower figure. If the supplier does not accept the correction of errors, its bid will be rejected.
2. If there is discrepancy in the unit price quoted in figures and words, the unit price, in figures or in words, as the case may be, which corresponds to the total bid price for the item shall be taken as correct.
3. It the vendor has not worked out the total bid price or the total bid price does not correspond to the unit price quoted either in words or figures, the unit price quoted in words shall be taken as correct.
4. Bank may waive off any minor infirmity or nonconformity or irregularity in a bid, which does not constitute a material deviation, provided such a waiving, does not prejudice or effect the relative ranking of any bidder**.**

8.6. Award of Contract

The Bank will award the contract to the successful Bidder, out of the Bidders who have responded to Bank's tender as referred above, who has been determined to qualify to perform the contract satisfactorily, and whose Bid has been determined to be substantially responsive, and is the lowest commercial Bid.

****

9. Special Terms and Conditions

9.1. Price

1. The price quoted by the bidder should be in Indian Rupee and should be inclusive of all local taxes, VAT, service tax, duties, levies, transportation costs, back to back support with OEM during warranty/AMC, insurance costs, training, implementation charges etc., till the bid validity period.
2. Once a contract price is arrived at, the same must remain firm throughout the period of contract and must not be subject to escalation during the performance of the contract due to fluctuation in foreign currency, change in the duty/tax structure, changes in costs related to the materials and labour or other components or for any other reason.
3. While any increase in the rates of applicable taxes or impact of new taxes imposed by GoI, subsequent to the submission of commercial bid shall be borne by SIDBI, any subsequent decrease in the rates of applicable taxes or impact of new taxes shall be passed on to SIDBI in its favour. This will remain applicable throughout the contract period (Warranty/AMC).
4. Octroi, if applicable, will be reimbursed as at actual, on production of the original octroi paid receipt in the name of the Bank.
5. No other cost whatsoever will be paid by SIDBI.

9.2. Terms of Payment

The standard payment terms of SIDBI would be:

1. **Payment for Supply, Installation, Warranty and Support**

   a) **50% payment:**

      i. On delivery and verification of items at respective locations/offices

      ii. Submission delivery challans duly signed, stamped, dated by SIDBI officials.

      iii. The vendor has to claim octroi paid, if any along with this payment.

   b) **40% payment:**

      i. On completion of Installation, configuration, integration with LAN/WAN and

      ii. Completion of training.

      iii. Installation certificate has to be submitted by the vendor as per format which will be given along with PO, duly signed, stamped and dated by the Bank officials.

   c) **10% payment:**

      i. On Acceptance of equipment by the Bank.

      ii. Submission of performance Bank Guarantee equivalent to 10% of the contract value. The BG shall be valid for a period of 36 MONTHS from the date of acceptance with invocation period of additional THREE months beyond expiry of warranty i.e, 36 months + 3 months. The performance bank guarantee should be as per the format given in **Annexure –XIV**.

iii. Submission of Back to back warranty certificate from OEM valid for a period of 3 years from date of acceptance and

iv. In case bidder does not submit PBG, the final 10% payment would be released after 3 months from completion of warranty period.

2. **Payment during AMC**

The payment terms during AMC would be paid annually 100% in advance on:

a) Submission of invoice

b) Proof of back to back alignment with OEM and

c) PBG (to be submitted annually) for 10% of the AMC value for the respective year valid for a period of 15 months.

d) In case vendor does not submit PBG, the payment would be released after 3 months from completion of AMC period.

3. All the payments will be made by SIDBI, Mumbai electronically through RTGS/ NEFT. Hence, Bidder to submit Bank Mandate Form (as per **Annexure –XIII**) along with cancelled cheque in original with technical bid.

4. Bidder will be required to furnish the documentary proof of delivery [delivery challan] and installation report duly signed by SIDBI officials, proof of back-to-back warranty arrangement certificate while claiming the appropriate payment.

5. TDS, if any, will be deducted while releasing the payment.

6. All Payments will be made to the Bidder in Indian Rupee only.

7. All payments will released within 4 weeks of receiving the undisputed invoice along with all the documentary proof.

8. The Bidder must accept the payment terms proposed by the Bank. The financial bid submitted by the Bidder must be in conformity with the payment terms proposed by the Bank. Any deviation from the proposed payment terms would not be accepted.

9. The Bank shall have the right to withhold any payment due to the Bidder, in case of delays or defaults on the part of the Bidder. Such withholding of payment shall not amount to a default on the part of the Bank.

9.3. Warranty and AMC

1. **Warranty**

a) The warranty of entire equipments / hardware (including OS) & software deployed for this project shall be onsite, comprehensive, back to back from OEM with NBD replacement of hardware for a period of 3 years (36 months) from the date of acceptance.

b) The bidder will warrant all the hardware and software against defects arising out of faulty design, materials and media workmanship of the hardware and software. The bidder will provide support for hardware and pre-installed software components including operating system during the warranty period. Defective hardware shall be replaced with new hardware by the vendor at his own cost, including the cost of transport.

c) The Bidder warrants that the Goods supplied under the Contract are new, unused, of the most recent or current models and incorporate all recent improvements in design and materials unless provided otherwise in the Contract.

d) The Bidder further warrants that all the Goods supplied under this Contract shall have no defect arising from design, materials or workmanship (except when the design and/or material is required by the Bank's Specifications) or from any act or omission of the Bidder, that may develop under normal use of the supplied Goods in the conditions prevailing at the final destination.

e) The warranty should cover all parts including updates, upgrades of software, maintenance and support for its proper operation, performance and output as specified in the tender technical specifications for a period of 36 months from the date of acceptance by the Bank at no cost to Bank.

f) In case equipment is taken away for repairs, the bidder shall provide similar standby equipment so that the equipments can be put to use in the absence of the originals/ replacements without disrupting the Bank's regular work.

g) Warranty should not become void if the Bank buys any other add-on hardware from a third party and installs it with in hardware items in the presence of the representative of the bidder. However, the warranty will not apply to such third-party hardware items installed by the Bank.

2. **Annual Maintenance Contract**

a) The selected bidder will enter into **comprehensive onsite AMC** with back to back from OEM for a period of 3 years, for post warranty maintenance after the expiry of the warranty period. However, if the support of the bidder is not satisfactory, the bank will be having right to go with any other vendor for AMC if so desired.

b) The bidder should provide changes, updates, upgrades with regard to changes in statutory requirements to the Bank at free of cost during the contract period. Also the bidder should provide and implement functionality changes as required by the Bank during the contract period.

c) In the case of authorized/ channel partners, AMC charges shall also include the cost for the back to back arrangement with OEM for maintenance of spares, providing support services, updates, upgrades for providing AMC support for period.

d) **Termination of AMC contract** [if contracted]**:** Bank will terminate the AMC contract on occurrence of the following:

i. Material(s) default by either party in the performance of any of its obligations to the other under this Agreement, if same is not cured within thirty days after written Notice thereof.

ii. Without prejudice to any other right or remedy, upon the filing of a petition in bankruptcy or insolvency by or against the other, or upon any act of bankruptcy, including a condition of insolvency, or should the other make an assignment for the benefit of creditors, and the appointment of a receiver subsequent to such filing, act, or assignment.

iii. Bidder failure to meet the performance requirement specified herein

iv. However, the selected bidder shall commit himself to service for a minimum period of 6 years, unless the service contract is terminated by the Bank and the selected bidder will have no right to terminate the contract within this period.

3. During the Warranty/AMC period, the Bidder will have to undertake system maintenance and replacement or repair of defective parts or systems.

4. The Bank shall promptly notify the Bidder in writing / e-mail / fax of any claims arising under this warranty. Upon receipt of such notice the Bidder shall, as mentioned below, repair or replace the defective goods or parts thereof, without any cost to the Bank.
5. Any corruption in the software or media shall be rectified during the full period of the contract including warranty/AMC, if contracted, at no extra cost to the Bank.
6. The bidder shall make available the spare parts, components etc, for the equipments for a minimum period of six years. If any of the peripherals/components are not available during the Warranty / AMC period, the substitution shall be carried out with peripherals/components of equivalent or higher capacity.
7. In case some equipment is declared by the bidder as beyond repairs, the bidder shall provide a NEW replacement equipment of the same of higher configuration from the same OEM with prior approval of the bank.
8. **Mean Time Between Failures (MTBF):** If during the warranty and AMC period, any hardware and/or software items fails on three or more occasions in a quarter, such hardware items shall be replaced by equivalent / superior NEW hardware items by the bidder at no additional cost to the Bank.
9. To periodically update bank on new features as and when released by the OEM through technical sessions, trainings etc.
10. During Warranty/AMC the bidder should provide comprehensive on-site 24X7X365 support free of cost.

9.4. Uptime

1. The bidder shall guarantee an uptime of **99.5%** for the equipment supplied at DC and DR, during Warranty and AMC period, which shall be calculated on monthly basis.
2. The "Downtime" is the time between the Time of Report by the Bank and Time of Restoration/resolution within the contracted hours. "Failure" is the condition that renders the bank unable to access the services hosted in data center or DR site . "Restoration" is the condition when the selected bidder demonstrates that the services hosted in data center and DR site are accessible.
3. The Downtime calculated shall not include any:
    a) Failure due to bank (Power, cabling fault, servers etc.)
    b) Preventive maintenance activity and
    c) Force Majeure.
4. The percentage uptime is calculated on monthly basis (24 hours a day).
5. The performance would be measured as under on monthly basis:

$$\text{Performance (\%)} = \frac{\text{(Total contracted minutes in a month – downtime Minutes within contracted minutes in a month)}}{\text{Total contracted minutes in a month}} \times 100$$

Shortfall in performance = uptime % - Performance %

6. Penalty would be charged for shortfall in performance compliance level.
7. **Call to Response:** Vendor's hardware engineer will report at SIDBI offices within **'TWO HOURS'** of reporting of breakdown through telephone/ email or portal to the vendor's centralized helpdesk as per call logging and escalation matrix.

8. **Call to Resolution:** Vendor shall resolve the issue within **'FOUR HOURS'** of its reporting.
9. The replacement of faulty hardware during Warranty/AMC should be **NBD**. However, in case both the hardware fails, the bidder to replace the hardware within 4 hours.

9.5. Penalty for Default Delivery

1. If the vendor fails to deliver the items within stipulated period, Bank will impose a penalty of 1% of the order value for the late delivered item for each weeks delay or part thereof, subject to maximum of 10% of value of the late delivered items.
2. In case the delay exceeds TEN weeks, Bank reserves the right to cancel the order. In such an event vendor will not be entitled to or recover from Bank any amount by ways of damages, loss or otherwise.
3. If orders are cancelled due to non delivery, the vendor will also be debarred by Bank for participating in any future tenders floated by Bank.

9.6. Penalty for Delay in Installation

1. If the vendor fails to install the items within Six (6) weeks from date of delivery, Bank will impose a penalty of 1% of the order value for the late installed item for each week's delay or part thereof, subject to maximum of 5% of value of the late installed items.
2. However, no penalty will be imposed for the durations leading to delays in installation of hardware / software due to reasons solely attributable to the Bank.
3. The vendor will be required to inform the banks well in advance the installation schedule / plan to enable the Bank to make the site ready and obtaining downtime etc.

9.7. Penalty for Non-Performance of Preventive Maintenance

1. If the vendor fails to carry out preventive maintenance during Warranty and AMC and submit the reports, Bank will impose a penalty of Rs.1,000/- for each incidence, subject to maximum of 10% of ordered / AMC value of the item.
2. No penalty will be imposed for any reason solely attributable to the Bank. However, in such case the bidder has to submit the reasons for not carrying out PM duly signed by the official of SIDBI at the location.
3. The vendor will be required to forward to the banks well in advance the PM schedule / plan to enable the Bank to intimate the locations/offices and obtaining downtime etc.

9.8. Penalty for shortfall in Performance Compliance Level

1. If the bidder fails to maintain guaranteed uptime of **99.5%** per month for all the ordered items, during Warranty and AMC the Bank shall impose penalty.
2. Amount of penalty to be calculated on monthly basis for the shortfall in performance compliance level is as under:

Shortfall in performance	Penalty (% of the contract value of the equipment)
<= 1%	1
>1% and <= 3%	3
>3% and <= 5%	5
>5% and <=6%	6
>6% and <=8%	8
>8%	10

4. The above penalty shall be applied for each equipment separately.
5. The amount of penalty may be claimed/ adjusted while releasing the Performance Bank Guarantee or vendor will be advised to pay the same.
6. However, no penalty will be imposed for the reasons solely attributable to the Bank, in such cases the bidder has to submit the proof.

****

10. General Terms and Conditions

10.1. Definitions

In this Contract, the following terms shall be interpreted as indicated:

1. "The Bank", "SIDBI" , "Buyer" means Small Industries Development Bank of India (SIDBI);
2. "Bidder'", "Vendor", "Supplier", "Seller" means the respondent to the RFP document.
3. "RFP" or "Tender" or "RfP" or 'Bid document' means the 'Request for Proposal document.
4. "Bid" may be referred to as 'Offer'.
5. "The Contract" means the agreement entered into between the Bank, represented by its Head Office / MSME Development Centre / Regional Offices and the Supplier, as recorded in the Contract Form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein;
6. "The Contract Price" means the price payable to the Supplier under the Contract for the full and proper performance of its contractual obligations;
7. "The Goods" means all of the equipment, machinery, software, and/or other materials which the Supplier is required to supply to the Bank under the Contract;
8. "The Services" means those services ancillary to the supply of the Goods, such as transportation and insurance, and any other incidental services, such as installation, commissioning, provision of technical assistance, support, maintenance, training and other such obligations of the Supplier covered under the Purchase Contract;
9. "The Project Site" means, Small industries Development Bank of India locations/offices.

10.2. Use of Contract Documents and Information

1. The Supplier shall not, without the Bank's prior written consent, disclose the Contract, or any provision thereof, or any specification, plan, drawing, pattern, sample or information furnished by or on behalf of the Bank in connection therewith, to any person other than a person employed by the Supplier in the performance of the Contract. Disclosure to any such employed person shall be made in confidence and shall extend only as far as may be necessary for purposes of such performance.
2. The Supplier will treat as confidential all data and information about the Bank, obtained in the execution of his responsibilities, in strict confidence and will not reveal such information to any other party without the prior written approval of the Bank.

10.3. Subcontracts

The Supplier shall not assign to others, in whole or in part, its obligations to perform under the contract without prior written permission from the Bank.

10.4. Technical Information

1. The Bidder should strictly quote for the Brand/ Model complying with technical specifications given in **Annexure – III**.
2. The technical documentation involving detailed instruction for operation and maintenance, users' manual etc., is to be delivered with every unit of the equipment supplied. The language of the documentation should be English.

3. The Models offered should strictly conform to the specifications given in the product literature and these models should be supported for a minimum period of 6 years including warranty period and post warranty maintenance (AMC). The Models proposed/ marked for withdrawal from the market and the models under quality testing should not be offered. Bank shall reserve right to ask for PROOF OF CONCEPT on working of the newly introduced Models in the market, if offered, on the agreed terms & conditions.
4. When the configuration/ feature required is not available in a particular model, the next available higher configuration model shall be offered.
5. In addition to the above, if any additional/ enhanced configuration is suggested in view of technological changes, it may be furnished as optional feature with/ without cost duly explaining the additional utility of the offered model in both the technical offer document as well as Commercial Offer document. However, the basic quote should be confined only to the configuration/ model offered for.

10.5. Governing language

1. The Contract shall be written in English. All correspondence and other documents pertaining to the Contract, which are exchanged by the parties, shall be written in English.
2. The technical documentation involving detailed instruction for operation and maintenance, users'
3. Manual, cables, accessories etc. is to be delivered with every unit of the equipment supplied. The language of the documentation should be English.

10.6. Applicable laws

The Contract shall be interpreted in accordance with the laws prevalent in India.

10.7. Compliance with all applicable laws

The Bidder shall undertake to 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 Tender 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 therefrom.

10.8. 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 therefrom and the Bank will give notice of any such claim or demand of liability within reasonable time to the bidder.

10.9. Performance security

1. **During Warranty**

   a) The successful bidder(s) shall provide Performance Security in the form of an unconditional Bank Guarantee (BG) from a scheduled commercial Bank for an amount equivalent to 10% of contract value and valid for WARRANTY period + THREE months (invocation period) from the date of acceptance.

   b) The performance guarantee to be submitted within ONE month after acceptance of goods and before release of full and final payment of the Contract for indemnifying Bank against any default / failure in execution of contract, as per the format provided by Bank.

   c) Since the validity of the BG is linked to the warranty/ acceptance of the hardware, the bidder shall submit the BG only after getting the confirmation from the Bank about the acceptance & warranty period.

2. **During AMC**

   The successful bidder(s) shall provide Performance Security in the form of an unconditional Bank Guarantee (BG) from a scheduled commercial Bank for an amount equivalent to 10% of annual AMC value and valid for 15 months (including invocation period of 3 months) from the date of start of AMC. The BG to be submitted annually for the AMC period.

10.10. Insurance

1. The Bidder is responsible for acquiring insurance for all components, equipment and software. The goods supplied under the Contract shall be fully insured.
2. The insurance shall be for an amount equal to 110 percent of the CIF value of the Goods delivered to SIDBI covering “All Risks” (fire, burglary, natural calamities such as Earth quake, floods etc.) valid till one month from the date of delivery. If the vendor fails to obtain insurance cover and any loss or damage occur, the vendor will have to replace the items with new ones without any cost to the Bank.
3. Where the Supplier is required under the Contract to transport the Goods to a specified place of destination within India, transport to such place of destination in India, including insurance and storage, as shall be specified in the Contract, shall be arranged by the Supplier
4. Should any loss or damage occur, the Bidder shall

   a) Initiate and pursue claim till settlement, and

   b) Promptly make arrangements for replacement of any damaged item/s irrespective of settlement of claim by the underwriters.

10.11. Inspections and tests

1. Inspection and Quality Control tests before evaluation, prior to shipment of Goods and at the time of final acceptance are as follows:

   a) Inspection/Pre-shipment Acceptance Testing of Goods as per quality control formats including functional testing, burn-in tests and mains fluctuation test at full load, facilities etc., as per the standards / specifications may be done at factory site of the Supplier before dispatch of goods, by the Bank / Bank’s Consultants /Testing Agency. The supplier should intimate the Bank before dispatch of goods to various

locations/ offices for conduct of pre-shipment testing. Successful conduct and conclusion of pre-dispatch inspection shall be the sole responsibility of the Supplier.

b) Provided that the Bank may, at its sole discretion, waive inspection of goods having regard to the value of the order and/or the nature of the goods and/or any other such basis as may be decided at the sole discretion of the Bank meriting waiver of such inspection of goods.

c) In the event of the hardware and software failing to pass the acceptance test, as per the specifications given, a period not exceeding two weeks will be given to rectify the defects and clear the acceptance test, failing which, the Bank reserves the right to cancel the Purchase Order.

2. Nothing stated herein above shall in any way release the Supplier from any warranty or other obligations under this Contract.

3. The Supplier shall provide complete and legal documentation of Systems, all subsystems, operating systems, system software and the other software. The Supplier shall also provide licensed software for all software products, whether developed by it or acquired from others. The Supplier shall also indemnify the Bank against any levies/penalties on account of any default in this regard.

4. On successful completion of acceptability test, receipt of deliverables, etc., and after the Bank is satisfied with the working on the system, the acceptance certificate will be signed by the, Testing Agency and the representative of the Bank.

10.12. Delivery and Installation Schedule

1. **Delivery**

a) The Bidder should deliver the goods within **EIGHT WEEKS FROM THE DATE OF PURCHASE ORDER**.

b) Delivery of the Goods shall be made by the Supplier in accordance with the terms of the Purchase Contract. The bidder should take responsibility of the Goods till it reaches the delivery destination as informed by Bank, transport to such place of destination in India, including insurance and storage, as shall be specified in the Contract, shall be arranged by the Supplier.

c) Products shall be supplied in a ready to use condition along with all Cables, Connectors, Software Drivers, Manuals and Media etc.

d) Bidder shall arrange the Road Permits or any other document wherever required. Any letter required for this will be given by the Bank.

e) The Bank will not be in a position to supply Form-C or Form-D and bidder will have to arrange for Form 31 or 32 or any other road permit, if required, on behalf of SIDBI

2. **Installation**

a) The Bidder shall install the goods and integrate with existing network within **SIX WEEKS** from the date of delivery of the equipment at respective location.

b) The Bidder to explain the Bank officials the details of all the features and functionality of the solution.

c) After completion of installation the bidder should obtain Installation certificate (the format of which would be shared with the shortlisted vendor(s)) from the Bank official at respective locations. SIDBI will carry out acceptance of hardware as per acceptance test plan.

d) Installation will be treated as incomplete in one/all of the following situations:

i. Non-delivery of any hardware or other components viz. accessories, documentation, software/ drivers media mentioned in the order.

ii. Non-delivery of supporting documentation.

iii. Delivery, but no installation of the components and/or software.

iv. Improper integration, configuration and migration of policies.

v. System operational, but unsatisfactory to the Bank.

3. The Bank will consider the inability of the Bidder to deliver or install the equipment within the specified time limit, as a breach of contract and would entail the payment of Liquidation Damages on the part of the Bidder.

4. The Bank shall, without prejudice to its other remedies under the Contract, deduct from the Contract Price, as liquidated damages, a sum as specified in Special Terms and Conditions

10.13. Locations for Delivery & Installation and Buy-back

The equipments to be delivered, installed and maintained at the following locations:

S.N.	Item Description	Qty.	Remarks	Address
A.	**Data Centre, Mumbai**			
1.	Core Switches	02	Refer Annexure – III (1.1) for detailed specifications.	SIDBI, MSME Development Centre, 3rd Floor, Information Technology Vertical (ITV), Plot No.C-11, G Block, Bandra Kurla Complex, Bandra(E), **Mumbai – 400051**
2.	Top of Rack Switches	06	Refer Annexure – III (1.2) for detailed specifications.	
3.	DMZ Switches	02	Refer Annexure – III (1.3) for detailed specifications.	
4.	Stackable switches	04	Refer Annexure – III (1.4) for detailed specifications.	
5.	Perimeter Firewall	02	Refer Annexure – III (1.5) for detailed specifications.	
6.	Dedicated IPS	02	Refer Annexure – III (1.6) for detailed specifications.	
B.	**DR Site, Chennai**			
1.	Core Switches	02	Refer Annexure –III (2.1) for detailed specifications.	SIDBI, Overseas Towers, 756-L, Anna Salai, **Chennai – 600002** Tamil Nadu
2.	Top of Rack Switches.	02	Refer Annexure –III (2.2) for detailed specifications.	
3.	DMZ Switches	02	Refer Annexure –III (2.3) for detailed specifications.	
4.	Layer 2 Stackable switches	04	Refer Annexure –III (2.4) for detailed specifications.	
5.	Core Firewall	02	Refer Annexure –III (2.5) for detailed specifications.	

10.14. Delivery and Documents

The details of shipping and/or other documents to be furnished by the Supplier are specified hereunder.

1. Original copy of the delivery challan. duly signed with name, designation, date and seal of the office concerned affixed. The challan should contain the seal and date of receipt of the equipment by SIDBI location.
2. Original copy of Supplier's invoices showing contract number, goods description, quantity, unit price and total amount;
3. Inspection Certificate issued by the nominated inspection agency and the Supplier's factory inspection report and Quality Control Test Certificates, if any. Commissioning of Solution
4. The Supplier is responsible for all unpacking and installation of Products. The Supplier will ensure that all systems along with software have been commissioned as per scope for successful and continuous operation at all installation sites.

10.15. Acceptance

1. The acceptance / performance test will be performed after completion of installation of all the equipments at the location. Complete hardware and Software as specified in the tender must have been supplied & installed properly by the Bidder prior to acceptance of the same. The acceptance test will be conducted by the Bank, their consultant or other such person nominated by the Bank at its option. The Bidder will be responsible for setting up and running the acceptance test without any extra cost to the Bank.
2. 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.
3. In the event of hardware and software failing to pass the acceptance test, a period not exceeding two weeks will be given to rectify the defects and clear the acceptance test, failing which the Bank reserves the right to get the corresponding component replaced by the Bidder at no extra cost to the Bank or to cancel the order and recall all the payments made by the bank to the bidder.
4. Successful conduct and conclusion of the acceptance tests for the installed components shall also be the sole responsibility and at the cost of the Bidder. During acceptance testing the bidder has to demonstrate all the features of the respective hardware items.
5. The Bank's right to inspect, test and, where necessary, reject the Goods after the Goods' arrival at destination shall in no way be limited or waived by reason of the Goods having previously been inspected, tested and passed by the Bank or its representative prior to the shipment of the goods.
6. Acceptance test would be carried out after five working days from the date of installation by the network management team at Datacenter, Mumbai. The vendors engineer from Mumbai should be available at SIDBI, Mumbai location during the acceptance testing.

S.N	Nature of activity	Remarks
1	Physical Delivery of the hardware items as per the PO and Installation.	➢ Delivery of ordered items along with accessories, cables, manuals etc as per order. ➢ Installation of the items in the rack after removal of old equipment.
2	Configuration	➢ Configuration of the equipment as per scope

S.N	Nature of activity	Remarks
		of work which includes: • Creation of various zones on the core and perimeter. • Adding policies on the firewalls (new and existing) • Integrate of all the equipments with existing network etc.
3	Verification of features	➢ Verification of features as asked for in technical bid.
4	Commissioning and go-live.	➢ Successful working of the solution for at least 10 working days.
5	Acceptance Certificate.	➢ On successful completion of acceptance test, bidder would be provided acceptance certificate.

10.16. Acceptance Date

1. Bidder shall submit all the duly signed Installation Certificates at Bank's Mumbai office.
2. For the convenience of the bidder and the Bank, single acceptance date would be arrived for the entire lot of purchase by taking weighted average of all the installation dates. Accordingly, the warranty period of 3 years starting from the date of acceptance, shall be determined and conveyed to the bidder in writing.
3. The **back to back warranty certificate from OEM should be from date of acceptance** and the same to be submitted for release of final payment.

10.17. Repeat Order / Order for Optional Items

1. The bank reserves the right to place order for additional hardware item(s) at same rates and terms & conditions during a period of one year from the date of acceptance of purchases order by the bidder. No additional cost whatsoever other than the cost contracted would be paid.
2. In case of any change in tax rates, the taxes prevailing at the time of placing repeat order would be applicable.

10.18. Change / Modification in Locations for Delivery/Installation/support

1. Bank reserves the right to change/modify locations for supply of the items. In the event of any change/modification in the locations where the hardware items are to be delivered, the bidder in such cases shall deliver, install and commission at the modified locations at no extra cost to the Bank.
2. In case the hardware items are already delivered, and if the modifications in locations are made after delivery, the bidder shall carry out installation and commissioning at the modified locations. The Bank in such cases shall bear the shifting charges/arrange shifting and the bidder shall shift the material to the alternate locations at mutually agreed price if bank request.
3. The Warranty/AMC/support should be applicable to the altered locations also.

4. The change / modification of location would be due to Banks requirement for re-allocation of hardware or due to co-location of data center and/or DR site during the contract period.

10.19. Forfeiture of performance security

The Bank shall be at liberty to set off/adjust the proceeds of the performance guarantee towards the loss, if any, sustained due to the supplier's failure to complete its obligations under the contract. This is without prejudice to the Bank's right to proceed against the Supplier in the event of the security being not enough to fully cover the loss/damage.

10.20. No Commitment to Accept Lowest or Any Offer

1. The Bank reserves its right to reject any or all the offers without assigning any reason thereof whatsoever.
2. The Bank will not be obliged to meet and have discussions with any bidder and/ or to entertain any representations in this regard.
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.

10.21. Conditional Bids

Conditional bids shall not be accepted on any ground and shall be rejected straightway. If any clarification is required, the same should be obtained before submission of bids.

10.22. Contacting the Bank

1. Bidder shall NOT contact the Bank on any matter relating to its Bid, from the time of opening of Bid to the time a communication in writing about its qualification or otherwise received from the Bank.
2. Any effort by the Bidder to influence the Bank in its decisions on Bid evaluation, Bid comparison may result in the rejection of the Bidder's Bid.

10.23. Taken / Brought over of Company

Subsequent to the order being placed with SIDBI, in the event of bidder or the concerned OEM being taken/ brought over by another company, all the obligations and execution of responsibilities under the agreement with SIDBI should be passed on for compliance by the new company in the negotiation for their transfer.

10.24. No Employer – Employee Relationship

The selected bidder or any of its holding / subsidiary / joint-venture / affiliate / group / client companies or any of their employees / officers / staff / personnel / representatives / agents shall not, under any circumstances, be deemed to have any employer-employee relationship with the Bank or any of its employees / officers / staff / representatives / personnel / agents.

10.25. Termination

1. Prior to the delivery of the hardware items, the Bank may at any time terminate the contract by giving written notice to the Bidder if the Bidder becomes bankrupt or otherwise insolvent. In this event, termination will not prejudice or affect any right of action or remedy, which has accrued or will accrue thereafter to the Bank.

2. The Bank reserves the right to cancel the contract in the event of happening one or more of the following Conditions:
    a) Failure of the successful bidder to accept the contract;
    b) Delay in delivery beyond the specified period;
    c) Delay in completing installation / configuration / implementation and acceptance tests / checks beyond the specified periods;
    d) Serious discrepancy in hardware noticed during the pre-dispatch factory inspection; and
3. In addition to the cancellation of purchase contract, Bank reserves the right to appropriate the damages through encashment of Bid Security / Performance Guarantee given by the Bidder.

10.26. Termination of AMC Contract

Bank will terminate the AMC contract on occurrence of the following:

1. Material(s) default by either party in the performance of any of its obligations to the other under this Agreement, if same is not cured within thirty days after written Notice thereof.
2. Without prejudice to any other right or remedy, upon the filing of a petition in bankruptcy or insolvency by or against the other, or upon any act of bankruptcy, including a condition of insolvency, or should the other make an assignment for the benefit of creditors, and the appointment of a receiver subsequent to such filing, act, or assignment.
3. Bidder failure to meet the performance requirement specified herein
4. However, the selected bidder shall commit himself to service for a minimum period of 6 years, unless the service contract is terminated by the Bank and the selected bidder will have no right to terminate the contract within this period.

10.27. Patent Rights

In the event of any claim asserted by a third party of infringement of copyright, patent, trademark, industrial design rights, etc. arising from the use of the Goods or any part thereof in India, the Supplier shall act expeditiously to extinguish such claim. If the Supplier fails to comply and the Bank is required to pay compensation to a third party resulting from such infringement, the Supplier shall be responsible for the compensation including all expenses, court costs and lawyer fees. The Bank will give notice to the Supplier of such claim, if it is made, without delay.

10.28. Corrupt and fraudulent practice

1. As per Central Vigilance Commission (CVC) directives, it is required that Bidders / Suppliers / Contractors observe the highest standard of ethics during the execution of this RfP and subsequent contract(s). In this context, the bidders to note the following:
    a) **"Corrupt Practice"** means the offering, giving, receiving or soliciting of anything of value to influence the action of an official in the procurement process or in contract execution.
    b) **"Fraudulent Practice"** means a misrepresentation of facts in order to influence a procurement process or the execution of contract to the detriment of the Bank and includes collusive practice among bidders (prior to or after bid submission) designed to establish bid prices at artificial non- competitive levels and to deprive the Bank of the benefits of free and open competition.

2. The Bank reserves the right to declare a bidder ineligible, either indefinitely or for a stated period of time, to be awarded a contract if at any time it determines that the bidder has engaged in corrupt or fraudulent practices in competing for or in executing the contract.

10.29. Waiver

No failure or delay on the part of either party relating to the exercise of any right power privilege or remedy provided under this RFP or subsequent agreement with the other party shall operate as a waiver of such right power privilege or remedy or as a waiver of any preceding or succeeding breach by the other party nor shall any single or partial exercise of any right power privilege or remedy preclude any other or further exercise of such or any other right power privilege or remedy provided in this RFP all of which are several and cumulative and are not exclusive of each other or of any other rights or remedies otherwise available to either party at law or in equity.

10.30. Violation of terms

The Bank clarifies that the Bank shall be entitled to an injunction, restraining order, right for recovery, specific performance or such other equitable relief as a court of competent jurisdiction may deem necessary or appropriate to restrain the Bidder from committing any violation or enforce the performance of the covenants, obligations and representations contained in this RFP. These injunctive remedies are cumulative and are in addition to any other rights and remedies the Bank may have at law or in equity, including without limitation a right for recovery of any amounts and related costs and a right for damages.

10.31. Confidentiality

1. This RfP contains information proprietary to SIDBI. Each recipient is entrusted to maintain its confidentiality. It should be disclosed only to those employees involved in preparing the requested responses. The information contained in the RfP may not be reproduced in whole or in part without the express permission of SIDBI. The Bidders shall submit a non-disclosure agreement as per **Annexure -X** on non-judicial stamp paper of appropriate value at the time of submission of bids.
2. In case the selected vendor acts is extending similar services to multiple customers, vendor shall take care to build strong safeguards so that there is no co-mingling of information, documents, records and assets related to services within the ambit of this RfP and subsequent purchase order.

10.32. IPR Infringement

As part of this project, bidder / service provider will deliver different software, if the use of any such software by / for SIDBI, infringes the intellectual property rights of any third person, Service provider shall be primarily liable to indemnify SIDBI to the extent of direct damages against all claims, demands, costs, charges, expenses, award, compensations etc. arising out of the proceedings initiated by third party for such infringement, subject to the condition that the claim relates to Software provided/used by Bidder/Service provider under this project.

10.33. Limitation of liability

Save and except the liability under Section of 'IPR Infringement' and/or indemnity provision in Clause 10.32 and Clause 10.39 hereinbelow, in no event shall either party be liable with respect to its obligations for indirect, consequential, exemplary, punitive, special, or incidental damages, including, but not limited to, loss of data / programs or lost profits, loss of goodwill, work stoppage, computer failure, loss of work product or any and all other

commercial damages or losses whether directly or indirectly caused, even if such party has been advised of the possibility of such damages. The aggregate liability of the Service Provider, arising at any time under this Agreement shall not exceed the order value.

10.34. Rights to Visit

1. All records of the Bidder with respect to any matters covered by this Tender document/ subsequent order shall be made available to SIDBI or its designees at any time during normal business hours, as often as SIDBI deems necessary, to audit, examine, and make excerpts or transcripts of all relevant data.
2. SIDBI, including its regulatory authorities like RBI etc., reserves the right to verify, through their officials or such other persons as SIDBI may authorise, the progress of the project at the development /customization site of the Bidder or where the services are being rendered by the bidder.
3. The Bank and its authorized representatives, including regulator like Reserve Bank of India (RBI) shall have the right to visit any of the Bidder's premises with prior notice to ensure that data provided by the Bank is not misused. The Bidder will have to cooperate with the authorized representative/s of the Bank and will have to provide all information/ documents required by the Bank.

10.35. Audit

The vendor shall allow the Bank, its authorised personnel, its auditors (internal and external), authorised personnel from RBI / other regulatory & statutory authorities, and grant unrestricted right to inspect and audit its books and accounts, to provide copies of any audit or review reports and findings made on the service provider, directly related to the services. In case any of the services are further outsourced/assigned/ subcontracted to other vendors, it will be the responsibility of the vendor to ensure that the authorities / officials as mentioned above are allowed access to all the related places, for inspection and verification.

10.36. Grievances Redressal Mechanism

Bank has a grievances redressal mechanism for its customers and designated grievances redressal officers. The bank would use the same mechanism to address the grievances, if any, of the customers related to the services being rendered within the ambit of this RfP.

10.37. Compliance with Statutory and Regulatory Provisions

It shall be the sole responsibility of the Vendor to comply with all statutory and regulatory provisions while delivering the services mentioned in this RFP, during the course of the contract.

10.38. Right of Publicity

Any publicity by the Bidder in which the name of SIDBI is to be used should be done only with the explicit written permission of SIDBI.

10.39. Indemnity

1. The Bidder/ successful bidder shall indemnify the Bank, and shall always keep indemnified and hold the Bank, its employees, personnel, officers, directors, harmless from and against any and all losses, liabilities, claims, actions, costs and expenses (including attorneys' fees) relating to, resulting directly or indirectly from or in any way arising out of any claim, suit or proceeding brought against the Bank as a result of:
2. Bank's authorized / bona fide use of the Deliverables and /or the Services provided by Bidder under this RfP document; and/or

3. An act or omission of the Bidder, employees, agents, sub contractors in the performance of the obligations of the Bidder under this RfP document; and/or
4. Claims made by employees or subcontractors or subcontractors' employees, who are deployed by the Bidder, against the Bank; and/or
5. Breach of any of the term of this RfP document and/or of the agreement to be entered subsequent this RfP or breach of any representation or false representation or inaccurate statement or assurance or covenant or warranty by the successful Bidder under this RfP document and/or of the agreement to be entered subsequent this RfP; and/or
6. Any or all Deliverables or Services infringing any patent, trademarks, copyrights or such other Intellectual Property Rights; and/or
7. Breach of confidentiality obligations of the Bidder contained in this RfP document; and/or
8. Negligence, fraudulence activities or gross misconduct attributable to the bidder or its employees or sub-contractors; and/or
9. The use of unlicensed and illegal Software and/or allied components by the successful Bidder
10. The Bidder will have to at its own cost and expenses defend or settle any claim against the Bank that the Deliverables and Services delivered or provided under this RfP document infringe a patent, utility model, industrial design, copyright, trade secret, mask work or trade mark in the country where the Deliverables and Services are used, sold or received, provided the Bank:
    a) Notifies the Bidder in writing; and
    b) Cooperate with the bidder in the defense and settlement of the claims.
11. The Bidder shall not be liable for defects or non-conformance resulting from:
    a) Software, hardware, interfacing not approved by Bidder; or
    b) Unauthorized modification of Software or any individual product supplied under this RfP document, or Bank's failure to comply with any mutually agreed environmental specifications.
    c) Use of a Deliverable in an application or environment for which it was not designed or not contemplated under this Agreement;
    d) Modification of a deliverable by anyone other than the bidder where the unmodified version of the deliverable would not be infringing.

10.40. Force majeure

1. If the performance as specified in this order is prevented, restricted, delayed or interfered by reason of Fire, explosion, cyclone, floods, War, revolution, acts of public enemies, blockage or embargo, Any law, order, proclamation, ordinance, demand or requirements of any Government or authority or representative of any such Government including restrict trade practices or regulations, Strikes, shutdowns or labour disputes which are not instigated for the purpose of avoiding
2. obligations herein, or Any other circumstances beyond the control of the party affected, then notwithstanding anything here before contained, the party affected shall be excused from its performance to the extent such performance relates to prevention, restriction, delay or interference and provided the party so affected uses its best efforts to remove such cause of non-performance and when removed the party shall continue performance with utmost dispatch.

3. If a Force Majeure situation arises, the Bidder shall promptly notify the Bank in writing of such condition, the cause thereof and the change that is necessitated due to the conditions. Until and unless otherwise directed by the Bank in writing, the Bidder shall continue to perform its obligations under the Contract as far s is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event

10.41. Resolution of Disputes

1. It will be the Bank's endeavor to resolve amicably any disputes or differences that may arise between the Bank and the Bidder from misconstruing the meaning and operation of the Tender and the breach that may result.
2. In case of Dispute or difference arising between the Bank and a Supplier relating to any matter arising out of or connected with this agreement, such disputes or difference shall be settled in accordance with the Arbitration and Conciliation Act, 1996. The Arbitrators shall be chosen by mutual discussion between the Bank and the Supplier OR in case of disagreement each party may appoint an arbitrator and such arbitrators may appoint an Umpire before entering on the reference. The decision of the Umpire shall be final.
3. The Bidder shall continue work under the Contract during the arbitration proceedings unless otherwise directed in writing by the Bank or unless the matter is such that the work cannot possibly be continued until the decision of the Arbitrator or the umpire, as the case may be, is obtained.
4. Arbitration proceedings shall be held at Mumbai, India, and the language of the arbitration proceedings and that of all documents and communications between the parties shall be English;
5. Not withstanding anything contained above, in case of dispute, claim & legal action arising out of the contract, the parties shall be subject to the jurisdiction of courts at Mumbai, India only.
6. Any notice given by one party to the other pursuant to this Contract shall be sent to the other party in writing or by fax and confirmed in writing to the other party's specified address. The same has to be acknowledged by the receiver in writing.
7. A notice shall be effective when delivered or on the notice's effective date, whichever is later.

****

11. Annexure

11.1. Annexure I - Bid Forwarding Letter

(To be submitted on Bidders letter head)

Date: _____

The General Manager (Systems)
Small Industries Development Bank of India,
3rd Floor, Information Technology Vertical
MSME Development Centre,
Plot No. C-11, G Block
Bandra Kurla Complex (BKC), Bandra (E)
Mumbai - 400 051

Dear Sir,

Procurement of Network Switches, Security Appliances and Implementation

1. We, the undersigned, offer to submit our bid in response and accordance with your tender No. 400/2016/1152/BYO/ITV dated February 24, 2016. Having examined the tender document including all Annexures carefully, we are hereby submitting our proposal along with all the requisite EMD and other documents as desired by the Bank.
2. Further, we agree to abide by all the terms and conditions as mentioned herein the tender document. We agree to abide by this offer till 180 days from the date of last day for submission of offer (Bid).
3. If our offer is accepted we undertake to provide on-site comprehensive service support for the hardware / software supplied as per the above referred RFP, during warranty of 3 years and AMC of 3 years.
4. The Warranty and AMC would be back to back from OEM. The warranty of equipment would start from date of acceptance of the solution by the Bank. Further, we would also undertake preventive maintenance periodically as specified in the tender. We also confirm that, we would stock adequate spares of all items supplied at our support locations and provide uptime etc as per requirements of RfP.
5. The price quoted by us includes back to back 3 years warranty and 3 years AMC with OEM and support.
6. We undertake that, in competing for (and, if the award is made to us, in executing) the above contract, we will strictly observe the laws against fraud and corruption in force in India namely “Prevention of Corruption Act 1988”.
7. We have also noted that SIDBI reserves the right to consider/ reject any or all bids without assigning any reason thereof.
8. We understand that the Bank is not bound to accept any proposal it receives.

Yours sincerely,

Date :……. **Name and Signature of Authorized Signatory:……**

Place: …… **Designation: ……** **Phone & Mail id:……**

Name of Organization :…… **Seal:……**

11.2. Annexure –II - Pre-Qualification / Minimum Eligibility Criteria

S.N.	Eligibility Criteria	Bidder's response
1	Name of the bidder company	
2	Year of establishment	
3	Type of Company	
	Documentary proof enclosed. (Yes / No)	
4	***Address of Registered Office with contact numbers***	
a	Address	
b	Land Line No.	
c	Fax No.	
d	Mail Id.	
5	***Address of Local Office at Mumbai with contact numbers [phone /fax/mail]***	
a	Address	
b	Land Line No.	
c	Fax No.	
6	***Address of Local Office at Chennai with contact numbers [phone /fax/mail]***	
a	Address	
b	Land Line No.	
c	Fax No.	
7	**MSME Status (Tick appropriate)**	
a	Company **does not qualify** the status of MSE.	
b	Company **does qualify** the MSE status.	
c	SC/ST	
d	MSE registration certificate or a certificate from Chartered Accountant attached. **(Yes/No)**	
8	PAN No.	
	Copy of PAN enclosed. **(Yes/No)**	
9	Sales Tax / VAT / Service tax registration certificate	
	Copy of Sales Tax / VAT / Service Tax certificate enclosed. **(Yes / No)**	
10	OEM or Authorized Partner of OEMs.	
	MAF from respective OEMs as per format given in **Annexure –V** enclosed. **(Yes /No)**	
11	No of Years of experience in supply, maintenance and support of network and Security solutions in India. At least 5 years as on date of the RfP.	

S.N.	Eligibility Criteria	Bidder's response
	Proof by way of purchase order or work completion order to be attached.	
12	Whether the Bidder has executed at least one order of Rs.100 lakh for supply, installation and support of Network and Security solutions for Data Centre in at least one organization in BFSI sector / PSU / Government Organization in India during last 5 years. (Yes/No)	
	Details of the organizations to be provided, which should include, (Name of organization, Contact Person Name, Designation along with mobile/phone No.)	1. 2.
	Proof by way of purchase order to be attached.	
13	Whether the bidder has OWN support arrangement from the same location at Mumbai and Chennai for extending support. (Yes/No).	
	Details of support location (address, phone no, contact person details) to be provided.	
14	Certificate from OEM on Non-End of Support for a minimum of 6 years (i.e. through the life of entire project period) from 01.06.2016 is attached. **(Yes/No)**	
15	The bidder should not have been black-listed by any Public Financial Institutions, Public Sector Bank, RBI or IBA or any other Government agencies during the last 3 years. Bidder must certify to that effect.	
	Self declaration to this effect on company's letter head signed by company's authorized signatory as per **Annexure-VIII** to be submitted.	
16	Whether, the Bidder has at least one certified engineer at Mumbai on **OEM technology for Network Switches** proposed in response to the RfP. (Yes/No)	
	Details of the engineer (Name, certification details etc) to be submitted.	
17	Whether the bidder have trained and experienced engineers on the proposed firewalls and IPS at Mumbai. (Yes/No).	
	Details of the engineer to be provided.	

S.N.	Eligibility Criteria		Bidder's response
17	**Contact Details of Bidder's authorized representative to make commitments to SIDBI. Power of attorney at per format given in Annexure – to be submitted.**		
a	Name		
b	Designation		
c	Land Line No.		
d	Mobile No.		
e	Fax No.		
f	Mail Id		
18	**Financials**		
	Parameter	**FY**	**Amount in lakh**
a	Annual Turnover	2012 - 2013	
		2013 - 2014	
		2014 - 2015	
b	Cash Profit	2012 - 2013	
		2013 - 2014	
		2014 - 2015	
c	Net worth	2012 - 2013	
		2013 - 2014	
		2014 - 2015	
d	*CA certificate attached. (Yes / No)*		
19	**OEM Details**		
A.	**Network Switches (Data Centre and DR Site)**		
a	Name of OEM		
b	Address of OEM's Office in India		
c	Whether the OEM of proposed network switches for Data Centre and DR Site, supplied and installed the same series/category of switches in at least 3 data centers in BFSI sector / PSU/ Government Organizations in India during last five years. (Yes/No)		
d	Declaration by the OEM on their letter head along with contact details of the customers to be submitted.		
B.	**Perimeter Firewall (Data Centre)**		
a	Name of OEM		
b	Address of OEM's Office in India		
c	Whether the OEM of proposed perimeter firewall feature in the Gartner's Magic Quadrant for Next Generation Firewall under the "leaders" or "challengers" quadrant as per latest Gartner report.		

S.N.	Eligibility Criteria	Bidder's response
d	Gartner Report Attached (Yes/No).	
C.	**Core Firewall (DR Site)**	
a	Name of OEM	
b	Address of OEM's Office in India	
c	Whether the OEM of proposed perimeter firewall feature in the Gartner's Magic Quadrant for Next Generation Firewall under the "leaders" or "challengers" quadrant as per latest Gartner report.	
d	Gartner Report Attached (Yes/No).	
D.	**Intrusion Prevention System (Data Centre)**	
a	Name of OEM	
b	Address of OEM's Office in India	
c	Whether the OEM of proposed Intrusion Prevention System feature in the Gartner's Magic Quadrant for Intrusion Prevention System under the "leaders" or "challengers" quadrant as per latest Gartner report.	
d	Gartner Report Attached (Yes/No).	
20	**EMD Details**	
a	DD / Pay Order / Bank Guarantee	
b	Number	
c	Date of Issue	
d	Issuing Bank	
e	Amount (Rs.)	
21	**Tender Form Cost Details**	
a	DD / Pay Order	
b	Number	
c	Date of Issue	
d	Issuing Bank	
e	Amount (Rs.)	
22	Pre-Contract Integrity Pact as per **Annexure – XI** attached. (Yes/No)	

Date :……. **Name and Signature of Authorized Signatory:……**

Place: …… **Designation: ……** **Phone & Mail id:……**

Name of Organization :…… **Seal:……**

Note

- Bidder response should be complete with all relevant documents attached..
- Documentary proof, sealed and signed by authorized signatory, must be submitted
- Details of clients and relevant contact details are mandatory. Bidders may take necessary approval of the clients in advance before submission of related information. SIDBI will not make any separate request for submission of such information.
- SIDBI will contact the bidder referenced customer for verifications of facts, the bidder to ensure that the customer is intimated. Further in case SIDBI feels to visit the site, the bidder to take necessary approvals for the same. SIDBI will not make any separate request to the bidders customers.
- Proposal of the bidders are liable to be rejected in case of incomplete information or wrong information or non-submission of documentary proof.

11.3. Annexure –III - Technical Bid

The bidder to note that:

- All the switches for Data Centre and DR site should be from same OEM.
- Bidder to ensure not to quote for products already declared or to be declared end of support during the contract period of 6 years.
- Firewalls at DC should not be of Fortigate and Firewall at DR should not be of Checkpoint.

1. Data Centre

1.1. Core Switches

a) **Quantity Required : 2 Numbers**

b) **Minimum Specifications**

S.N.	Minimum Specifications	Vendor Response	Deviations, if any
A.	**Make / Model Details**		
1.	MAKE		
2.	Model No.		
3.	Commercial Launch date of the quoted Model.		
4.	End of Life (EoL) or End of support (EoS) date announced by the OEM. In case such date is not announced, mention the number of years for which as a practice, OEM is supporting such hardware		
B.	**Architecture**		
5.	19” Rack mountable.		
6.	Maximum of 2RU size.		
7.	Must have Redundancy Power Supply Units (PSUs), Hot-swappable, field-replaceable power supplies, 1:1 power redundancy.		
8.	Must have N:1 fan module redundancy.		
9.	All components (including elements such as I/O cards, Expansion Module, power supplies and fans) must be hot swappable with zero disruption to traffic forwarding (Unicast or multicast).		
10.	Port Throughput of 1.92 Tbps		
11.	Latency of 1 to 2 microseconds		
C.	**Interface Supports**		
12.	Must support Standard SFPs including QSFP, SFP+, 1000BASE-T SFP, Gigabit Ethernet SFP.		
13.	Must support minimum 48 x 1/10 G SFP+ and 12 X 40G QSFP ports from day 1.		
14.	The switch should be populated from day one with:		

S.N.	Minimum Specifications	Vendor Response	Deviations, if any
	• 8X40G QSFP Multimode transceiver modules. • 2X10G of 10G Fiber Multimode transceiver modules and • 4 X 1G UTP transceiver modules.		
15.	Must have provision to install 4 x 100G ports to support Inter-Switch backbone links or uplinks by changing or adding an additional module.		
D.	**Switching Features**		
16.	Physical standards for Network Device		
17.	Must support Fast Ethernet (IEEE 802.3u, 100BASE-TX)		
18.	Must support Gigabit Ethernet (IEEE 802.3z, 802.3ab)		
19.	Must support Ten Gigabit Ethernet (IEEE 802.3ae)		
20.	Software based standards for Network Device		
21.	Must support IEEE 802.1d - Spanning-Tree Protocol		
22.	Must support IEEE 802.1w - Rapid Spanning Tree		
23.	Must support IEEE 802.1s - Multiple Spanning Tree Protocol		
24.	Must support IEEE 802.1q - VLAN encapsulation		
25.	Must support IEEE 802.3ad - Link Aggregation Control Protocol (LACP)		
26.	Must support IEEE 802.1ab - Link Layer Discovery Protocol (LLDP)		
27.	Must support IEEE 802.3x Flow Control		
28.	Must support auto-sensing and auto-negotiation (Link Speed/Duplex)		
29.	Routing protocol support when upgraded with Layer3 License		
30.	Must support Static IP routing		
31.	Must support Open Shortest Path First (OSPF) v2 (RFC 2328)		
32.	Must support Protocol Independent Multicast Version 2 (PIMv2) sparse mode, Source Specific Multicast (SSM), Multicast Source Discovery Protocol (MSDP), and Internet Group Management Protocol Versions 2, and 3 (IGMP v2, and v3)		
33.	Must support Border Gateway Protocol - BGPv4 (RFC 1771)		
34.	Must have Routed ports on platform interfaces, switch virtual interface (SVI), PortChannels, subinterfaces, and		

S.N.	Minimum Specifications	Vendor Response	Deviations, if any
	PortChannel subinterfaces for a total of 4096 entries		
35.	Support for up to 32000 multicast ipv4 routes and 8000 multicast ipv6 routers		
36.	Support for 1000 VRF entries		
37.	Virtual Route Forwarding (VRF): VRF-lite (IP VPN); VRF-aware unicast; and BGP-, OSPF- and VRF-aware multicast		
38.	Must support 64-way equal-cost multipathing (ECMP)		
39.	Must support In-Service Software Upgrade (ISSU) for Layer 2		
40.	Must have Layer 2 IEEE 802.1p		
41.	Must have 4 hardware queues per port with per port QoS configuration		
42.	Must have Modular QoS classification compliance		
43.	Must have per port virtual output queuing or Egress Queuing		
44.	Must have ether channel support allowing upto 32 ports per EtherChannel		
45.	Must support Jumbo Frame Size (9k)		
46.	IEEE 802.3ad Link Aggregation or equivalent capabilities		
47.	Must provide for at least 32 physical ports grouped together into a single logical link		
48.	Must be able to load balance across a logical bundle using the following algorithms:		
a.	*Source IP*		
b.	*Destination IP*		
c.	*Source and Destination IP*		
d.	*Source MAC*		
e.	*Destination MAC*		
f.	*Source and Destination MAC*		
g.	*TCP Port (destination and/or source)*		
h.	*UDP Port (destination and/or source)*		
49.	Switch must support VXLAN (Bridging and Routing) as well as NVGRE overlay encapsulation protocol in hardware to support multiple hypervisor deployment in the Data Center		
E.	**Qos Features**		
50.	Must support IEEE 802.1p class-of-service (CoS) prioritization		
51.	Must have 4 Hardware queues per port		
52.	Must have Per-Port QoS configuration		
53.	Must have CoS Trust		
54.	Must have CoS-based egress queuing		
55.	Must have Egress strict-priority queuing		
56.	Must have Modular QoS classification		

S.N.	Minimum Specifications	Vendor Response	Deviations, if any
	compliance		
57.	Must have per port virtual output queuing or Egress Queuing		
58.	Must support Egress port-based scheduling: Weighted Round-Robin (WRR)		
59.	Must have ACL-based QoS classification (Layers 2, 3, and 4)		
F.	**Management Features**		
60.	Must provide management using 10/100/1000-Mbps management or console ports		
61.	Must have CLI-based console to provide detailed out-of-band management		
62.	Must have In-band switch management		
63.	Must have Configuration synchronization & Configuration rollback		
64.	Must support Secure Shell Version 2 (SSHv2), Telnet & SNMPv1, v2, and v3		
65.	Must support AAA, AAA with RBAC or equivalent, Radius, TACACS+ for user authentication		
66.	Must support RMON		
67.	Must support XML		
68.	Must have Advanced Encryption Standard (AES) for management traffic		
69.	Must support Unified username and passwords across CLI and SNMP		
70.	Must support Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)		
71.	Must have Digital certificates for management between switch and RADIUS server		
72.	Must have Switched Port Analyzer (SPAN) or Port mirroring on physical, PortChannel, VLAN		
G.	**Troubleshooting capabilities**		
73.	Must provide Comprehensive bootup diagnostic tests		
74.	Must have Ingress and egress packet counters per interface		
75.	Must support SPAN /Port Mirroring on physical, PortChannel or equivalent, VLAN		
76.	Must have call home / Smart Call Home or equivalent feature		
77.	Must have Embedded packet analyzer or equivalent		
78.	Version of software for supplied switch should be latest release		
79.	Must be EAL2 certified		

S.N.	Minimum Specifications	Vendor Response	Deviations, if any
H.	**Documents**		
80.	Data Sheets attached.		

1.2. Top of Rack (TOR) Switches

a) **Quantity Required : 6 Nos**

b) **Minimum Specifications**

S.N.	Feature Description	Vendor Response	Deviations, If any
A.	**Make / Model Details**		
1.	**Make**		
2.	**Model No.**		
3.	Commercial Launch date of the quoted Model.		
4.	End of Life (EoL) or End of support (EoS) date announced by the OEM. In case such date is not announced, mention the number of years for which as a practice, OEM is supporting such hardware		
B.	**Architecture**		
5.	19" Rack mountable .		
6.	Maximum of 2RU size.		
7.	Must have Redundancy Power Supply Units (PSUs), Hot-swappable, field-replaceable power supplies, 1:1 power redundancy.		
8.	Must have N:1 fan module redundancy.		
9.	All components (including elements such as I/O cards, Expansion Module, power supplies and fans) must be hot swappable with zero disruption to traffic forwarding (Unicast or multicast).		
10.	Port Throughput of 1.44 Tbps scalable to 1.92 Tbps		
11.	Latency of 1 to 2 microseconds		
C.	**Interface Supports**		
12.	Must support QSFP+, 1000BASE-T and 10 G - T		
13.	Must have minimum 48 x 1/10 G - T and 6 X 40 G QSFP+ ports from day1.		
14.	Switch must be loaded from day one with minimum 4 nos. QSFP Multimode transceiver modules and 48 x 1/10G-T.		
15.	Must have provision to install 12 x 40G QSFP ports or 4 x 100G ports to support Inter-Switch backbone links or uplinks by changing or adding an additional module.		
D.	**Switching Features**		
16.	Physical standards for Network Device		
17.	Must support Fast Ethernet (IEEE 802.3u,		

S.N.	Feature Description	Vendor Response	Deviations, If any
	100BASE-TX)		
18.	Must support Gigabit Ethernet (IEEE 802.3z, 802.3ab)		
19.	Must support Ten Gigabit Ethernet (IEEE 802.3ae)		
20.	Software based standards for Network Device		
21.	Must support IEEE 802.1d - Spanning-Tree Protocol		
22.	Must support IEEE 802.1w - Rapid Spanning Tree		
23.	Must support IEEE 802.1s - Multiple Spanning Tree Protocol		
24.	Must support IEEE 802.1q - VLAN encapsulation		
25.	Must support IEEE 802.3ad - Link Aggregation Control Protocol (LACP)		
26.	Must support IEEE 802.1ab - Link Layer Discovery Protocol (LLDP)		
27.	Must support IEEE 802.3x Flow Control		
28.	Must support auto-sensing and auto-negotiation (Link Speed/Duplex)		
29.	Routing protocol support when upgraded with Layer3 License		
30.	Support for Static IP routing		
31.	Support Open Shortest Path First (OSPF) v2 (RFC 2328)		
32.	Must support Protocol Independent Multicast Version 2 (PIMv2) sparse mode, Source Specific Multicast (SSM), Multicast Source Discovery Protocol (MSDP), and Internet Group Management Protocol Versions 2, and 3 (IGMP v2, and v3)		
33.	Support Border Gateway Protocol - BGPv4 (RFC 1771)		
34.	Must have Routed ports on platform interfaces, switch virtual interface (SVI), PortChannels, subinterfaces, and PortChannel subinterfaces for a total of 4096 entries		
35.	Support for up to 32000 multicast ipv4 routes and 8000 multicast ipv6 routers		
36.	Support for 1000 VRF entries		
37.	Support Virtual Route Forwarding (VRF): VRF-lite (IP VPN); VRF-aware unicast; and BGP-, OSPF- and VRF-aware multicast		
38.	Must support 64-way equal-cost multipathing (ECMP)		
39.	Must support In-Service Software Upgrade (ISSU) for Layer 2		

S.N.	Feature Description	Vendor Response	Deviations, If any
40.	Must have Layer 2 IEEE 802.1p		
41.	Must have 4 hardware queues per port with per port QoS configuration		
42.	Must have Modular QoS classification compliance		
43.	Must have per port virtual output queuing or Egress Queuing		
44.	Must have ether channel support allowing upto 32 ports per EtherChannel		
45.	Must support Jumbo Frame Size (9k)		
46.	IEEE 802.3ad Link Aggregation or equivalent capabilities		
47.	Must provide for at least 32 physical ports grouped together into a single logical link		
48.	Must be able to load balance across a logical bundle using the following algorithms:		
a.	*Source IP*		
b.	*Destination IP*		
c.	*Source and Destination IP*		
d.	*Source MAC*		
e.	*Destination MAC*		
f.	*Source and Destination MAC*		
g.	*TCP Port (destination and/or source)*		
h.	*UDP Port (destination and/or source)*		
49.	Switch must support VXLAN (Bridging and Routing) as well as NVGRE orverlay encapsulation protocol in hardware to support multiple hypervisor deployment in the Data Center		
E.	**QoS Features**		
50.	Must support IEEE 802.1p class-of-service (CoS) prioritization		
51.	Must have 4 Hardware queues per port		
52.	Must have Per-Port QoS configuration		
53.	Must have CoS Trust		
54.	Must have CoS-based egress queuing		
55.	Must have Egress strict-priority queuing		
56.	Must have Modular QoS classification compliance		
57.	Must have per port virtual output queuing or Egress Queuing		
58.	Must support Egress port-based scheduling: Weighted Round-Robin (WRR)		
59.	Must have ACL-based QoS classification (Layers 2, 3, and 4)		
F.	**Management Features**		
60.	Must provide management using 10/100/1000-Mbps management or console ports		
61.	Must have CLI-based console to provide		

S.N.	Feature Description	Vendor Response	Deviations, If any
	detailed out-of-band management		
62.	Must have In-band switch management		
63.	Must have Configuration synchronization & Configuration rollback		
64.	Must support Secure Shell Version 2 (SSHv2), Telnet & SNMPv1, v2, and v3		
65.	Must support AAA, AAA with RBAC or equivalent, Radius, TACACS+ for user authentication		
66.	Must support RMON		
67.	Must support XML		
68.	Must have Advanced Encryption Standard (AES) for management traffic		
69.	Must support Unified username and passwords across CLI and SNMP		
70.	Must support Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)		
71.	Must have Digital certificates for management between switch and RADIUS server		
72.	Must have Switched Port Analyzer (SPAN) or Port mirroring on physical, PortChannel, VLAN		
G.	**Troubleshooting capabilities**		
73.	Must provide Comprehensive bootup diagnostic tests		
74.	Must have Ingress and egress packet counters per interface		
75.	Must support SPAN /Port Mirroring on physical, PortChannel or equivalent, VLAN		
76.	Must have call home / Smart Call Home or equivalent feature		
77.	Must have Embedded packet analyzer or equivalent		
78.	Version of software for supplied switch should be latest release		
79.	Must be EAL2 certified		
H.	**Documents**		
80.	Data Sheets to be attached.		

1.3. DMZ Switch

a) **Quantity Required : 2Nos**

b) **Minimum Specifications:**

S.N	Feature Description	Vendor Response	Deviations, if any
A.	**Make / Model Details**		
1.	**Make**		
2.	**Model No.**		
3.	Commercial Launch date of the quoted Model.		
4.	End of Life (EoL) or End of support (EoS) date announced by the OEM. In case such date is not announced, mention the number of years for which as a practice, OEM is supporting such hardware		
B.	**Architecture**		
5.	19" Rack mountable .		
6.	Maximum of 2RU size.		
7.	Must have Redundancy Power Supply Units (PSUs), Hot-swappable, field-replaceable power supplies, 1:1 power redundancy.		
8.	Must have N:1 fan module redundancy.		
9.	All components (including elements such as I/O cards, Expansion Module, power supplies and fans) must be hot swappable with zero disruption to traffic forwarding (Unicast or multicast).		
10.	Port Throughput of 1.44 Tbps scalable to 1.92 Tbps		
11.	Latency of 1 to 2 microseconds		
C.	**Interface Supports**		
12.	Must support QSFP+, 1000BASE-T and 10 G - T		
13.	Must have minimum 48 x 1/10 G - T and 6 X 40 G QSFP+ ports from day1.		
14.	The switch must be populated from day 1 with 48 x 1/10G-T and 4 X 40G QSFP ports.		
15.	The switch must be scaleable to 12 x 40G QSFP ports or 4 x 100G ports by changing or adding an additional module. 100G must be supported on the switch from day 1.		
D.	**Switching Features**		
16.	Physical standards for Network Device		
17.	Must support Fast Ethernet (IEEE 802.3u, 100BASE-TX)		
18.	Must support Gigabit Ethernet (IEEE 802.3z, 802.3ab)		
19.	Must support Ten Gigabit Ethernet (IEEE 802.3ae)		
20.	Software based standards for Network		

S.N	Feature Description	Vendor Response	Deviations, if any
	Device		
21.	Must support IEEE 802.1d - Spanning-Tree Protocol		
22.	Must support IEEE 802.1w - Rapid Spanning Tree		
23.	Must support IEEE 802.1s - Multiple Spanning Tree Protocol		
24.	Must support IEEE 802.1q - VLAN encapsulation		
25.	Must support IEEE 802.3ad - Link Aggregation Control Protocol (LACP)		
26.	Must support IEEE 802.1ab - Link Layer Discovery Protocol (LLDP)		
27.	Must support IEEE 802.3x Flow Control		
28.	Must support auto-sensing and auto-negotiation (Link Speed/Duplex)		
29.	Routing protocol support when upgraded with Layer3 License		
30.	Must support Static IP routing		
31.	Must support Open Shortest Path First (OSPF) v2 (RFC 2328)		
32.	Must support Protocol Independent Multicast Version 2 (PIMv2) sparse mode, Source Specific Multicast (SSM), Multicast Source Discovery Protocol (MSDP), and Internet Group Management Protocol Versions 2, and 3 (IGMP v2, and v3)		
33.	Must support Border Gateway Protocol - BGPv4 (RFC 1771)		
34.	Must have Routed ports on platform interfaces, switch virtual interface (SVI), PortChannels, subinterfaces, and PortChannel subinterfaces for a total of 4096 entries		
35.	Support for up to 32000 multicast ipv4 routes and 8000 multicast ipv6 routers		
36.	Support for 1000 VRF entries		
37.	Virtual Route Forwarding (VRF): VRF-lite (IP VPN); VRF-aware unicast; and BGP-, OSPF- and VRF-aware multicast		
38.	Must support 64-way equal-cost multipathing (ECMP)		
39.	Must support In-Service Software Upgrade (ISSU) for Layer 2		
40.	Must have Layer 2 IEEE 802.1p		
41.	Must have 4 hardware queues per port with per port QoS configuration		
42.	Must have Modular QoS classification compliance		
43.	Must have per port virtual output queuing or		

S.N	Feature Description	Vendor Response	Deviations, if any
	Egress Queuing		
44.	Must have ether channel support allowing upto 32 ports per EtherChannel		
45.	Must support Jumbo Frame Size (9k)		
46.	IEEE 802.3ad Link Aggregation or equivalent capabilities		
47.	Must provide for at least 32 physical ports grouped together into a single logical link		
48.	Must be able to load balance across a logical bundle using the following algorithms:		
a.	*Source IP*		
b.	*Destination IP*		
c.	*Source and Destination IP*		
d.	*Source MAC*		
e.	*Destination MAC*		
f.	*Source and Destination MAC*		
g.	*TCP Port (destination and/or source)*		
h.	*UDP Port (destination and/or source)*		
49.	Switch must support VXLAN (Bridging and Routing) as well as NVGRE orverlay encapsulation protocol in hardware to support multiple hypervisor deployment in the Data Center		
E.	**QoS Features**		
50.	Must support IEEE 802.1p class-of-service (CoS) prioritization		
51.	Must have 4 Hardware queues per port		
52.	Must have Per-Port QoS configuration		
53.	Must have CoS Trust		
54.	Must have CoS-based egress queuing		
55.	Must have Egress strict-priority queuing		
56.	Must have Modular QoS classification compliance		
57.	Must have per port virtual output queuing or Egress Queuing		
58.	Must support Egress port-based scheduling: Weighted Round-Robin (WRR)		
59.	Must have ACL-based QoS classification (Layers 2, 3, and 4)		
F.	**Management Features**		
60.	Must provide management using 10/100/1000-Mbps management or console ports		
61.	Must have CLI-based console to provide detailed out-of-band management		
62.	Must have In-band switch management		
63.	Must have Configuration synchronization & Configuration rollback		
64.	Must support Secure Shell Version 2 (SSHv2), Telnet & SNMPv1, v2, and v3		

S.N	Feature Description	Vendor Response	Deviations, if any
65.	Must support AAA, AAA with RBAC or equivalent, Radius, TACACS+ for user authentication		
66.	Must support RMON		
67.	Must support XML		
68.	Must have Advanced Encryption Standard (AES) for management traffic		
69.	Must support Unified username and passwords across CLI and SNMP		
70.	Must support Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)		
71.	Must have Digital certificates for management between switch and RADIUS server		
72.	Must have Switched Port Analyzer (SPAN) or Port mirroring on physical, PortChannel, VLAN		
G.	**Troubleshooting capabilities**		
73.	Must provide Comprehensive bootup diagnostic tests		
74.	Must have Ingress and egress packet counters per interface		
75.	Must support SPAN /Port Mirroring on physical, PortChannel or equivalent, VLAN		
76.	Must have call home / Smart Call Home or equivalent feature		
77.	Must have Embedded packet analyzer or equivalent		
78.	Version of software for supplied switch should be latest release		
79.	Must be EAL2 certified		
H.	**Documents**		
80.	Data sheets to be attached.		

1.4. Stackable Switches

a) **Quantity Required: 4Nos (2 each in a stack with stacking cables)**

b) **Minimum Specifications**

S.N.	Feature Description	Vendor Response	Deviations, if any
A.	**Make / Model Details**		
1.	**Make**		
2.	**Model No.**		
3.	Commercial Launch date of the quoted Model.		
4.	End of Life (EoL) or End of support (EoS) date announced by the OEM. In case such date is not announced, mention the number		

S.N.	Feature Description	Vendor Response	Deviations, if any
	of years for which as a practice, OEM is supporting such hardware		
B.	**Switch Hardware features**		
5.	Switch should have minimum 24 10/100/1000 Base-T ports. with additional 4 Nos. of 1G SFP Based ports for uplink connectivity and 2 stacking ports with all accessories for stacking purpose from day1		
6.	Switch should be 1 RU rack mountable in nature, stackable with dedicated 80Gbps of throughput with minimum of 4 switches in a stack with single IP management.		
7.	Switch should support IEEE Standards of Ethernet: IEEE 802.1d, 802.1s, 802.1w, 802.3ad, 802.3x, 802.1D, 802.1p, 802.1Q, 802.3, 802.3u, 802.3ab, 802.3z, 100Base-T, 1000BASE-T, 1000BASE-X (mini-GBIC/SFP), 1000BASE-SX, 1000BASE-LX/LH, IEEE 802.3ae 10Gigabit Ethernet and IEEE 802.3ah (100BASE-X single/multimode fiber only)		
8.	Switch should support Auto MDI/MDIX		
9.	All SFP modules should be hot swappable		
10.	Switch should have minimum 120 Gbps switching bandwidth capacity (Gbps) per switch		
	Switch should have minimum 70 Mpps throughput per switch		
C.	**Layer-2 Requirements**		
11.	Switch should support minimum 15000 MAC address per switch		
12.	The switch should have IPV4 & IPv6 support from day one		
13.	It should support Jumbo packets up to 9,216-byte frame size to improve performance of large data transfers.		
14.	Should support IEEE 802.1Q VLAN encapsulation and up to 1000 active VLANs per switch		
15.	Switch should support Voice VLAN for easier administration and troubleshooting		
16.	Switch should support cross-stack etherchannel using LACP and no performance impact for voice traffic during stack convergence		
17.	Switch should be having Zero Turn-Around Time to configure policies based on device-types.		
18.	It should support IEEE 802.3ad Link Aggregation Control Protocol (LACP) with up		

S.N.	Feature Description	Vendor Response	Deviations, if any
	to 8 links (ports) per trunk.		
19.	Switch should support link aggregation for minimum 6 GE ports and minimum 24 LAG groups.		
20.	Should be able to discover the neighboring device of the same vendor giving the details about the platform, IP Address, Link connected through etc, thus helping in troubleshooting connectivity problems		
21.	Should support a mechanism to detect connectivity issues with both fiber and copper cabling. Ensures that a partially failed link is shut down on both sides, to avoid L2/L3 protocol convergence issues		
22.	The Switch should support IGMP V1,V2,V3 and MLD V1 and V2		
23.	Switch should support auto-recovery of error-disabled ports due to network errors.		
24.	The Switch Should support auto detection and plug and play of the device onto the network with configuration as per the template.		
25.	It should support IEEE 802.1s Multiple Spanning Tree Protocol and provide legacy support for IEEE 802.1d STP and IEEE 802.1w RSTP		
26.	The switch should support feature which shuts down Spanning Tree PortFast-enabled interfaces when BPDUs are received to avoid accidental topology loop		
27.	The switch should support feature which provides multicast authentication by filtering out non-subscribers and limits the number of concurrent multicast streams available per port (Optional)		
28.	It should support IEEE 802.1AB Link Layer Discovery Protocol (LLDP)		
29.	Should support Port Mirroring based on acl, port basis / vlan basis to support intrusion prevention system deployment in different VLANs. Should support port mirroring across the stack switches to remotely monitor ports in a Layer 2 switch network from any other switch in the same network.		
30.	Switch should provide minimum 2 or more mirror sessions		
D.	**Security Requirements**		
31.	It should support protected ports to isolate specified ports from all other ports on the switch.		

S.N.	Feature Description	Vendor Response	Deviations, if any
32.	Switch Should support VLAN Based and Port Based ACLs		
33.	It should support IEEE 802.1X user authentication using an IEEE 802.1X supplicant in conjunction with a RADIUS server.		
34.	switch should provide 802.1x support for VLAN assignment, Guest VLAN, MAC-Auth-Bypass and ACL support		
35.	It should support MAC-based authentication allowing client to be authenticated with the RADIUS server based on client‟s MAC address.		
36.	It should support TACACS+ or RADIUS authentication for secure switch CLI logon.		
37.	It should support management access (CLI, Web, MIB) securely encrypted through SSHv2, SSL, and SNMPv3.		
38.	Per-port storm control for preventing broadcast, multicast, and unicast storms		
39.	The switch should support monitoring, capturing, and recording of flows to provide network traffic statistics for further analysis, accounting, network monitoring and network planning. Flows need to be captured from physical ethernet port or from vlan interface.		
40.	The switch should support feature to prevent malicious attacks on the switch by not relaying invalid ARP requests and responses to other ports in the same VLAN.		
41.	The switch should provide Bidirectional data support on the mirror port to allow Intrusion Detection to take action when an intruder is detected. (Optional)		
E.	**Qos Requirements**		
42.	It should support IEEE 802.1p traffic prioritization delivering data to devices based on the priority and type of traffic.		
43.	should have strict priority queuing or high strict priority queue		
44.	Switch should support 802.1p based CoS and differentiated services code point (DSCP) based field classification, marking and reclassification on a per-packet basis for L2,L3,L4 information.		
F.	**Management Requirements**		
45.	It should support SNMPv1/v2c/v3.		
46.	It should support RMON providing advanced monitoring and reporting capabilities for statistics, history, alarms, and events.		

S.N.	Feature Description	Vendor Response	Deviations, if any
47.	Switch should support following IPv6 features and functions :- • IPv6 Host support (IPv6 support: Addressing; IPv6: ICMPv6, TCP/UDP over IPv6; Applications: Ping/Traceroute/VTY/SSH/TFTP, SNMP for IPv6 objects) HTTP and HTTP(s) over IPv6, Syslog over IPv6) • IPv6 management • IPv6 MLD v1 and v2 snooping		
48.	The Switch Should support single point of management enabling (zero-touch deployment) plug-and-play configuration, archiving of configurations and image-management for switches		
49.	Switch should support NTP		
G.	**Troubleshooting Requirements**		
50.	Switch should support Layer 2 traceroute to identify the physical path that a packet takes from source to destination		
51.	Switch should support feature which enabled devices to perform proactive diagnostics on their own components to provide real-time alerts and remediation advice when an issue is detected and also communicate with support center using email and open support case with support center. (Optional)		
52.	Switch should generate hardware failure information in a log file and need to be stored in flash so that support center can access these files and to identify the root cause.		
H.	**Documents**		
53.	Data Sheets to be attached.		

1.5. Intrusion Prevention System (IPS)

a) **Quantity Required :2Nos in HA**

b) **Minimum Specifications**

S.N.	Description	Vendor Response	Deviations, if any
A.	**Make / Model Details**		
1.	**MAKE**		
2.	**MODEL NO.**		
3.	Commercial Launch date of the quoted Model.		
4.	End of Life (EoL) or End of support (EoS) date announced by the OEM. In case such		

S.N.	Description	Vendor Response	Deviations, if any
	date is not announced, mention the number of years for which as a practice, OEM is supporting such hardware		
5.	The OEM of proposed dedicated IPS should feature in the Gartner's Magic Quadrant under the "leaders" or "challengers" quadrant as per latest Gartner report for Intrusion Prevention System.		
B.	**General Requirements**		
6.	Each Appliance should provide Real World IPS throughput of atleast 1.2 Gbps		
7.	The Solution should support for Active–Active and Active-Passive as High Availability option.		
8.	Each Appliance should be supplied with minimum 4 * 1G Copper Interfaces from Day one.		
9.	Each Appliance should have a flexibility of adding atleast additional 4 No's of either Copper or Fiber Interfaces for scalability without changing the appliance.		
10.	Each Appliance should have a dedicated 1G Management Interface		
11.	The IPS should support for minimum 1.5 million concurrent sessions.		
12.	The IPS Should support for minimum 40,000 New connections per second.		
C.	**IPS Capabilities**		
13.	The proposed solution must be based on standard computer technology (not ASICs) so that future enhancements and protocols do not require hardware refresh to support		
14.	The proposed solution platforms must be based on a hardened operating system.		
15.	The detection engine must be capable of operating in both passive (i.e., monitoring) and inline (i.e., blocking) modes.		
16.	The detection engine should support Layer 2 deployment so that it provides packet switching and inspection between two or more network segments.		
17.	The detection engine should support Layer 3 deployment where it can route and inspect traffic between two or more interfaces.		
18.	Detection rules must be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.		
19.	Detection rules provided by the vendor must be documented, with full descriptions of the		

S.N.	Description	Vendor Response	Deviations, if any
	identity, nature, and severity of the associated vulnerabilities and threats being protected against.		
20.	The detection engine must be capable of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, zero-day threats, etc.).		
21.	The detection engine must be capable of detecting variants of known threats, as well as new threats (i.e., so-called “unknown threats”).		
22.	The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioral anomaly detection techniques. Identify and explain each type of detection mechanism supported.		
23.	The detection engine must inspect not only Network Layer details and information resident in packet headers, but a broad range of protocols across all layers of the computing stack and packet payloads as well.		
24.	The detection engine must be resistant to various URL obfuscation techniques common to HTML-based attacks.		
25.	The solution must incorporate measures to minimize the occurrence of both false positives and false negatives (i.e., mistaken and missed detection events, respectively).		
26.	Solution must be capable of detecting multi-part or extended threats by aggregating and correlating the multiple, disparate events associated with them.		
27.	The detection engine must be capable of inspecting traffic associated with different network segments differently (as opposed to having only one policy per interface).		
28.	Sensors must be capable of performing packet-level forensics and capturing raw packet data in response to individual events without significant performance degradation.		
29.	The detection engine must support multiple options for directly responding to events, such as monitor only, block offending traffic, replace packet payload, and capture		

S.N.	Description	Vendor Response	Deviations, if any
	packets.		
30.	The management platform must be capable of setting thresholds such that multiple instances of specific events are required before an alert is issued.		
31.	The solution must be capable of detecting and blocking IPv6 attacks.		
32.	The solution must provide IP reputation feed that comprised of several regularly updated collections of IP addresses determined by the proposed security vendor to have a poor reputation.		
33.	The solution must support IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist.		
D.	**Real-Time Contextual Awareness**		
34.	The solution must be capable of passively gathering information about network hosts and their activities, such as operating system, services, open ports, client applications, and vulnerabilities, to assist with multiple activities, such as intrusion event data correlation, elimination of false positives, and policy compliance.		
35.	The solution must be capable of passively gathering information about session flows for all monitored hosts, including start/end time, ports, services, and amount of data.		
36.	The solution must be capable of passively detecting pre-defined services, such as FTP, HTTP, POP3, Telnet, etc., as well as custom services.		
37.	The solution must be capable of storing user-defined host attributes, such as host criticality or administrator contact information, to assist with compliance monitoring.		
38.	The solution must be capable of passively gathering user identity information, mapping IP addresses to username, and making this information available for event management purposes.		
39.	The solution must be capable of passively gathering details unique to mobile devices traffic to identify a wide variety of mobile operating systems, mobile applications and associated mobile device hardware.		
40.	The solution must be capable of identifying “Jailbroken” mobile devices, which can help		

S.N.	Description	Vendor Response	Deviations, if any
	to enforce mobile device usage policies on the network.		
41.	The solution must provide a detailed, interactive graphical summary that includes data on applications, application statistics, connections, intrusions events, hosts, servers, users, file-types, malwares and relevant URLs. These data should be presented in the form of vivid line, bar, pie and donut graphs accompanied by detailed lists (Administrator should easily create and apply custom filters to fine-tune the analysis).		
42.	The aforementioned network and user intelligence must be passively gathered using existing IPS devices (no separate hardware required).		
E.	**Application Visibility and Control**		
43.	Should have identification support for atleast 3000 applications and the identification should be regardless of ports. The application needs to be predefined on the box.		
44.	The proposed system shall have the ability to identify, block the following common P2P applications : Gnutella (Napshare, iMesh, Mldonkey, morph, Xolox, BearShare, FOXY), Bittorrent, Kaaza, WinY, edonkey etc).		
45.	Solution should provide granual control of applications.		
46.	The solution must integrate application control to reduce risks associated with applications usage and client-side attacks.		
47.	It should provide a means of enforcing acceptable use policies of up to 3000 application detectors, solution must support creation of user-defined application protocol detectors.		
48.	The solution must have content awareness with comprehensive file detection policies and blocking of files by types, protocols and directions.		
F.	**Intelligent Security Automation**		
49.	The solution must be capable of employing an extensive set of contextual information (e.g., pertaining to the composition, configuration, and behavior of the network and its hosts) to improve the efficiency and accuracy of both manual and automatic		

S.N.	Description	Vendor Response	Deviations, if any
	analysis of detected events.		
50.	The solution must be capable of significantly reducing operator effort and accelerating response to threats by automatically prioritizing alerts, ideally based on the potential for correlated threats to successfully impact the specific hosts they are directed toward.		
51.	The solution must be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.		
52.	The solution must be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports.		
53.	The solution shall give CVE number for the Intrusion events detected and shall capture packet for each intrusion event.		
54.	The device shall allow administrators to create Custom IPS signatures.		
55.	Consists of vendor's original threat intelligence and is not overly dependent on information available in the public domain.		
56.	Device Signature Updating that provides a feature to automatically download the signatures and push the updates on the managed NIPS devices.		
57.	The solution must be capable of defending against IPS-evasion attacks by automatically using the most appropriate defragmentation and stream reassembly routines for all traffic based on the characteristics of each destination host.		
G.	**Control Compliance**		
58.	The solution must integrate application control to reduce risks associated with applications usage and client-side attacks. It should provide a means of enforcing acceptable use policies of up to 1200 application detectors.		
59.	The solution must support creation of user-defined application protocol detectors.		
60.	The solution must have content awareness with comprehensive file detection policies and blocking of files by types, protocols and directions.		
a	- Protocols: HTTP, SMTP, IMAP, POP		
b	- Direction: Upload, Download, Both		
c	- File Types: Office Documents, Archive,		

S.N.	Description	Vendor Response	Deviations, if any
	Multimedia, Executable, PDF, Encoded, Graphics, and System Files.		
61.	The solution must provide capabilities for establishing and enforcing host compliance policies and alerting on violations.		
62.	The solution must be capable of exempting specific hosts from specific compliance rules and suppressing corresponding compliance events and alerts.		
63.	The solution must be capable of easily identifying all hosts that exhibit a specific attribute or non-compliance condition.		
H.	**Network Behavior Analysis (NBA)**		
64.	The solution must provide a full-featured NBA capability to detect threats emerging from inside the network (i.e., ones that have not passed through a perimeter IPS). This includes the ability to establish "normal" traffic baselines through flow analysis techniques (e.g., NetFlow) and the ability to detect deviations from normal baselines.		
65.	The NBA capability must provide visibility into how network bandwidth is consumed to aid in troubleshooting network outages and performance degradations.		
66.	The NBA capability must provide the ability to link Active Directory and/or LDAP usernames to IP addresses related to suspected security events.		
67.	The NBA capability must provide the option of supplying endpoint intelligence to the IPS for correlation against intrusion events to aid in event impact prioritization.		
68.	The same network devices used for IPS must also be used as part of the NBA capability. No NBA-only device should be required.		
69.	The same management platform used for IPS must also be used to manage the NBA capability. No NBA-only management components should be required.		
I.	**Management and Usability**		
70.	The management platform must be capable of centralized, life cycle management for all sensors.		
71.	The management platform must be provided in the form or dedicated physical appliance or virtual appliance.In case of virtual appliance, management system and UI must provide the same features and		

S.N.	Description	Vendor Response	Deviations, if any
	functions as in the physical appliance.		
72.	The management platform must be capable of aggregating IDS/IPS events and centralized, real-time monitoring and forensic analysis of detected events.		
73.	The management platform must be accessible via a web-based interface and ideally with no need for additional client software.		
74.	The management platform must provide a highly customizable dashboard.		
75.	The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows.		
76.	The management platform must be capable of role-based administration, enabling different sets of views and configuration capabilities for different administrators subsequent to their authentication.		
77.	The management platform must include a scheduling subsystem to facilitate automation of routine tasks, such as backups, upgrades, report creation, and policy application.		
78.	The management platform must include one or more default (i.e., pre-defined) detection policy configurations to help simplify initial deployment.		
79.	The management platform must be capable of grouping both sensors and policies to help simplify configuration management.		
80.	The management platform must provide the capability to easily view, enable, disable, and modify individual rules, as well as groups or categories of rules.		
81.	The management platform must be capable of automatically receiving rule updates published by the vendor and automatically distributing and applying those rule updates to sensors.		
82.	The management platform must be capable of backup and rollback for sensor configurations and the management platform itself.		
83.	The management platform must include flexible workflow capabilities for managing the complete life cycle of an event, from initial notification through to any response and resolution activities that might be		

S.N.	Description	Vendor Response	Deviations, if any
	required.		
84.	The management platform must provide the ability to view the corresponding detection rule for each detected event, along with the specific packet(s) that caused it to be triggered.		
85.	The management platform must support both internal and external databases/systems for storage of event data, logs, and other system-generated information.		
86.	The management platform must support both internal and external databases/systems for storage of event data, logs, and other system-generated information.		
87.	The management platform must be capable of logging all administrator activities, both locally and to a remote log server.		
88.	Policy per Device Port, provide a feature to configure different security policies for different device ports.		
89.	The solution must support LDAP for single sign-on to sensors and the management console.		
J.	**Reporting & Alerting**		
90.	The management platform must provide robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.		
91.	The reporting tool needs to be bundled or quoted along with the solution. The logging and analysis should either be an appliance or on a dedicated PC/ Server platform. The bidder should take the responsibility of supplying the hardware and the OS with suitable warranty.		
92.	The management platform must allow quick report customization by importing from dashboards, workflows and statistics summaries.		
93.	The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.		
94.	Sending Notifications, capability to send SNMP or SMTP alert after detection of the attack.		
95.	Packet Capture, provide feature to capture attack packets in the raw format and export		

S.N.	Description	Vendor Response	Deviations, if any
	these captured packets to .cap file so that it can be analyzed in packet analyzer.		
96.	Logging of Administrative Changes that provides a detailed audit trail for administrative activities.		
97.	The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).		
K.	**Reliability and Availability**		
98.	Sensors must support built-in capability of failing open, such that communications traffic is still allowed to pass if the inline sensor goes down.		
99.	The product must support "Lights Out Management" capability where remote upgrade, restore, and downgrade functionality without physical access to the appliance being required.		
100.	The sensor platforms must support a range of models, including modular design on the high-end and standard connectivity options on the low-end. The high-end sensor platforms must be capable of offering additional flexibility through stacking to increase throughput as your inspection needs grow without using external load balancing solutions.		
101.	The management platform must be capable of monitoring the health of all components and issuing alerts for anomalous conditions.		
102.	Intra-system communications must be secure.		
103.	The supplier must have a detailed process for customer submission of product-related faults and the resolution of those faults, including provisions for escalation of critical or unresolved issues.		
L.	**Third-Party Integration**		
104.	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable automatic response to threats by external components and remediation applications, such as routers, firewalls, patch management systems, etc.		
105.	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to enable events and log data to be shared with external network and security		

S.N.	Description	Vendor Response	Deviations, if any
	management applications, such as trouble-ticketing systems, Security Information and Event Managers (SIEMs), systems management platforms, and log management tools.		
106.	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to receive information from external sources, such as configuration management databases, vulnerability management tools, and patch management systems, for threat correlation and IT policy compliance purposes.		
107.	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to export SNMP information to network management systems.		
108.	The management platform must include an integration mechanism, preferably in the form of open APIs and/or standard interfaces, to obtain network intelligence (i.e., NetFlow) from Cisco routers and switches.		
M.	**Virtual Protection**		
109.	The proposed vendor must have the technology option to offer IDS/IPS solution for virtual infrastructure along with a virtual management console. It should provide the capability to inspect VM-to-VM communications, providing full IDS/IPS capabilities to protect virtual networks.		
110.	The "Virtual Sensor" must be deployed within the virtual environments (i.e. deployed in the physical hosts containing VMs) to monitors traffic between virtual networks and/or virtual machines. It must not involve any third party joint solution that required redirection of traffic externally for inspection.		
	The "Virtual Sensor" and "Virtual Centralized Management System" must be in virtual appliance format and must minimally support VMware ESX/ESXi 4.1/5.0 platform.		
111.	The Virtualization solution must be able to integrate with VMware vShield to dynamically restricts any policy-violating activity within virtual environments		
112.	The “Virtual Centralized Management System” should function with all the features		

S.N.	Description	Vendor Response	Deviations, if any
	same as that of an appliance form factor.		
N.	**Advance Threat Protection**		
113.	Solution should be capable of detecting & blocking callbacks to CnC Servers.		
114.	Shall also have the capability to detect, monitor, prevent and block Advanced Targeted Attacks.		
115.	Solution should be capable of blocking threats based on both signatures and behaviour.		
116.	The Sandbox should be a propreitary custom built malware analysis solution and not open source or generic sandbox.		
117.	The Solution should be capable of employing an extensive set of contextual information (e.g., pertaining to the composition, configuration, and behavior of the network and its hosts) to improve the efficiency and accuracy of both manual and automatic analysis of detected events.		
118.	The solution should be capable of inspecting MS Office Documents, Portable Documents, Archive Files, Multimedia Files and executable binaries.		
119.	The solution shall have the ability to trace & graphically represent the file path & IP Addresses of all users that downloaded a particular file from Internet		
120.	The solution shall have the ability to point out applications that introduce the most amount of malware into network.		
121.	The solution shall have the capability to report on the most used file types and file types that are associated with most infections in the network.		
122.	The solution should be capable of exempting specific hosts from specific compliance rules and suppressing corresponding compliance events and alerts.		
123.	The solution should be capable of whitelisting trusted applications from being inspected to avoid business applications from being affected & in turn productivity		
124.	The Solution should provide visibility into how network bandwidth is consumed to aid in troubleshooting network outages and detecting Advanced Malware related DoS & DDoS activity from within the network.		
O.	**Documents**		
125.	Data Sheets attached.		

1.6. Firewall

a) **Quantity Required :2 nos in HA**

b) **Minimum Specifications**

S.N.	Description	Compliance	Deviations, if any
A.	**Make / Model Details**		
1.	**MAKE**		
2.	**MODEL No:**		
3.	Commercial Launch date of the quoted Model.		
4.	End of Life (EoL) or End of support (EoS) date announced by the OEM. In case such date is not announced, mention the number of years for which as a practice, OEM is supporting such hardware		
5.	The OEM of proposed firewalls should feature in the Gartner's Magic Quadrant under the "leaders" or "challengers" quadrant as per latest Gartner report for Next Generation Firewall.		
B.	**General Requirements**		
6.	The solution should have a separate or inbuilt management & Reporting solution. In case of separate management & Reporting solution the same should be on separate appliance and needs to be integrated with firewall.		
7.	The firewall appliance should support Application control functionalities.		
8.	The firewall appliance should support Secure Remote access to corporate application over the internet.		
9.	The firewall appliance should support for Active–Active and Active-Passive as High Availability option.		
10.	In case of Active/Active the Appliance should support Load Balancing.		
11.	The Licensing for all the components forming the solution should be a per device and not user/IP based (i.e. should support unlimited users)		
12.	The firewall appliance should support IPv4 and IPv6 from day one.		
13.	The appliance should support VOIP traffic filtering.		
14.	The Firewall appliance Architecture should be on multiple core/tire CPU or ASIC based.		
15.	The communication between Firewall System and management & reporting solution should		

S.N.	Description	Compliance	Deviations, if any
	be encrypted with SSL or PKI.		
16.	The Firewall system should have a provision to handle the bandwidth management. It should offer the Bandwidth Management for every TCP, IPSEC, & VoIP protocols with attributes of Minimum Committed Bandwidth per protocol; Maximum Bandwidth per protocol; Priority for the queues etc.		
17.	The Firewall system should support the IPSec VPN for both Site-Site & Remote Access VPN.		
18.	The Firewall system should support virtual tunnel interfaces to provision Route-Based IPSec VPN.		
19.	The firewall system should have at least 500GB local hard-disk or should be provided through external Firewall Management for storing logs.		
20.	The Firewall & Integrated IPSEC VPN Applications should be ICSA Labs certified for ICSA 4.0, FIPS 140-2 certified.		
B.	**Hardware and Interface Requirements**		
21.	The firewall appliance must be supplied with at least 8 numbers of 10/100/1000 Mbps interfaces on Copper from day one.		
22.	The firewall appliance should support at least 6 numbers of 10GBase-F SFP+ Ports for future up-gradation without changing the appliance.		
23.	The appliance should support atleast one 10/100/1000 dedicated management interfaces to configure/manage the firewall policies, perform image upgrades even in case of failure of the data interfaces. Data ports should not be used for management purpose		
24.	The firewall appliance should have Console port and USB Port.		
25.	The firewall appliance should support VLAN tagging (IEEE 802.1q)		
26.	The firewall appliance should support Link Aggregation functionality to group multiple ports as single port.		
27.	The firewall appliance should support Ethernet Bonding functionality for Full Mesh deployment architecture.		
28.	The Firewall should support CA functionality.		
C.	**Performance Requirements**		
29.	Firewall performance (Large packets) Should be 4 Gbps and above		
30.	Firewall should provide atleast 2 Gbps of Multi-protocol/IMIX real-world throughput based on protocols like HTTP, SMTP, FTP, IMAP , DNS		

S.N.	Description	Compliance	Deviations, if any
	(Only UDP based performance nos. will not be considered)		
31.	Firewall should support minimum 1,000,000 concurrent connections.		
32.	Firewall should support minimum 50,000 new connections per second (cps).		
33.	The appliance should be supplied with redundant inbuilt power supplies from day one.		
34.	Firewall should support 3Des/AES IPSec VPN throughput of atleast 1 Gbps		
35.	Firewall should support atleast 5000 concurrent SSL vpn peers		
36.	Firewall should support atleast 1024 vlans.		
37.	Firewall should support Jumbo Frames upto 9216 bytes.		
D.	**General Firewall Features**		
38.	Firewall should support IPv4 & IPv6 dual stack functionality to be able to use IPv4 & IPv6 simultaneously		
39.	Firewall should support creating access-rules with IPv4 & IPv6 objects simultaneously eg: Ipv4 source & Ipv6 destination		
40.	Firewall should support operating in routed & transparent mode.		
41.	In transparent mode firewall should support arp-inspection to prevent spoofing at Layer-2.		
42.	Firewall should support passing of BPDU's & filtering of non-ip traffic with ether-type acls.		
43.	Firewall should provide application inspection for DNS, FTP, HTTP. SMTP,ESMTP, LDAP, MGCP, RTSP, SIP, SCCP, SQLNET, TFTP, H.323, SNMP.		
44.	Firewall should provide IPv6 application inspection for DNS, FTP, HTTP, SIP, SMTP & IPv6.		
45.	Application inspection engine for DNS should support matching specific flag in the DNS header, DNS type including Query & RR type, DNS class, DNS Question, resource-record, Authority RR, DNS message domain name list, & setting actions like drop all packets, drop connection, send-protocol-error, reset the connection & send logs.		
46.	Firewall should support Single Sign On (SSO).		
47.	Should support translating between IPv4 and IPv6 for the following inspections: ➢ DNS ➢ FTP ➢ HTTP ➢ ICMP		

S.N.	Description	Compliance	Deviations, if any
48.	Network address translation (NAT) shall be supported so that the private IP addresses of hosts and the structure of an internal network can be concealed by the firewall.		
49.	Network Address Translation (NAT) shall be configurable as 1:1, 1: many, many: 1, many: many, flexible NAT (overlapping IPs). Reverse NAT shall be supported.		
50.	Dynamic Host Configuration Protocol (DHCP) over Virtual Private Network (VPN) shall be supported for dynamic allocation of IP addresses.		
51.	Point-to-Point Protocol over Ethernet (PPPoE) shall be supported.		
52.	The firewall shall mask the internal network from the external world.		
53.	The firewall shall provide robust access control capability and be fast in making access control decisions. Access Control shall be done based on criteria such as source, destination IPs, port number, protocol, traffic type, application, date information (day of week, time of day), etc.		
54.	Multi-layer, stateful, application-based filtering shall be done.		
55.	It shall provide network segmentation features with powerful capabilities that facilitate deploying security for various internal, external and DMZ (Demilitarized Zone) sub-groups on the network, to prevent unauthorized access.		
56.	There shall be support for detection of reconnaissance attempts such as IP address sweep, port scanning etc.		
57.	Firewall itself shall be resistant to attack and shall have protection against firewall evasion techniques.		
58.	Some basic attack protection features listed below but not limited to :		
a	Maximum no of protections against attacks that exploit weaknesses in the TCP/IP protocol suite		
b	It shall enable rapid detection of network attacks		
c	TCP reassembly for fragmented packet protection		
d	Brute force attack mitigation		
e	SYN cookie protection , SYN Flood, Half Open Connections and NUL Packets		
f	Protection against IP spoofing		
g	Malformed packet protection		
h	Java blocking, and real-time alerts		

S.N.	Description	Compliance	Deviations, if any
59.	Firewall should support DOS protection functionalities like TCP intercept/TCP Syn cookie protection, Dead Connection Detection/ TCP sequence randomization, TCP normalization to clear tcp packets of anomalies like clearing or allowing selective tcp options, reserved bits, urgent flags & provide TTL evasion protection.		
60.	Firewall should be able to create access policies based on the User/group info from the Active Directory either through clientless or agent based mechanism .		
	Firewall should support static nat, pat, dynamic nat, pat & destination based nat		
61.	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4-to-IPv6) functionality		
62.	Firewall should support integration with Radius, Tacacs+, RSA, Ldap v3 Directory servers, Kerberos, NT server & Local Database.		
63.	Firewall should support stateful failover of sessions in Active/Standby & Active/Active mode		
64.	Firewall should support etherchannel functionality for the failover control & date interfaces for provide additional level of redundancy.		
65.	Firewall should support the functionality for allowing Asymmetrically Routed Packets in active/active mode		
66.	Firewall should support redundant interfaces to provide interface level redundancy before device failover		
67.	Firewall should support 802.3ad Etherchannel functionality to increase the bandwidth for a segment.		
68.	Firewall should support failover of IPv4 & IPv6 sessions		
69.	Firewall should replicate Nat translations, TCP,UDP connection states, ARP table, HTTP connection states, ISAKMP & IPSec SA's, SIP signalling sessions		
70.	Failover function should ensure that the routes learned via dynamic routing protocols are maintained in the standby unit as well		
71.	The broad default policy for the firewall for handling inbound traffic shall be to block all packets and connections unless the traffic type and connections have been specifically		

S.N.	Description	Compliance	Deviations, if any
	permitted.		
72.	Should support Packet Tracer capabilities for troubleshooting purposes		
73.	Should support full-featured stateful inspection firewall with enhanced application inspection capabilities. Basic application inspection support for all major protocols. Enhanced inspection for HTTP, FTP, Instant Messenger, File Sharing, SIP, H.323, SCCP, SMTP, ESMPT, DNS, RPC, CIFS, MSRPC, and NETBIOS. With the enhanced application inspection features, it should be possible to exercise a great deal of control over the behavior of network communications using those protocols. For example, with SIP inspection, you can utilize regular expressions (REGEX) to deny SIP-based VOIP communications with certain addresses or countries.		
74.	The FW should deliver per-flow, policy-based QoS services, with support for LLQ and Traffic Policing for prioritizing latency-sensitive network traffic and limiting bandwidth usage of administrator-specified applications.		
75.	Should support DTLS with SSL connections to avoid latency and bandwidth problems associated with some SSL-only connections and improves the performance of real-time applications that are sensitive to packet delays.		
76.	The FW should support Identity Firewall which provides more granular access control based on users' identities. You can configure access rules and security policies based on user names and user groups name rather than through source IP addresses.		
77.	Should support inspection of IPv6 traffic based on the extension header		
78.	It shall support SNMP (Simple Network Management Protocol) v 2.0 and v 3.0.		
79.	IPv6-enabled inspection services for applications based on HTTP, FTP, SMTP, ICMP, TCP, and UDP. In addition, SSHv2, Telnet, HTTP and HTTPS, and ICMP-based management over IPv6		
E.	**VOIP Support**		
80.	Full H.323 v1-5 (Firewall Traversal), SIP (Session Initiation Protocol), gatekeeper support, outbound bandwidth management, full interoperability with common and popular VoIP/VC gateway and communications		

S.N.	Description	Compliance	Deviations, if any
	devices shall be supported, apart from supporting all protocols.		
F.	**VPN Features**		
81.	Key exchange with latest Internet Key Exchange (IKE), IKEv2, Public Key Infrastructure PKI (X.509) shall be catered to.		
82.	Site-to-site VPN tunnels: full-mesh / star topology shall be supported.		
83.	Layer Two Tunneling Protocol (L2TP) support shall be provided.		
84.	The firewall shall support Internet Protocol Security (IPSec) & SSL.		
85.	Firewall should support RFC 6379 based Suite-B Cryptography Suites/algorithms like AES-GCM/GMAC support (128-, 192-, and 256-bit keys), ECDH support (groups 19, 20, and 21), ECDSA support (256-, 384-, and 521-bit elliptic curves) for enhanced VPN security.		
86.	Firewall should support latest IKEv2 standards for supporting SHA-2 256, 384 & 512 bit message integrity algorithms in hardware to ensure there is no performance bottleneck & higher security.		
87.	Should support pre-shared keys & Digital Certificates for VPN peer authentication.		
88.	Should support perfect forward secrecy & dead peer detection functionality.		
89.	Should support Nat-T for IPSec VPN		
G.	**Routing Features**		
90.	Configuration of VPN shall be intuitive and user friendly.		
91.	Firewall should support IPv4 & IPv6 static routing, RIP, OSPF v2 & v3		
92.	Firewall should support PIM multicast routing		
93.	Should support stateful failover for ospfv3		
94.	Firewall should support SLA monitoring for static routes		
H.	**Management Capabilities**		
95.	Should provides wide options to filter IPv6 traffic based on headers, fragments, extensions & options.		
96.	Firewall should support management of firewall policies via Cli, Telnet, SSH & inbuilt GUI management interface.		
97.	Firewall should support syslog with the functionality of sending syslogs messages via email to different teams based on syslog severity		
98.	Firewall should support SNMP logging & specify which messages are to be sent to		

S.N.	Description	Compliance	Deviations, if any
	SNMP servers		
99.	Firewall should support rate-limiting of syslog messages to avoid Dos attacks on the firewall		
100.	Firewall should support Netflow /jflow to provide detailed flow information about the connections		
101.	Firewall should support SNMP v1,2c & 3 simultaneously		
102.	Firewall should support the functionality of identifying issues quickly with continuous monitoring & providing notifications of potential problems in which a service request has been raised with all diagnostic data attached.		
103.	Firewall should support the functionality to automatically generate service request with the OEM support center, route it to the appropriate support team which provides detailed diagnostic information to speed up problem resolution.		
104.	Firewall Gui management interface should support backing up & restoring configurations.		
105.	Firewall Gui should support inbuilt function to simulate network traffic to check firewall rules & for troubleshooting network access issues.		
106.	Firewall should support packet capturing functionality to send the packet capture to ethereal/wireshark for detailed packet analysis.		
107.	Firewall should support the functionality of Auto-Update to check for latest software versions & download the same & replicate the image to the standby unit.		
J.	**Documents**		
108.	Data Sheets attached.		

2. DR Site

2.1. Core Switches

a) **Quantity Required :2 Nos**

b) **Minimum Specifications**

S.N	Feature Description	Vendor Response	Deviations, if any
A.	**Make / Model Details**		
1.	**MAKE**		
2.	**MODEL NO**		
3.	Commercial Launch date of the quoted Model.		
4.	End of Life (EoL) or End of support (EoS) date announced by the OEM. In case such date is not announced, mention		

S.N	Feature Description	Vendor Response	Deviations, if any
	the number of years for which as a practice, OEM is supporting such hardware		
B.	**Architecture**		
5.	19" Rack mountable .		
6.	Maximum of 2RU size.		
7.	Must have Redundancy Power Supply Units (PSUs),Hot-swappable, field-replaceable power supplies, 1:1 power redundancy.		
8.	Must have N:1 fan module redundancy.		
9.	All components (including elements such as I/O cards, Expansion Module, power supplies and fans) must be hot swappable with zero disruption to traffic forwarding (Unicast or multicast).		
10.	Port Throughput of 1.92 Tbps		
11.	Latency of 1 to 2 microseconds		
C.	**Interface Supports**		
12.	Must support Standard SFPs including QSFP, SFP+, 1000BASE-T SFP, Gigabit Ethernet SFP.		
13.	Must have minimum 48 x 1/10 G SFP+ and 12 X 40 G QSFP ports from day 1.		
14.	Switch must be loaded from day 1 with minimum: • 4 nos. QSFP Multimode transceiver modules • 2 nos. of 10G Fiber Multimode transceiver modules and • 4 nos. of 1G UTP transceiver modules		
15.	Must have provision to install 4 x 100G ports to support Inter-Switch backbone links or uplinks by changing or adding an additional module.		
D.	**Switching Features**		
16.	Physical standards for Network Device		
17.	Must support Fast Ethernet (IEEE 802.3u, 100BASE-TX)		
18.	Must support Gigabit Ethernet (IEEE 802.3z, 802.3ab)		
19.	Must support Ten Gigabit Ethernet (IEEE 802.3ae)		
20.	Software based standards for Network Device		
21.	Must support IEEE 802.1d - Spanning-Tree Protocol		
22.	Must support IEEE 802.1w - Rapid Spanning Tree		
23.	Must support IEEE 802.1s - Multiple Spanning Tree Protocol		
24.	Must support IEEE 802.1q - VLAN encapsulation		
25.	Must support IEEE 802.3ad - Link		

S.N	Feature Description	Vendor Response	Deviations, if any
	Aggregation Control Protocol (LACP)		
26.	Must support IEEE 802.1ab - Link Layer Discovery Protocol (LLDP)		
27.	Must support IEEE 802.3x Flow Control		
28.	Must support auto-sensing and auto-negotiation (Link Speed/Duplex)		
29.	Routing protocol support when upgraded with Layer3 License		
30.	Must support Static IP routing		
31.	Must support Open Shortest Path First (OSPF) v2 (RFC 2328)		
32.	Must support Protocol Independent Multicast Version 2 (PIMv2) sparse mode, Source Specific Multicast (SSM), Multicast Source Discovery Protocol (MSDP), and Internet Group Management Protocol Versions 2, and 3 (IGMP v2, and v3)		
33.	Must support Border Gateway Protocol - BGPv4 (RFC 1771)		
34.	Must have Routed ports on platform interfaces, switch virtual interface (SVI), PortChannels, subinterfaces, and PortChannel subinterfaces for a total of 4096 entries		
35.	Support for up to 32000 multicast ipv4 routes and 8000 multicast ipv6 routers		
36.	Support for 1000 VRF entries		
37.	Virtual Route Forwarding (VRF): VRF-lite (IP VPN); VRF-aware unicast; and BGP-, OSPF- and VRF-aware multicast		
38.	Must support 64-way equal-cost multipathing (ECMP)		
39.	Must support In-Service Software Upgrade (ISSU) for Layer 2		
40.	Must have Layer 2 IEEE 802.1p		
41.	Must have 4 hardware queues per port with per port QoS configuration		
42.	Must have Modular QoS classification compliance		
43.	Must have per port virtual output queuing or Egress Queuing		
44.	Must have ether channel support allowing upto 32 ports per EtherChannel		
45.	Must support Jumbo Frame Size (9k)		
46.	IEEE 802.3ad Link Aggregation or equivalent capabilities		
47.	Must provide for at least 32 physical ports grouped together into a single logical link		
48.	Must be able to load balance across a logical bundle using the following algorithms:		
a.	*Source IP*		

S.N	Feature Description	Vendor Response	Deviations, if any
b.	*Destination IP*		
c.	*Source and Destination IP*		
d.	*Source MAC*		
e.	*Destination MAC*		
f.	*Source and Destination MAC*		
g.	*TCP Port (destination and/or source)*		
h.	*UDP Port (destination and/or source)*		
49.	Switch must support VXLAN (Bridging and Routing) as well as NVGRE orverlay encapsulation protocol in hardware to support multiple hypervisor deployment in the Data Center		
E.	**Qos Features**		
50.	Must support IEEE 802.1p class-of-service (CoS) prioritization		
51.	Must have 4 Hardware queues per port		
52.	Must have Per-Port QoS configuration		
53.	Must have CoS Trust		
54.	Must have CoS-based egress queuing		
55.	Must have Egress strict-priority queuing		
56.	Must have Modular QoS classification compliance		
57.	Must have per port virtual output queuing or Egress Queuing		
58.	Must support Egress port-based scheduling: Weighted Round-Robin (WRR)		
59.	Must have ACL-based QoS classification (Layers 2, 3, and 4)		
F.	**Management Features**		
60.	Must provide management using 10/100/1000-Mbps management or console ports		
61.	Must have CLI-based console to provide detailed out-of-band management		
62.	Must have In-band switch management		
63.	Must have Configuration synchronization & Configuration rollback		
64.	Must support Secure Shell Version 2 (SSHv2), Telnet & SNMPv1, v2, and v3		
65.	Must support AAA, AAA with RBAC or equivalent, Radius, TACACS+ for user authentication		
66.	Must support RMON		
67.	Must support XML		
68.	Must have Advanced Encryption Standard (AES) for management traffic		
69.	Must support Unified username and passwords across CLI and SNMP		
70.	Must support Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)		
71.	Must have Digital certificates for management		

S.N	Feature Description	Vendor Response	Deviations, if any
	between switch and RADIUS server		
72.	Must have Switched Port Analyzer (SPAN) or Port mirroring on physical, PortChannel, VLAN		
G.	**Troubleshooting capabilities**		
73.	Must provide Comprehensive bootup diagnostic tests		
74.	Must have Ingress and egress packet counters per interface		
75.	Must support SPAN /Port Mirroring on physical, PortChannel or equivalent, VLAN		
76.	Must have call home / Smart Call Home or equivalent feature		
77.	Must have Embedded packet analyzer or equivalent		
78.	Version of software for supplied switch should be latest release		
79.	Must be EAL2 certified		
H.	**Documents**		
80.	Data Sheets to be attached.		

2.2. Top of Rack (TOR) Switches

a) **Quantity Required :2 Nos**

b) **Minimum Specifications:**

S.N	Feature Description	Vendor Response	Deviations, if any
A.	**Make / Model Details**		
1.	**MAKE**		
2.	**MODEL NO**		
3.	Commercial Launch date of the quoted Model.		
4.	End of Life (EoL) or End of support (EoS) date announced by the OEM. In case such date is not announced, mention the number of years for which as a practice, OEM is supporting such hardware		
B.	**Architecture**		
5.	19” Rack mountable .		
6.	Maximum of 2RU size.		
7.	Must have Redundancy Power Supply Units (PSUs),Hot-swappable, field-replaceable power supplies, 1:1 power redundancy.		
8.	Must have N:1 fan module redundancy.		
9.	All components (including elements such as I/O cards, Expansion Module, power supplies and fans) must be hot swappable with zero disruption to traffic forwarding (Unicast or multicast).		
10.	Port Throughput of 1.44 Tbps scalable to 1.92 Tbps		

S.N	Feature Description	Vendor Response	Deviations, if any
11.	Latency of 1 to 2 microseconds		
C.	**Interface Supports**		
12.	Must support QSFP+, 1000BASE-T and 10 G - T		
13.	Must have minimum 48 x 1/10 G - T and 6 X 40 G QSFP+ ports from day1.		
14.	Switch must be loaded with minimum 4 nos. QSFP Multimode transceiver modules and 48 x 1/10G-T from Day 1.		
15.	Must have provision to install 12 x 40G QSFP ports or 4 x 100G ports to support Inter-Switch backbone links or uplinks by changing or adding an additional module.		
D.	**Switching Features**		
16.	Physical standards for Network Device		
17.	Must support Fast Ethernet (IEEE 802.3u, 100BASE-TX)		
18.	Must support Gigabit Ethernet (IEEE 802.3z, 802.3ab)		
19.	Must support Ten Gigabit Ethernet (IEEE 802.3ae)		
20.	Software based standards for Network Device		
21.	Must support IEEE 802.1d - Spanning-Tree Protocol		
22.	Must support IEEE 802.1w - Rapid Spanning Tree		
23.	Must support IEEE 802.1s - Multiple Spanning Tree Protocol		
24.	Must support IEEE 802.1q - VLAN encapsulation		
25.	Must support IEEE 802.3ad - Link Aggregation Control Protocol (LACP)		
26.	Must support IEEE 802.1ab - Link Layer Discovery Protocol (LLDP)		
27.	Must support IEEE 802.3x Flow Control		
28.	Must support auto-sensing and auto-negotiation (Link Speed/Duplex)		
29.	Routing protocol support when upgraded with Layer3 License		
30.	Support for Static IP routing		
31.	Support Open Shortest Path First (OSPF) v2 (RFC 2328)		
32.	Must support Protocol Independent Multicast Version 2 (PIMv2) sparse mode, Source Specific Multicast (SSM), Multicast Source Discovery Protocol (MSDP), and Internet Group Management Protocol Versions 2, and 3 (IGMP v2, and v3)		
33.	Support Border Gateway Protocol - BGPv4 (RFC 1771)		

S.N	Feature Description	Vendor Response	Deviations, if any
34.	Must have Routed ports on platform interfaces, switch virtual interface (SVI), PortChannels, subinterfaces, and PortChannel subinterfaces for a total of 4096 entries		
35.	Support for up to 32000 multicast ipv4 routes and 8000 multicast ipv6 routers		
36.	Support for 1000 VRF entries		
37.	Support Virtual Route Forwarding (VRF): VRF-lite (IP VPN); VRF-aware unicast; and BGP-, OSPF- and VRF-aware multicast		
38.	Must support 64-way equal-cost multipathing (ECMP)		
39.	Must support In-Service Software Upgrade (ISSU) for Layer 2		
40.	Must have Layer 2 IEEE 802.1p		
41.	Must have 4 hardware queues per port with per port QoS configuration		
42.	Must have Modular QoS classification compliance		
43.	Must have per port virtual output queuing or Egress Queuing		
44.	Must have ether channel support allowing upto 32 ports per EtherChannel		
45.	Must support Jumbo Frame Size (9k)		
46.	IEEE 802.3ad Link Aggregation or equivalent capabilities		
47.	Must provide for at least 32 physical ports grouped together into a single logical link		
48.	Must be able to load balance across a logical bundle using the following algorithms:		
a.	*Source IP*		
b.	*Destination IP*		
c.	*Source and Destination IP*		
d.	*Source MAC*		
e.	*Destination MAC*		
f.	*Source and Destination MAC*		
g.	*TCP Port (destination and/or source)*		
h.	*UDP Port (destination and/or source)*		
49.	Switch must support VXLAN (Bridging and Routing) as well as NVGRE orverlay encapsulation protocol in hardware to support multiple hypervisor deployment in the Data Center		
E.	**QoS Features**		
50.	Must support IEEE 802.1p class-of-service (CoS) prioritization		
51.	Must have 4 Hardware queues per port		
52.	Must have Per-Port QoS configuration		
53.	Must have CoS Trust		
54.	Must have CoS-based egress queuing		

S.N	Feature Description	Vendor Response	Deviations, if any
55.	Must have Egress strict-priority queuing		
56.	Must have Modular QoS classification compliance		
57.	Must have per port virtual output queuing or Egress Queuing		
58.	Must support Egress port-based scheduling: Weighted Round-Robin (WRR)		
59.	Must have ACL-based QoS classification (Layers 2, 3, and 4)		
F.	**Management Features**		
60.	Must provide management using 10/100/1000-Mbps management or console ports		
61.	Must have CLI-based console to provide detailed out-of-band management		
62.	Must have In-band switch management		
63.	Must have Configuration synchronization & Configuration rollback		
64.	Must support Secure Shell Version 2 (SSHv2), Telnet & SNMPv1, v2, and v3		
65.	Must support AAA, AAA with RBAC or equivalent, Radius, TACACS+ for user authentication		
66.	Must support RMON		
67.	Must support XML		
68.	Must have Advanced Encryption Standard (AES) for management traffic		
69.	Must support Unified username and passwords across CLI and SNMP		
70.	Must support Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)		
71.	Must have Digital certificates for management between switch and RADIUS server		
72.	Must have Switched Port Analyzer (SPAN) or Port mirroring on physical, PortChannel, VLAN		
G.	**Troubleshooting capabilities**		
73.	Must provide Comprehensive bootup diagnostic tests		
74.	Must have Ingress and egress packet counters per interface		
75.	Must support SPAN /Port Mirroring on physical, PortChannel or equivalent, VLAN		
76.	Must have call home / Smart Call Home or equivalent feature		
77.	Must have Embedded packet analyzer or equivalent		
78.	Version of software for supplied switch should be latest release		
79.	Must be EAL2 certified		
H.	**Documents**		
80.	Data Sheets to be attacheds.		

2.3. DMZ Switch

a) **Quantity Required : 2Nos**

b) **Minimum Specifications:**

S.N	Feature Description	Compliance (Y/N)	Deviations, if any
A.	**Make / Model Details**		
1.	**MAKE**		
2.	**MODEL No:**		
3.	Commercial Launch date of the quoted Model.		
4.	End of Life (EoL) or End of support (EoS) date announced by the OEM. In case such date is not announced, mention the number of years for which as a practice, OEM is supporting such hardware		
B.	**Architecture**		
5.	19" Rack mountable .		
6.	Maximum of 2RU size.		
7.	Must have Redundancy Power Supply Units (PSUs), Hot-swappable, field-replaceable power supplies, 1:1 power redundancy.		
8.	Must have N:1 fan module redundancy.		
9.	All components (including elements such as I/O cards, Expansion Module, power supplies and fans) must be hot swappable with zero disruption to traffic forwarding (Unicast or multicast).		
10.	Port Throughput of 1.44 Tbps scalable to 1.92 Tbps		
11.	Latency of 1 to 2 microseconds		
C.	**Interface Supports**		
12.	Must support QSFP+, 1000BASE-T and 10 G - T		
13.	Must have minimum 48 x 1/10 G - T and 6 X 40 G QSFP+ ports from day1		
14.	The switch must be populated from day 1 with 48 x 1/10G-T and 4 X 40G QSFP ports.		
15.	The switch must be scaleable to 12 x 40G QSFP ports or 4 x 100G ports by changing or adding an additional module. 100G must be supported on the switch from day 1.		
D.	**Switching Features**		
16.	Physical standards for Network Device		
17.	Must support Fast Ethernet (IEEE 802.3u, 100BASE-TX)		
18.	Must support Gigabit Ethernet (IEEE 802.3z, 802.3ab)		
19.	Must support Ten Gigabit Ethernet (IEEE 802.3ae)		

S.N	Feature Description	Compliance (Y/N)	Deviations, if any
20.	Software based standards for Network Device		
21.	Must support IEEE 802.1d - Spanning-Tree Protocol		
22.	Must support IEEE 802.1w - Rapid Spanning Tree		
23.	Must support IEEE 802.1s - Multiple Spanning Tree Protocol		
24.	Must support IEEE 802.1q - VLAN encapsulation		
25.	Must support IEEE 802.3ad - Link Aggregation Control Protocol (LACP)		
26.	Must support IEEE 802.1ab - Link Layer Discovery Protocol (LLDP)		
27.	Must support IEEE 802.3x Flow Control		
28.	Must support auto-sensing and auto-negotiation (Link Speed/Duplex)		
29.	Routing protocol support when upgraded with Layer3 License		
30.	Must support Static IP routing		
31.	Must support Open Shortest Path First (OSPF) v2 (RFC 2328)		
32.	Must support Protocol Independent Multicast Version 2 (PIMv2) sparse mode, Source Specific Multicast (SSM), Multicast Source Discovery Protocol (MSDP), and Internet Group Management Protocol Versions 2, and 3 (IGMP v2, and v3)		
33.	Must support Border Gateway Protocol - BGPv4 (RFC 1771)		
34.	Must have Routed ports on platform interfaces, switch virtual interface (SVI), PortChannels, subinterfaces, and PortChannel subinterfaces for a total of 4096 entries		
35.	Support for up to 32000 multicast ipv4 routes and 8000 multicast ipv6 routers		
36.	Support for 1000 VRF entries		
37.	Virtual Route Forwarding (VRF): VRF-lite (IP VPN); VRF-aware unicast; and BGP-, OSPF- and VRF-aware multicast		
38.	Must support 64-way equal-cost multipathing (ECMP)		
39.	Must support In-Service Software Upgrade (ISSU) for Layer 2		
40.	Must have Layer 2 IEEE 802.1p		
41.	Must have 4 hardware queues per port with per port QoS configuration		
42.	Must have Modular QoS classification compliance		
43.	Must have per port virtual output queuing or Egress Queuing		

S.N	Feature Description	Compliance (Y/N)	Deviations, if any
44.	Must have ether channel support allowing upto 32 ports per EtherChannel		
45.	Must support Jumbo Frame Size (9k)		
46.	IEEE 802.3ad Link Aggregation or equivalent capabilities		
47.	Must provide for at least 32 physical ports grouped together into a single logical link		
48.	Must be able to load balance across a logical bundle using the following algorithms:		
a.	*Source IP*		
b.	*Destination IP*		
c.	*Source and Destination IP*		
d.	*Source MAC*		
e.	*Destination MAC*		
f.	*Source and Destination MAC*		
g.	*TCP Port (destination and/or source)*		
h.	*UDP Port (destination and/or source)*		
49.	Switch must support VXLAN (Bridging and Routing) as well as NVGRE orverlay encapsulation protocol in hardware to support multiple hypervisor deployment in the Data Center		
E.	**QoS Features**		
50.	Must support IEEE 802.1p class-of-service (CoS) prioritization		
51.	Must have 4 Hardware queues per port		
52.	Must have Per-Port QoS configuration		
53.	Must have CoS Trust		
54.	Must have CoS-based egress queuing		
55.	Must have Egress strict-priority queuing		
56.	Must have Modular QoS classification compliance		
57.	Must have per port virtual output queuing or Egress Queuing		
58.	Must support Egress port-based scheduling: Weighted Round-Robin (WRR)		
59.	Must have ACL-based QoS classification (Layers 2, 3, and 4)		
F.	**Management Features**		
60.	Must provide management using 10/100/1000-Mbps management or console ports		
61.	Must have CLI-based console to provide detailed out-of-band management		
62.	Must have In-band switch management		
63.	Must have Configuration synchronization & Configuration rollback		
64.	Must support Secure Shell Version 2 (SSHv2), Telnet & SNMPv1, v2, and v3		
65.	Must support AAA, AAA with RBAC or equivalent, Radius, TACACS+ for user		

S.N	Feature Description	Compliance (Y/N)	Deviations, if any
	authentication		
66.	Must support RMON		
67.	Must support XML		
68.	Must have Advanced Encryption Standard (AES) for management traffic		
69.	Must support Unified username and passwords across CLI and SNMP		
70.	Must support Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)		
71.	Must have Digital certificates for management between switch and RADIUS server		
72.	Must have Switched Port Analyzer (SPAN) or Port mirroring on physical, PortChannel, VLAN		
G.	**Troubleshooting capabilities**		
73.	Must provide Comprehensive bootup diagnostic tests		
74.	Must have Ingress and egress packet counters per interface		
75.	Must support SPAN /Port Mirroring on physical, PortChannel or equivalent, VLAN		
76.	Must have call home / Smart Call Home or equivalent feature		
77.	Must have Embedded packet analyzer or equivalent		
78.	Version of software for supplied switch should be latest release		
79.	Must be EAL2 certified		
H.	**Documents**		
80.	Data Sheets to be attached.		

2.4. Stackable Switches

a) **Quantity Required : 4nos(2 each in a stack with stacking cables)**

b) **Minimum Specifications:**

S.N	Feature Description	Compliance (Y/N)	Deviations, if any
A.	**Make / Model Details**		
1.	**MAKE**		
2.	**MODEL No:**		
3.	Commercial Launch date of the quoted Model.		
4.	End of Life (EoL) or End of support (EoS) date announced by the OEM. In case such date is not announced, mention the number of years for which as a practice, OEM is supporting such hardware		
B.	**Switch Hardware features**		
5.	Switch should have minimum 24 10/100/1000 Base-T ports. with additional 4 Nos. of 1G SFP Based ports for uplink connectivity and 2		

S.N	Feature Description	Compliance (Y/N)	Deviations, if any
	stacking ports with all accessories for stacking purpose from day1		
6.	Switch should be 1 RU rack mountable in nature, stackable with dedicated 80Gbps of throughput with minimum of 4 switches in a stack with single IP management.		
7.	Switch should support IEEE Standards of Ethernet: IEEE 802.1d, 802.1s, 802.1w, 802.3ad, 802.3x, 802.1D, 802.1p, 802.1Q, 802.3, 802.3u, 802.3ab, 802.3z, 100Base-T, 1000BASE-T, 1000BASE-X (mini-GBIC/SFP), 1000BASE-SX, 1000BASE-LX/LH, IEEE 802.3ae 10Gigabit Ethernet and IEEE 802.3ah (100BASE-X single/multimode fiber only)		
8.	Switch should support Auto MDI/MDIX		
9.	All SFP modules should be hot swappable		
10.	Switch should have minimum 120 Gbps switching bandwidth capacity (Gbps) per switch		
11.	Switch should have minimum 70 Mpps throughput per switch		
C.	**Layer-2 Requirements**		
12.	Switch should support minimum 15000 MAC address per switch		
13.	The switch should have IPV4 & IPv6 support from day one		
14.	It should support Jumbo packets up to 9,216-byte frame size to improve performance of large data transfers.		
15.	Should support IEEE 802.1Q VLAN encapsulation and up to 1000 active VLANs per switch		
16.	Switch should support Voice VLAN for easier administration and troubleshooting		
17.	Switch should support cross-stack etherchannel using LACP and no performance impact for voice traffic during stack convergence		
18.	Switch should be having Zero Turn-Around Time to configure policies based on device-types.		
19.	It should support IEEE 802.3ad Link Aggregation Control Protocol (LACP) with up to 8 links (ports) per trunk.		
20.	Switch should support link aggregation for minimum 6 GE ports and minimum 24 LAG groups.		
21.	Should be able to discover the neighboring device of the same vendor giving the details about the platform, IP Address, Link connected		

S.N	Feature Description	Compliance (Y/N)	Deviations, if any
	through etc, thus helping in troubleshooting connectivity problems		
22.	Should support a mechanism to detect connectivity issues with both fiber and copper cabling. Ensures that a partially failed link is shut down on both sides, to avoid L2/L3 protocol convergence issues		
23.	The Switch should support IGMP V1,V2,V3 and MLD V1 and V2		
24.	Switch should support auto-recovery of error-disabled ports due to network errors.		
25.	The Switch Should support auto detection and plug and play of the device onto the network with configuration as per the template.		
26.	It should support IEEE 802.1s Multiple Spanning Tree Protocol and provide legacy support for IEEE 802.1d STP and IEEE 802.1w RSTP		
27.	The switch should support feature which shuts down Spanning Tree PortFast-enabled interfaces when BPDUs are received to avoid accidental topology loop		
28.	The switch should support feature which provides multicast authentication by filtering out non-subscribers and limits the number of concurrent multicast streams available per port (Optional)		
29.	It should support IEEE 802.1AB Link Layer Discovery Protocol (LLDP)		
30.	Should support Port Mirroring based on acl, port basis / vlan basis to support intrusion prevention system deployment in different VLANs. Should support port mirroring across the stack switches to remotely monitor ports in a Layer 2 switch network from any other switch in the same network.		
31.	Switch should provide minimum 2 or more mirror sessions		
D.	**Security Requirements**		
32.	It should support protected ports to isolate specified ports from all other ports on the switch.		
33.	Switch Should support VLAN Based and Port Based ACLs		
34.	It should support IEEE 802.1X user authentication using an IEEE 802.1X supplicant in conjunction with a RADIUS server.		
35.	switch should provide 802.1x support for VLAN assignment, Guest VLAN, MAC-Auth-Bypass		

S.N	Feature Description	Compliance (Y/N)	Deviations, if any
	and ACL support		
36.	It should support MAC-based authentication allowing client to be authenticated with the RADIUS server based on client‟s MAC address.		
37.	It should support TACACS+ or RADIUS authentication for secure switch CLI logon.		
38.	It should support management access (CLI, Web, MIB) securely encrypted through SSHv2, SSL, and SNMPv3.		
39.	Per-port storm control for preventing broadcast, multicast, and unicast storms		
40.	The switch should support monitoring, capturing, and recording of flows to provide network traffic statistics for further analysis, accounting, network monitoring and network planning. Flows need to be captured from physical ethernet port or from vlan interface.		
41.	The switch should support feature to prevent malicious attacks on the switch by not relaying invalid ARP requests and responses to other ports in the same VLAN.		
42.	The switch should provide Bidirectional data support on the mirror port to allow Intrusion Detection to take action when an intruder is detected. (Optional)		
E.	**Qos Requirements**		
43.	It should support IEEE 802.1p traffic prioritization delivering data to devices based on the priority and type of traffic.		
44.	should have strict priority queuing or high strict priority queue		
45.	Switch should support 802.1p based CoS and differentiated services code point (DSCP) based field classification, marking and reclassification on a per-packet basis for L2,L3,L4 information.		
F.	**Management Requirements**		
46.	It should support SNMPv1/v2c/v3.		
47.	It should support RMON providing advanced monitoring and reporting capabilities for statistics, history, alarms, and events.		
48.	Switch should support following IPv6 features and functions :- IPv6 Host support (IPv6 support: Addressing; IPv6: ICMPv6, TCP/UDP over IPv6; Applications: Ping/Traceroute/VTY/SSH/TFTP, SNMP for IPv6 objects), HTTP and HTTP(s) over IPv6, SysLog over IPv6) IPv6 management		

S.N	Feature Description	Compliance (Y/N)	Deviations, if any
	IPv6 MLD v1 and v2 snooping		
49.	The Switch Should support single point of management enabling (zero-touch deployment) plug-and-play configuration, archiving of configurations and image-management for switches		
50.	Switch should support NTP		
G.	**Troubleshooting Requirements**		
51.	Switch should support Layer 2 traceroute to identify the physical path that a packet takes from source to destination		
52.	Switch should support feature which enabled devices to perform proactive diagnostics on their own components to provide real-time alerts and remediation advice when an issue is detected and also communicate with support center using email and open support case with support center. (Optional)		
53.	Switch should generate hardware failure information in a log file and need to be stored in flash so that support center can access these files and to identify the root cause.		
H.	**Documents**		
54.	Data Sheets attached.		

2.5. Core Firewall

a) **Quantity Required : 2Nos in HA**

b) **Minimum Specifications:**

S.N.	Description	Compliance	Deviations, if any
A.	**Make / Model Details**		
1	**MAKE**		
2.	**MODEL N:**		
3.	Commercial Launch date of the quoted Model.		
4.	End of Life (EoL) or End of support (EoS) date announced by the OEM. In case such date is not announced, mention the number of years for which as a practice, OEM is supporting such hardware		
5.	The Proposed Firewall OEM should be in Gartners leaders & Challengers Quadrant as per the latest Report for Next Generation Firewall.		
B.	**General Requirements**		
6.	The solution should have separate or inbuilt management solution. In case of separate management solution the same should be on separate appliance and the same needs to be		

S.N.	Description	Compliance	Deviations, if any
	integrated with firewall.		
7.	The solution should have separate reporting solution which should be on separate appliance and needs to be integrated with the firewall.		
8.	The firewall appliance should support Application control functionalities.		
9.	The firewall appliance should support Secure Remote access to corporate application over the internet.		
10.	The firewall appliance should support for Active–Active and Active-Passive as High Availability option.		
11.	In case of Active/Active the Appliance should support Load Balancing.		
12.	The Licensing for all the components forming the solution should be a per device and not user/IP based (i.e. should support unlimited users)		
13.	The firewall appliance should support IPv4 and IPv6 from day one.		
14.	The appliance should support VOIP traffic filtering.		
15.	The Firewall appliance Architecture should be on multiple core/tire CPU or ASIC based.		
16.	The communication between Firewall System and management & reporting solution should be encrypted with SSL or PKI.		
17.	The Firewall system should have a provision to handle the bandwidth management. It should offer the Bandwidth Management for every TCP, IPSEC, & VoIP protocols with attributes of Minimum Committed Bandwidth per protocol; Maximum Bandwidth per protocol; Priority for the queues etc.		
18.	The Firewall system should support the IPSec VPN for both Site-Site & Remote Access VPN.		
19.	The Firewall system should support virtual tunnel interfaces to provision Route-Based IPSec VPN.		
20.	The firewall system should have at least 100GB local hard-disk or should be provided through external Firewall Management for storing logs.		
21.	The Firewall & Integrated IPSEC VPN Applications should be ICSA Labs certified for ICSA 4.0, FIPS 140-2 certified.		
B.	**Hardware and Interface Requirements**		
22.	The firewall appliance must be supplied with at least 8 numbers of 10/100/1000 Mbps		

S.N.	Description	Compliance	Deviations, if any
	interfaces on Copper from day one.		
23.	The firewall appliance must be supplied with at least 2 numbers of 10GBase-F SFP+ Ports with required 10G modules from day one.		
24.	The firewall appliance should support at least 2 numbers of additional 10GBase-F SFP+ Ports for future up-gradation without changing the appliance.		
25.	The appliance should support atleast one 10/100/1000 dedicated management interfaces to configure/manage the firewall policies, perform image upgrades even in case of failure of the data interfaces. Data ports should not be used for management purpose		
26.	The firewall appliance should have Console port and USB Port.		
27.	The firewall appliance should support VLAN tagging (IEEE 802.1q)		
28.	The firewall appliance should support Link Aggregation functionality to group multiple ports as single port.		
29.	The firewall appliance should support Ethernet Bonding functionality for Full Mesh deployment architecture.		
30.	The Firewall should support CA functionality.		
C.	**Performance Requirements**		
31.	Firewall performance (Large packets) Should be 40 Gbps and above		
32.	Firewall should provide atleast 10 Gbps of Multi-protocol/IMIX real-world throughput based on protocols like HTTP, SMTP, FTP, IMAP , DNS (Only UDP based performance nos. will not be considered)		
33.	The Integrated IPS throughput should be at least 6 Gbps or above with all protections enabled for Multiprotocol/IMIX traffic.		
34.	The firewall should support a minimum of 20 Gbps of IPSec VPN Throughput		
35.	Firewall should support minimum 10 Million concurrent connections.		
36.	Firewall should support minimum 20,00,00 new connections per second (cps).		
37.	The appliance should be supplied with redundant inbuilt power supplies from day one.		
38.	The Firewall Should support for at least 25,000 client to gateway VPN tunnels.		
39.	The Firewall Should provide combined		

S.N.	Description	Compliance	Deviations, if any
	throughput of atleast 5Gbps by enabling multiprotocol/IMIX Traffic and IPS in blocking /Protection Mode.		
40.	Should support firewall virtualization and minimum 5 Virtual Firewall licenses should be included.		
D.	**Network and Routing Requirements**		
41.	Static routing must be supported.		
42.	Policy based Routing must be supported.		
43.	Dynamic Routing: RIPv1 and v2, OSPF v2 and v3, ISIS, BGP4.		
44.	Multicast Routing must be supported.		
E.	**Firewall Filtering Requirements**		
45.	The Firewall technology should be ICSA Labs and EAL 4 certified.		
46.	Firewall should able to operate in "transparent mode" apart from the standard NAT mode		
47.	The Firewall must provide NAT functionality: NAT64, NAT46, static NAT, dynamic NAT, PAT		
48.	Should support "Policy-based NAT" and "central NAT " Table		
49.	The Firewall should provide advanced NAT		
50.	capabilities, supporting NAT Traversal for services like SIP/H.323 /SCCP		
51.	Firewall should support Voice based protocols like H.323, SIP, SCCP, MGCP etc		
52.	The Firewall should support Address objects: subnet, IP, IP range, GeoIP (Geography), FQDN		
53.	The Firewall should support User-Group based Authentication (Identity based Firewalling) & Scheduling		
54.	The Firewall should support device based security policy and device identification		
55.	Should support integrated Traffic shaping and QOS: shared policy shaping, per-IP shaping, maximum & guaranteed bandwidth, maximum concurrent connections per IP, traffic prioritization, Type of Service (TOS) and Differentiated Services (DiffServ)		
F.	**Authentication Requirements**		
56.	Support for authentication for Users and Firewall Administrators (Local and Remote – RADIUS, LDAP & TACACS+)		
57.	Should support single sign on for Windows AD, Novell eDirectory, Citrix and Terminal Server Agent		
58.	Support for RSA SecureID or other 3rd party		

S.N.	Description	Compliance	Deviations, if any
	Token.		
59.	Should support PKI / Digital Certificate based two-factor Authentication for both Users and Firewall Administrators		
60.	Should support captive portal authentication		
61.	Device should support separate guest group profile and it should have expiry time for all the guest		
62.	Device should support local user password expiration feature		
63.	Firewall Should support device Identification ,OS, User, destination hostname & geographic visibility		
64.	Firewall should also support Real-time client reputation monitoring		
G.	**High Availability Requirements**		
65.	The device must support Active-Active as well as Active-Passive redundancy.		
66.	Should support Redundant heartbeat interfaces		
67.	Should have HA reserved management interface		
68.	The Firewall must support stateful failover for both Firewall and VPN sessions.		
69.	Should support Port, local & remote link monitoring		
70.	Should support Failure detection notification		
H.	**IPSEC/SSLVPN Requirements**		
71.	The VPN should be integrated with firewall and should be ICSA Labs certified for both IPSec and SSL-TLS. Should support the following protocols		
a	DES & 3DES		
b	MD5, SHA-1 & the more secure SHA-256 authentication		
c	Diffie-Hellman Group 1, Group 2, Group 5 & the more secure Group 14.		
d	Internet Key Exchange (IKE) v1 as well as IKE v2 algorithm		
e	The new encryption standard AES 128, 192 & 256 (Advanced Encryption Standard)		
72.	IPSec VPN should support XAuth over RADIUS and RSA SecurID or similar product.		
73.	Should have integrated SSL VPN with no user license restriction. Please specify if the product does not follow the required licensing policy		
74.	Should support SSL portal concurrent users limiting		
75.	Should support one time login per user		

S.N.	Description	Compliance	Deviations, if any
	options: prevents concurrent logins using same username		
76.	Should support SSL-VPN Two-factor Authentication		
77.	Should support single sign-on for FTP and SMB		
78.	Should support Windows, and MAC OS for SSL-VPN (Should have always-on clients for these OS apart from browser based access)		
79.	Should support Host integrity checking and OS check (for windows terminals only) prior to SSL tunnel mode connections		
80.	Should support MAC host check per portal		
81.	Should have Cache cleaning option just before the SSL VPN session ends		
82.	Should also support Virtual desktop option to isolates the SSL VPN session from the client computer's desktop environment		
83.	Should able to view and manage current IPSEC and SSL VPN connections in details		
84.	Device should support client for both IPSec and SSL-VPN		
85.	Should support NAT within IPSec/SSL VPN tunnels		
86.	Should also support PPTP and L2TP over IPSec VPN protocols.		
I.	**IPS Requirements**		
87.	Should have integrated Network Intrusion Prevention System (NIPS) and should be ICSA and NSS Labs certified.		
88.	Should have a built-in Signature and Anomaly based IPS engine on the same unit.		
89.	Should support SSL inspection for IPS and Application Control		
90.	Should support minimum 5000+ IPS signatures		
91.	Should support automatic pull or push signature update		
92.	Should have IPS Actions: default, monitor, block, reset, or quarantine (attackers IP, attackers IP and Victim IP, incoming interface) with expiry time		
93.	Should have Packet logging option		
94.	Should have Filter Based Selection: severity, target, OS, application and/or protocol		
95.	Should support IPv4 and IPv6 Rate based DOS protection		
96.	Supports user-defined signatures (ie Custom Signatures) with Regular Expressions.		
97.	Should support Application based control		

S.N.	Description	Compliance	Deviations, if any
	feature for over 3000 applications and in 18 Categories		
98.	Should have Filter based selection: by category, popularity, technology, risk, vendor and/or protocol		
99.	Should have Actions: block, reset session, monitor only, application control traffic shaping		
100	Custom application signature support		
101	Should Support SSH inspection		
102	Should support Deep inspection for cloud based application		
103	Should support replacement message for blocked Applications		
104	Should able to protect from Botnet and Phishing		
105	Should perform Traffic Shaping of popular P2P applications like KaZaa, Gnutella, BitTorrent, WinNY, eDonkey etc		
106	Should control popular IM/P2P applications regardless of port/protocol like Yahoo, MSN, Skype, AOL, ICQ etc		
107	Should support Botnet C&C blocking with IP reputation DB		
108	Administrator shall be able to configure DoS policies that are used to associate DoS settings with traffic that reaches an interface based on defined services, source and destinations IP/Range.		
109	Supports attack recognition inside IPv6 encapsulated packets		
J.	**Other Requirements**		
110	Provision to create secure zones / DMZ (ie Multi-Zone support)		
111	Should support Gateway Data Loss Prevention (DLP) feature for popular protocols like HTTP, HTTPS, FTP, POP3, IMAP, SMTP, POP3S, IMAPS, SMTPS		
112	The DLP feature should support popular file types like MS-Word, PDF etc. Should also support DLP fingerprinting		
113	Should support DLP watermarking: allows filter files that pass through the unit and contain a corporate identifier (a text string) and a sensitivity level (Critical, Private, and Warning) hidden in a watermark.		
114	Should Support Packet Capture/sniffer to capture and examine the contents of individual data packets that traverse the firewall appliance for troubleshooting, diagnostics and general network activity		

S.N.	Description	Compliance	Deviations, if any
115	The device should belong to a family of products that attains NSS Approved Certification, IPv6 Ready Phase 2 and USGv6 IPv6 Certified		
116	Should able to support Geo-IP block and able to block country wise traffic.		
117	ICSA labs certification for Firewall, SSL, IPSEC VPN, AV, IPS.		
K.	**Documents**		
118	Data Sheets to be attached.		

3. Warranty, AMC and Support for all Equipments

S.N.	Description	Compliance	Deviations, if any
1.	Warranty – comprehensive, on-site, 3 years back to back with OEM		
2.	AMC – comprehensive, on-site, 3 years back to back with OEM		
3.	NBD replacement of failed hardware		
4.	In case of failure of both the equipment, replacement should be within 4 hours from time call is logged.		
5.	Uptime of equipment – 99.5%		
6.	Call to Response – 2 hours		
7.	Call to Resolution – 4 hours		
8.	**Bidder support**		
a	Onsite L1 support		
b	24X7X365		
9.	**OEM support**		
a	L2 and above		
b	Through telephone or mail. In case issue not resolved on-site engineer to be deployed.		
c	24X7X365		

Date :…….. Name and Signature of Authorized Signatory:…….

Place: …… Designation: …… Phone & Mail id:……

Name of Organization :…… Seal:……

11.4. Annexure –IV:- Commercial Bid - cum- Price Break-up Format

(RfP No.400/2016/1152/ BYO/ITV dated February 24, 2016)

1. Cost of New Hardware

S.N.	Description	Qty.	Unit Cost				Total Cost
			Figures	Words	Taxes	Total	
		A	B		C	D=B+C	E=AXD
A.	**Data Center Hardware**						
1.	Cost of core switches with three years warranty and support and specifications as per **Annexure-III, S.N.(1.1)**	02					
2.	Cost of Top of Rack switches with three years warranty and support and specifications as per **Annexure-III, S.N.(1.2).**	06					
3.	Cost of DMZ switches with three years warranty and support and specifications as per **Annexure-III, S.N.(1.3).**	02					
4.	Cost of stackable switches with three years warranty and support, including 2 stackable cables and specifications as per **Annexure-III, S.N.(1.4).**	04					
5.	Cost of Intrusion Prevention System with three years warranty and support and specifications as per **Annexure-III, S.N.(1.5).**	02					
6.	Cost of perimeter firewall with three years warranty and support and	02					

S.N.	Description	Qty.	Unit Cost				Total Cost
			Figures	Words	Taxes	Total	
		A	B		C	D=B+C	E=AXD
	specifications as per **Annexure-III, S.N.(1.6).**						
7.	**Total Cost of Data Center hardware – 'X'**						
B.	**DR Site Hardware**						
1.	Cost of core switches with three years warranty and support and specifications as per **Annexure-III, S.N.(2.1).**	02					
2.	Cost of Top of Rack switches with three years warranty and support and specifications as per **Annexure-III, S.N.(2.2).**	02					
3.	Cost of DMZ switches with three years warranty and support and specifications as per **Annexure-III, S.N.(2.3).**	02					
4.	Cost of stackable switches with three years warranty and support, including 2 stackable cables and specifications as per **Annexure-III, S.N.(2.4).**	04					
5.	Cost of core firewalls with three years warranty and support and specifications as per **Annexure-III, S.N.(2.5).**	02					
6.	**Total Cost of DR Site Hardware –'Y'**						
C.	**Total Cost of Data Center and DR Site Hardware – (X+Y)**						

2. AMC Charges

a) Table 2 (a) :Fourth Year AMC Charges

S.N.	Description	Qty.	Unit Cost				Total Cost
			Figures	Words	Taxes	Total	
		A	B		C	D=B+C	E=AXD
A.	**Data Center Hardware**						
1.	Core switches	02					
2.	Top of Rack Switches	06					
3.	DMZ Switches	02					
4.	Stackable Switches	04					
5.	Perimeter Firewall	02					
6.	Intrusion Prevention System (IPS)	02					
7.	***Total Data Center Hardware AMC charges for 4th Year - X***						
B.	**DR Site Hardware**						
1.	Core switches	02					
2.	Top of Rack Switches	02					
3.	DMZ Switches	02					
4.	Stackable Switches	04					
5.	Core Firewall	02					
6.	***Total DR Site Hardware AMC charges for 4th Year - Y***						
C.	**Total fourth Year AMC Charges for Data Center and DR Site – (X + Y)**						

b) Table 2(b) : Fifth Year AMC Charges

S.N.	Description	Qty.	Unit Cost				Total Cost
			Figures	Words	Taxes	Total	
		A	B		C	D=B+C	E=AXD
A.	**Data Center Hardware**						
1.	Core switches	02					
2.	Top of Rack Switches	06					

S.N.	Description	Qty.	Unit Cost				Total Cost
			Figures	Words	Taxes	Total	
		A	B		C	D=B+C	E=AXD
3.	DMZ Switches	02					
4.	Stackable Switches	04					
5.	Perimeter Firewall	02					
6.	Intrusion Prevention System	02					
7.	**Total Data Center Hardware AMC charges for 5th Year - X**						
B.	**DR Site Hardware**						
1.	Core switches	02					
2.	Top of Rack Switches	02					
3.	DMZ Switches	02					
4.	Stackable Switches	04					
5.	Core Firewall	02					
6.	***Total DR Site Hardware AMC charges for 5th Year - Y***						
C.	**Total Fifth Year AMC Charges for Data Center and DR Site – (X + Y)**						

c) Table 2(c) : Sixth Year AMC Charges

S.N.	Description	Qty.	Unit Cost				Total Cost
			Figures	Words	Taxes	Total	
		A	B		C	D=B+C	E=AXD
A.	**Data Center Hardware**						
1.	Core switches	02					
2.	Top of Rack Switches	06					
3.	DMZ Switches	02					
4.	Stackable Switches	04					
5.	Perimeter Firewall	02					
6.	Intrusion Prevention System	02					
7.	**Total Data Center Hardware AMC charges for 6th Year - X**						

S.N.	Description	Qty.	Unit Cost				Total Cost
			Figures	Words	Taxes	Total	
		A	B		C	D=B+C	E=AXD
B.	**DR Site Hardware**						
1.	Core switches	02					
2.	Top of Rack Switches	02					
3.	DMZ Switches	02					
4.	Stackable Switches	04					
5.	Core Firewall	02					
6.	***Total DR Site Hardware AMC charges for 6^{h} Year - Y***						
C.	**Total Sixth Year AMC Charges for Data Center and DR Site – (X + Y)**						

3. Table 3: Implementation and Training Charges

S.N.	Description	Cost			
		Figures	Words	Taxes	Total
		B		C	D=B+C
1.	Commissioning, Installation, Configuration of entire solution at specified location(s) as per the scope mentioned in the RfP and OEM training cost for switches, firewalls and IPS for two resources.				

4. Table 4: Optional Items Cost

S.N.	Description	Qty.	Cost			
			Figures	Words	Taxes	Total
			B		C	D=B+C
1.	1X10G Fiber Multimode transceiver module for Core switch at DC	01				
2.	1X40G Fiber Multimode transceiver module for Core switch at DC	01				
3.	1X40G (QSFP) Multimode transceiver	01				

S.N.	Description	Qty.	Cost			
			Figures	Words	Taxes	Total
			B		C	D=B+C
	module for TOR switches at DC.					
4.	1X40G (QSFP) Multimode transceiver module for DMZ switch at DC.					
5.	**Total**					

5. Total Cost of Ownership

S.N.	Description	Amount (Rs)
1.	Total cost of New Hardware as per **Table 1**	
2.	Total Cost of AMC for 4th Year as per **Table 2(a)**	
3.	Total Cost of AMC for 5th Year as per **Table 2(b)**	
4.	Total Cost of AMC for 6th Year as per **Table 2(c)**	
5.	Implementation and training charges (one time) as per **Table 3**	
6.	Optional Cost as per **Table 4**	
7.	**Total Cost of Ownership**	

6. TAX Rates

Bidders are required to specify all types of tax rate(s) applicable for the delivery of the hardware / software / Services as mentioned above in Annexure III. Below mentioned rate chart will be used in future with the selected bidder, to arrive the cost of item (In case tax rate is changed); while placing the repeat order / order of optional items as per RfP clause 10.17 during a period of one year. If required, more rows may be added to the table detailed below:

S.N.	Tax Head	Applicable for Item(s) as detailed in Annexure -III (Hardware / Software)	Tax %
1.	Value Added Tax (VAT)		
2.	Central Sales Tax (CST)		
3.	Work Contract Tax (WCT)		
4.	Service Tax (ST)		
5.	Swachh Bharat Cess		

Bidders are requested to note the following:

1. Conditional commercial bids would be rejected.
2. All the details must be provided as per format, table wise summation to be calculated and updated, deviation from above format would enable the commercial bid to be rejected.
3. Masked commercial bids must be given with technical bid.
4. All the rates must be quoted in INR. The cost should be inclusive of all taxes.
5. SIDBI can place repeat order for additional hardware (if so desired) at the above mentioned prices within one year from the date of acceptance.
6. Octroi amount, if any, shall be reimbursed separately on the production of original receipt in the name of SIDBI.

Date :……. **Name and Signature of Authorized Signatory:…….**

Place: ……. **Designation: …….** **Phone & Mail id:……**

Name of Organization :…… **Seal:……**

11.5. Annexure –V - Manufacturer Authorisation Format

(To be submitted on OEM's letter head for each of the products quoted)

Ref: Date:

To
The General Manager [Systems]
Small Industries Development Bank of India
MSME Development Center, 3rd Floor
Information Technology Vertical
Plot No.C-11, G Block
Bandra Kurla Complex
Bandra [East]
Mumbai 400 051

Dear Sir,

Manufacturer Authorisation for
RfP No. 400/2016/1152 /BYO/ITV dated February 24, 2016

We **<OEM Name>** having our registered office at **<OEM Address>** are an established and reputed manufacturer of **<hardware details>** do hereby authorise M/s_____ **(Name and address of the Partner)** to offer their quotation, negotiate and conclude the contract with you against the above invitation for tender offer.

We hereby extend our full guarantee and warranty as per terms and conditions of the tender and the contract for the solution, products/equipment and services offered against this invitation for tender offer by the above firm and will extend technical support and updates / upgrades if contracted by the bidder.

We also confirm that we will ensure all product upgrades (including management software upgrades and new product feature releases) are provided by **M/s ……..**for all the products quoted for and supplied to the bank during the six year product warranty and AMC period.

<OEM Name>

<Authorised Signatory>

Name: _____

Designation:_____

Note: This letter of authority should be on the letterhead of the OEM and should be signed by a person competent and having the power of attorney to bind the manufacturer. It should be included by the bidder in its bid.

11.6. Annexure –VI - Undertaking of Authenticity

[to be signed by authority not lower than the Company Secretary of the Bidder]

Ref: Date:

The General Manager [Systems]
Small Industries Development Bank of India
MSME Development Center, 3rd Floor
Information Technology Vertical
Plot No.C-11, G Block
Bandra Kurla Complex
Bandra [East]
Mumbai 400 051

Dear Sir,

Undertaking of Authenticity

With reference to the hardware items (network switches, firewalls and IPS) quoted to you vide our quotation No.: _____dated _____ in response to your **tender no. 400/2016/1152/BYO/ITV dated February 24, 2016,** we hereby undertake that all the components / parts / assembly / software used in network switches/other hardware items shall be original/ new from respective OEMs of the products and that no refurbished / duplicate / second hand components / parts / assembly / software are being used or shall be used.

We also undertake that in respect of licensed operating system if asked for by you in the purchase order, the same shall be supplied along with the authorised license certificate and also that it shall be sourced from the authorised source.

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 the IT hardware / software already billed, we agree to take back the same, if already supplied and return the money if any paid to us by you in this regard.

We **(Vendor name)** also take full responsibility of both parts & service SLA as per the content even if there is any defect by our authorised service centre / reseller / SI etc.

Date	Signature of Authorised Signatory …
Place	Name of the Authorised Signatory …
	Designation …
	Phone & E-mail:
	Name of the Organisation …
	Seal …

11.7. Annexure –VII - Power of Attorney

(Sample Format – To be executed on a non-judicial stamped paper of Rs.100/-)

BY THIS POWER OF ATTORNEY executed on _____, 2015, We _____, a Company incorporated under the Companies Act, 1956, having its Registered Office at _____ (hereinafter referred to as "the Company") doth hereby nominate, constitute and appoint **<Name>, <Employee no.>, < Designation>** of the Company, as its duly constituted Attorney, in the name and on behalf of the Company to do and execute any or all of the following acts, deeds, matters and things, namely :-

- Execute and submit on behalf of the Company a Proposal and other papers / documents with 'Small Industries Development Bank of India' ("SIDBI") relating to 'Request for proposal **No. 400/2016/1152/BYO/ITV dated February 24, 2016** for purchase and installation of network switches, security equipment and to attend meetings and hold discussions on behalf of the Company with SIDBI in this regard.

THE COMPANY DOTH hereby agree to ratify and confirm all whatsoever the attorney shall lawfully do or cause to be done under or by virtue of these presents including anything done after revocation hereof but prior to actual or express notice thereof being received by the person or persons for the time being dealing with the attorney hereunder.

IN WITNESS WHEREOF, _____ has caused these presents to be executed by _____ on the day, month and year mentioned hereinabove.

For and on behalf of the Board of Directors of

_____

WITNESS:
Signature of _____

_____
Attested

_____

11.8. Annexure –VIII -Non Blacklisting

[To be submitted on the letter head of the Company]

Place: _____

Date: _____

To
The General Manager [Systems]
Small Industries Development Bank of India
MSME Development Center, 3rd Floor
Information Technology Vertical
Plot No.C-11, G Block
Bandra Kurla Complex
Bandra [East]
Mumbai 400 051

Dear Sir,

We _____ (bidder name), hereby undertake that:

1. We are not blacklisted by Public Financial Institutions, Public Sector Bank, RBI or IBA or any other Government agencies during the last three years.
2. 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: _____

Company Seal:

11.9. Annexure –IX - EMD / Bid Security Form

(Sample Format – To be executed on a non-judicial stamped paper of requisite value)

To: **SMALL INDUSTRIES DEVELOPMENT BANK OF INDIA**

WHEREAS …….. (Name of Vendor) (hereinafter called the 'the Vendor") has undertaken, in pursuance of Request for Proposal (RFP) No. 400/2016/1152/BYO/ITV Dated February 24, 2016 to supply and implement Network Switches and security equipment for Data Center and DR Site (Herein after called the 'the RFP") to you.

AND WHEREAS, it has been stipulated by you in the said RFP that the Vendor shall furnish you with a Bank Guarantee from a commercial Bank for the sum specified therein, as security for compliance with the Vendor's performance obligations in accordance with the RFP.

AND WHEREAS we ----------Bank having its registered office at ----- and inter alia a branch office situate at ------- have agreed to give a performance guarantee in lieu of EMD of ₹ --------- (Rupees ---------- only) on behalf of the Vendor.

We **----------Bank** further undertake not to revoke and make ineffective the guarantee during it's currency except with the previous consent of the buyer in writing.

We ------ Bank do hereby unconditionally and irrevocably undertake to pay to SIDBI without any demur or protest, merely on demand from SIDBI, an amount not exceeding Rs. ---------- (--------- only).by reason of any breach of the terms of the RFP dated ---- by vendor. We hereby agree that the decision of the SIDBI regarding breach of the terms of the RFP shall be final, conclusive and binding

WE do hereby guarantee and undertake to pay forthwith on demand to SIDBI a sum not exceeding ₹……/-. (Rupees …….. …only) (amount of the Guarantee in words and figures) and we undertake to pay you upon your first written demand declaring the Vendor to be in default under the RFP and without cavil or argument, any sum or sums within the limit of `……/-. (Rupees ……..… only) (Amount of guarantee) as aforesaid, without your needing to prove or to show grounds or reasons for your demand or the sum specified therein.

Our obligation to make payment under this Guarantee shall be a primary, independent and absolute obligation and we shall not be entitled to delay or withhold payment for any reason. Our obligations hereunder shall not be affected by any act, omission, matter or thing which but for this provision might operate to release or otherwise exonerate us from our obligations hereunder in whole or in part, including and whether or not known to us or you:

1. Any time or waiver granted to the vendor;
2. The taking, variation, compromise, renewal or release of or refusal or neglect to perfect or enforce any rights, remedies or securities against the vendor;
3. Any Variation of or amendment to the RFP or any other document or security so that references to the Contract in this Guarantee shall include each such Variation and amendment;
4. any unenforceability, invalidity or frustration of any obligation of the VENDOR or any other person under the RFP or any other document or security waiver by you of any

of the terms provisions conditions obligations UNDER RFP or any failure to make demand upon or take action against the VENDOR;

5. any other fact, circumstance, provision of statute or rule of law which might, were our liability to be secondary rather than primary, entitle us to be released in whole or in part from our undertaking; and;
6. any change in constitution of the vendor;
7. any petition for the winding up of the VENDOR has been admitted and a liquidator or provisional liquidator has been appointed or an order of bankruptcy or an order for the winding up or dissolution of the vendor has been made by a Court of competent jurisdiction;

The written demand referred to in paragraph above shall be deemed to be sufficiently served on us if you deliver to us at the address as set out in paragraph 3.

This guarantee is valid until the …….. day of ……. And a claim in writing is required to be presented to us within six months from i.e. on or before ----all your rights will be forfeited and we shall be relieved of and discharged from all our liabilities mentioned hereinabove.

Signature and Seal of Guarantors (**Vendor's Bank**)
……..

Date…….

Address ……
……
……

11.10. Annexure –X -Non-Disclosure Agreement

(Sample Format – To be executed on a non-judicial stamped paper of Rs.100/-)

WHEREAS, we, _____, having Registered Office at _____, hereinafter referred to as the COMPANY, are agreeable to execute "**Procurement and Implementation of network switches and security equipment**" as per scope defined in the **Request for Proposal (RfP) No.**400/2016/1152/BYO/ITV dated February 24, 2016 for Small Industries Development Bank of India, having its Head office at SIDBI Tower, 15 Ashok Marg, Lucknow, 226001, and office at, MSME Development Centre, Plot No. C-11, G Block, Bandra Kurla Complex (BKC), Bandra (E), Mumbai - 400 051 (hereinafter referred to as the BANK) and,

WHEREAS, the COMPANY understands that the information regarding the Bank's Infrastructure shared by the BANK in their Request for Proposal is confidential and/or proprietary to the BANK, and

WHEREAS, the COMPANY understands that in the course of submission of the offer for the said RfP and/or in the aftermath thereof, it may be necessary that the COMPANY may perform certain jobs/duties on the Bank's properties and/or have access to certain plans, documents, approvals, data or information of the BANK;

NOW THEREFORE, in consideration of the foregoing, the COMPANY agrees to all of the following conditions, in order to induce the BANK to grant the COMPANY specific access to the BANK's property/information, etc.;

The COMPANY will not publish or disclose to others, nor, use in any services that the COMPANY performs for others, any confidential or proprietary information belonging to the BANK, unless the COMPANY has first obtained the BANK's written authorisation to do so;

The COMPANY agrees that information and other data shared by the BANK or, prepared or produced by the COMPANY for the purpose of submitting the offer to the BANK in response to the said RfP, will not be disclosed to during or subsequent to submission of the offer to the BANK, to anyone outside the BANK;

The COMPANY shall not, without the BANK's written consent, disclose the contents of this Request for Proposal (Bid) or any provision thereof, or any specification, plan, pattern, sample or information (to be) furnished by or on behalf of the BANK in connection therewith, to any person(s) other than those employed/engaged by the COMPANY for the purpose of submitting the offer to the BANK and/or for the performance of the Contract in the aftermath. Disclosure to any employed/ engaged person(s) shall be made in confidence and shall extend only so far as necessary for the purposes of such performance.

Yours sincerely,

Authorized Signatories

Name: _____

Designation: _____

Company Seal:

11.11. Annexure –XI –Pre Contract Integrity Pact

(To be submitted by bidders on letter head. Shortlisted bidders to submit on non-judicial stamp paper of Rs.100/-.)

1 General

This pre-bid-pre-contract Agreement (hereinafter called the Integrity Pact) is made at _____ place___ on ---- day of the month of -----, 2015 between Small Industries Development Bank of India, having its Head Office at 15, Ashok Marg, Lucknow – 226001 and inter alia, its Corporate Office at MSME Development Centre, C-11, G-Block, Bandra-Kurla Complex, Bandra(E), Mumbai 400051 (hereinafter called the "BUYER"/SIDBI, which expression shall mean and include, unless the context otherwise requires, its successors and assigns) of the First Part and M/s --- represented by Shri ----, Chief Executive Officer (hereinafter called the "BIDDER/Seller" which expression shall mean and include, unless the context otherwise requires, his successors and permitted assigns) of the Second Part.

WHEREAS the BUYER proposes to shortlist vendor for carrying out Procurement and Implementation of Network Switches and security equipment for Data Center and DR site and the BIDDER/Seller is willing to offer/has offered the services and

WHEREAS the BIDDER is a private company/public company/Government undertaking/partnership/ registered export agency, constituted in accordance with the relevant law in the matter and the BUYER is a corporation set up under an Act of Parliament.

NOW, THEREFORE,

To avoid all forms of corruption by following a system that is fair, transparent and free from any influence /prejudiced dealing prior to, during and subsequent to the currency of the contract to be entered into with a view to :-

- Enabling the BUYER to obtain the desired said stores/equipment/services at a competitive price in conformity with the defined specifications by avoiding the high cost and the distortionary impact of corruption on public procurement and
- Enabling BIDDERs to abstain from bribing or indulging in any corrupt practice in order to secure the contract by providing assurance to them that their competitors will also abstain from bribing and other corrupt practices and the BUYER will commit to prevent corruption in any form by its officials by following transparent procedures.

The parties hereto hereby agree to enter into this integrity Pact and agree as follows:

2 Commitments of the BUYER

2.1 The BUYER undertakes that no official of the BUYER, connected directly or indirectly with the contract, will demand, take a promise for or accept, directly or through intermediaries, any bribe, consideration, gift, reward, favour or any material or immaterial benefit or any other advantage from the BIDDER, either for themselves or for any person, organization or third party related to the contract in exchange for an advantage in the bidding process, bid evaluation, contracting or implementation process related to the contract.

2.2 The BUYER will during the pre-contract stage, treat all BIDDERs alike, and will provide to all BIDDERs the same information and will not provide any such information to any particular BIDDER which could afford an advantage to that particular BIDDER in comparison to other BIDDERs.

2.3 All the officials of the BUYER will report to the appropriate Government office any attempted or completed breaches of the above commitments as well as any substantial suspicion of such a breach.

2.4 In case any such preceding misconduct on the part of such official(s) is reported by the BIDDER to the BUYER with full and verifiable facts and the same is prima facia found to be correct by the BUYER, necessary disciplinary proceedings, or any other action as deemed fit, including criminal proceedings may be initiated by the BUYER and during such a period shall be debarred from further dealings related to the contract process. In such a case while an enquiry is being conducted by the BUYER the proceedings under the contract would not be stalled.

3 Commitments of BIDDERs

The BIDDER commits itself to take all measures necessary to prevent corrupt practices, unfair means and illegal activities during any stage of its bid or during any pre-contract or post-contact stage in order to secure the contract or in furtherance to secure it and in particular commit itself to the following : -

3.1 The BIDDER will not offer, directly or through intermediaries, any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any officials of the BUYER, connected directly or indirectly with bidding process, or to any person, organization or third party related to the contract in exchange for any advantage in the bidding, evaluation, contracting and implementation of the contract.

3.2 The BIDDER further undertakes that it has not given, offered or promised to give, directly or indirectly any bribe , gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the BUYER or otherwise in procuring the Contract or forbearing to do or having done any act in relation to the obtaining or execution of the contract or any other contract with the Government for showing or forbearing to show favour or disfavor to any person in relation to the contract or any other contract with the Government.

3.3 BIDDERs shall disclose the name and address of agents and representatives and Indian BIDDERs shall disclose their foreign principals or associates.

3.4 BIDDERs shall disclose the payments to be made by them to agents/brokers or any other intermediary, in connection with this bid/contract.

3.5 The BIDDER further confirms and declares to the BUYER that the BIDDER is the original manufacture/integrator/authorized government sponsored export entity of the defence stores and has not engaged any individual or firm or company whether Indian or foreign to intercede, facilitate or any way to recommend to the BUYER or any of its functionaries, whether officially or unofficially to the award of the contract to the BIDDER , or has any amount been paid, promised or intended to be paid to any such individual, firm or company in respect of any such intercession, facilitation or recommendation.

3.6 The BIDDER, either while presenting the bid or during pre-contract negotiations or before signing the contract, shall disclose any payments he has made, is committed to or intends to make to officials of the BUYER or their family members, agents, brokers or any other intermediaries in connection with contract and the details of services agree upon for such payments.

3.7 The BIDDER will not collude with other parties interested in the contract to impair the transparency, fairness and progress of the bidding process, bid evaluation, contracting and implementation of the contract.

3.8 The BIDDER will not accept any advantage in exchange for any corrupt practice, unfair means and illegal activities.

3.9 The BIDDER shall not use improperly, for purposes of competition or personal gain or pass on the others, any information provided by the BUYER as part of the business relationship, regarding plans, technical proposals and business details, including information contained in any electronic data carrier. The BIDDER also undertakes to exercise due and adequate care lest any such information is divulged.

3.103BIDDER commits to refrain from giving any complaint directly or through any other manner without supporting it with full and verifiable facts.

3.11The BIDDER shall not instigate or cause to instigate any third person to commit any of the actions mentioned above.

3.12if the BIDDER or any employee of the BIDDER or any person acting on behalf of the BIDDER, either directly or indirectly, is a relative to any of the officers of the BUYER or alternatively, if any relative of the officer of the BUYER has financial interest/stake in the BIDDER's firm , the same shall be disclosed by the BIDDER at the time of filling of tender.

The term 'relative' for this purpose would be as defined in Section 2 (77) of the Companies Act, 2013.

3.13The BIDDER shall not lend to or borrow any money from or enter into any monetary dealings or transactions, directly or indirectly, with any employee of the BUYER.

4 Previous Transgression

4.1 The BIDDER declares that no previous transgression occurred in the last three years immediately before signing of this integrity Pact, with any other company in any country in respect of any corrupt practices envisaged hereunder or with any Public Sector Enterprise in India or any Government Department in India that could justify BIDDER's exclusion from the tender process.

4.2 The BIDDER agrees that if it makes incorrect statement on this subject, BIDDER can be disqualified from the tender process or the contract, if already awarded, can be terminated for such reason.

5 Earnest Money (Security Deposit)

5.1 While submitting commercial bid, the BIDDER shall deposit an amount **Rs.1,50,000/-** as Earnest Money/Security Deposit, with the BUYER through any of the following instrument.

(i) Bank Draft or a Pay Order in favour of Small Industries Bank of India, Payable at Mumbai.

(ii) A confirmed guarantee by an Indian Nationalised Bank, promising payment of the guaranteed sum to the BUYER immediately on demand without any demur whatsoever and without seeking any reasons whatsoever. The demand for payment by the BUYER shall be treated as conclusive proof of payment.

5.2 Earnest Money/Security Deposit shall be valid till the date of bid validity as mentioned in the RfP.

5.3 In case of the successful BIDDER a clause would also be incorporated in the Article pertaining to Performance Bond in the Purchase Contract that the provision of Sanctions for Violation shall be applicable for forfeiture of Performance Bond in case of a decision by the BUYER to forfeit the same without assigning any reason for imposing sanction for violation of this Pact.

5.4 No interest shall be payable by the BUYER to the BIDDER on Earnest Money/Security Deposit for the period of its currency.

6 **Sanctions for Violations**

6.1 Any breach of the aforesaid provision by the BIDDER or any one employed by it or acting on its behalf (whether with or without the knowledge of the BIDDER) shall entitle the BUYER to take all or any one of the following actions, wherever required :-

i. To immediately call off the pre contract negations without assigning any reason or giving any compensation to the BIDDER. However, the proceedings with other BIDDER(s) would continue

ii. The Earnest Money Deposit (in pre-contract stage) and /or Security Deposit/Performance Bond) (after the contract is signed) shall stand forfeited either fully or partially, as decided by the BUYER and the BUYER shall not be required to assign any reason therefore.

iii. To immediately cancel the contract, if already signed, without giving any compensation to the BIDDER

iv. To recover all sums already paid by the BUYER, and in case of Indian BIDDER with interest thereon at 2% higher than the prevailing Prime Lending Rate of State Bank of India, while in case of a bidder from a country other than India with interest thereon at 2% higher than LIBOR. If any outstanding payment is due to the bidder from the buyer in connection with any other contract for any other stores, such outstanding payment could also be utilized to recover the aforesaid sum and interest.

v. To encash the advance bank guarantee and performance bond/warranty bond, if furnished by the BIDDER, in order to recover the payments, already made by the BUYER alongwith interest.

vi. To cancel all or any other Contracts with the BIDDER, the BIDDER shall be liable to pay compensation for any loss or damage to the BUYER resulting from such cancellation/rescission and the BUYER shall be entitled to deduct the amount so payable from the money(s) due to the BIDDER

vii. To debar the BIDDER from participating in future bidding processes of the buyer or its associates or subsidiaries for minimum period of five years, which may be further extended at the discretion of the BUYER.

viii. To recover all sums paid in violation of this Pact by BIDDER(s) to any middleman or agent or broker with a view to securing the contract.

ix. In cases where irrevocable Letters of Credit have been received in respect of any contract signed by the BUYER with BIDER, the same shall not be opened.

x. Forfeiture of Performance Bond in case of decision by the BUYER to forfeit the same without assigning any reason for imposing sanction for violation of this Pact.

6.2 The BUYER will be entitled to take all or any of the actions mentioned at para 6.1(i) to (x) of this Pact also on the commission by the BIDDER or any one employed by it or acting on its behalf (whether with or without the knowledge of the BIDDER), of an offence as defied in Chapter IX of the Indian Penal code, 1860 or Prevention of Corruption Act, 1988 or any other statute enacted for prevention of corruption.

6.3 The decision of the BUYER to the effect that a breach of the provision of this Pact has been committed by the BIDDER shall be final and conclusive on the BIDDER. However, the BIDDER can approach the independent Monitor(s) appointed for the purposes of this Pact.

7 **Fall Clause**

7.1 The BIDDER undertakes that it has not supplied/is not supplying similar products /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 and if it is found at any stage that similar product/systems or sub systems was supplied by the BIDDER to any other Ministry/Department of the Government of India or a PSU at a lower price, then that very price, with due allowance for elapsed time, 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.

8 Independent Monitors

8.1 The BUYER is in the process of appointing Independent Monitors (hereinafter referred to as Monitors) for this Pact in consultation with the Central Vigilance Commission.

8.2 The task of the Monitors shall be to review independently and objectively, whether and to what extent the parties comply with the obligations under this Pact.

8.3 The Monitors shall not be subject to instruction by the representatives of the parties and perform their functions neutrally and independently.

8.4 Both the parties accept that the Monitors have the right to access all the documents relating to the project/procurement, including minutes of meetings.

8.5 As soon as the Monitor notices or has reason to believe, a violation of the Pact, he will so inform the Authority designated by the BUYER

8.6 The BIDDER(s) accepts that the Monitor has the right to access without restriction to all Project documentation of the BUYER including that provided by the BIDDER. The BIDDER will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documents. The same is applicable to Subcontractors. The Monitor shall be under contractual obligation to treat the information and documents of the BIDDER/Subcontractor(s) with confidentiality

8.7 The BUYER will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the parties. The parties will offer to the Monitor the option to participate in such meetings

8.8 The Monitor will submit a written report to the designed Authority of the BUYER within 8 to 10 weeks from the date of reference or intimation to him by the BUYER/BIDDER and should the occasion arise, submit proposals for correcting problematic situations.

9 Facilitation of Investigation

In case of any allegation of violation of any provision of this Pact or payment of commission, the BUYER or its agencies shall be entitled to examine all the documents including the Books of Accounts of the BIDDER and the BIDDER shall provide necessary information and documents in English and shall extend all possible help for the purpose of such examination.

10 Law and Place of Jurisdiction

This Pact is subject to Indian Law. The place of performance and jurisdiction is the seat of the BUYER.

11 Other Legal Actions

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

12 Validity

12.1 The validity of this Integrity Pact shall be from date of its signing and extend upto 5 years or the complete execution of the contract to the satisfaction of both the BUYER and the BIDDER/Seller, including warranty period, whichever is later in case BIDDER is unsuccessful, this integrity Pact shall expire after six months from the date of the signing of the contract.

12.2 Should one or several provisions of the Pact turn out to be invalid, the remainder of this Pact shall remain valid. In this case, the parties will strive to come to an agreement to their original intentions.

13 The parties hereby sign this integrity Pact, at _____ on _____

BUYER	BIDDER
Name of the Officer	
Designation	CHIEF EXECUTIVE OFFICER
SIDBI	
Witness	Witness
1._____	1._____
2._____	2._____

11.12. Annexure –XII -Statement of Deviations

Bidder is required to provide details of all deviations, comments and observations or suggestions in the following format with seal and signature. It also needs to provide a reference of the page number, state the clarification point as stated in tender document and the comment/ suggestion/ deviation that you propose as shown below.

SIDBI may at its sole discretion accept or reject all or any of the deviations, however it may be noted that the acceptance or rejection of any deviation by SIDBI will not entitle the bidder to submit a revised commercial bid. **Clarifications given in Pre-bid will not be further entertained.**

S.N.	Page Number	Section Number	Clarification point as stated in the tender document	Comment/ Suggestion/ Deviation
1.				
2.				
3.				
4				
5				
6				

Signature of Authorised Signatory …

Date

Place

Name of the Authorised Signatory …

Designation …

Name of the Organisation …

Seal …

11.13. Annexure –XIII –Bank Mandate Form

(To be submitted in Duplicate)

Please fill in the information in CAPITAL LETTERS. Please TICK wherever it is applicable)

1. Name of Borrower / vendor / supplier: _____

2. Vendor Code (if applicable):_____

3. Address of the Borrower / vendor / supplier:_____

_____

City _____ Pin Code _____ E-mail id:_____

Phone No. with STD code:_____ Mobile:No.: _____

Permanent Account Number _____

MSE Registration / CA Certificate (if applicable):_____

3. Particulars of Bank account:

Beneficiary Name			
Bank Name		Branch Name	
Branch Place		Branch City	
PIN Code		Branch Code	
MICR No.			
Account type	Saving	Current	Cash Credit
Account No.	(As appearing in the Cheque book)		
(Code number appearing on the MICR1 cheque supplied by the Bank. Please attach a cancelled cheque of your bank for ensuring accuracy of the bank name, branch name & code and Account Number)			
IFSC CODE2	For RTGS transfer		For NEFT transfer

4. Date from which the mandate should be effective :

I hereby declare that the particulars given above are correct and complete. If any transaction is delayed or not effected for reasons of incomplete or incorrect information, I shall not hold SIDBI / IDBI Bank responsible. I also undertake to advise any change in the particulars of my account to facilitate updation of records for purpose of credit of amount through **RBI RTGS/NEFT**.

Place : _____
Date : _____

Signature of:
the party / Authorized Signatory

……

Certified that particulars furnished above are correct as per our records.

Bank's stamp :
Date :

[Signature of Authorized Official from the Bank]

N.B.: RTGS/NEFT charges if any, is to be borne by the party

1, 2: Note on IFSC / MICR

Indian Financial System Code (IFSC) is an alpha numeric code designed to uniquely identify the bank-branches in India. This is 11 digit code with first 4 characters representing the bank's code, the next character reserved as control character (presently 0 appears in the fifth position) and remaining 6 characters to identify the branch. The MICR code, (Magnetic Ink Character Recognition) that appears on cheques, has 9 digits to identify the bank-branch. RBI had since advised all the banks to print IFSC on cheque leaves issued to their customers. A customer may also contact his bank-branch and get the IFS Code of that branch.

****

11.14. Annexure –XIV- Performance Guarantee Format

(Sample Format – To be executed on a non-judicial stamped paper of requisite value)

KNOW ALL MEN BY THESE PRESENTS that in consideration of the Small Industries Development Bank of India (SIDBI), a Corporation constituted and established under the Small Industries Development Bank of India Act, 1989, and having its Head Office at SIDBI Tower, 15 Ashok Marg, Lucknow, 226001, and office at 3rd Floor, SME Development Centre, Plot No. C-11, G Block, Bandra Kurla Complex (BKC), Bandra (E), Mumbai - 400 051 (hereinafter called the Corporation) having agreed to accept from M/s. 'Vendor Name' having its office at 'Vendor's Office Address', (hereinafter called "the Vendor") an agreement of guarantee for Rs. _____ (Rupees _____ only), for the due fulfillment by the vendor of the terms and conditions of the Purchase order No. _____ dated _____ made between the vendor and the Corporation for providing services for SIDBI's 'Project Details' hereinafter called "the said Agreement").

1. We, Bank (Bank Name and Details), do hereby undertake to indemnify and keep indemnified the Corporation to the extent of Rs. _____ (Rupees _____ only) against any loss or damage caused to or suffered by the Corporation during warranty period by reason of any breach by the Vendor of any of the terms and conditions contained in the said Agreement of which breach the opinion of the Corporation shall be final and conclusive.

2.And we Bank (Bank Name and Details), do hereby guarantee and undertake to pay forthwith on demand to the Corporation such sum not exceeding the said sum of Rs. _____ (Rupees _____ only) only as may be specified in such demand, in the event of the vendor failing or neglecting to execute fully efficiently and satisfactorily the order for implementation services for the 'Project Details' placed with it (the work tendered for by it) within the period stipulated in the said Agreement in accordance with the design, specification, terms and conditions contained or referred to in the said Agreement or in the event of the Vendor refusing or neglecting to maintain satisfactory operation of the equipment or work or to make good any defect therein notified by the Corporation to the vendor during the warranty period or otherwise to comply with and conform to the design, specification, terms and conditions contained or referred to the said Agreement.

3. We, Bank (Bank Name and Details), further agree that the guarantee herein contained shall remain in full force and effect during the period that would be taken for the performance of the said order as laid down in the said agreement including the "Warranty obligations" or till validity date of this guarantee i.e. upto _____, whichever is earlier and subject to the terms of the "the said Agreement" it shall continue to be enforceable for the breach of warranty conditions within warranty period and till all the defects notified by the Corporation to the vendor during the warranty period have been made good to the satisfaction of Corporation & the Corporation or its authorized representative certified that the terms and conditions of the said agreement have been fully and properly complied with by the vendor or till validity of this guarantee i.e _____, whichever is earlier.

4. We, Bank (Bank Name and Details), may extend the validity of Bank Guarantee at the request of the Vendor for further period or periods from time to time beyond its present validity period, but at our sole discretion.

5. The liability under this guarantee is restricted to Rupees _____/- only and will expire on _____ and unless a claim in writing is presented to us at Bank (Bank Name and Details) within 3 months from _____ , i.e. on or before _____, all your rights will be forfeited and we shall be relieved of and discharged from all our liabilities there-under.

6. The Guarantee herein contained shall not be determined or affected by Liquidation or winding up or insolvency or closure of the Vendor.

7. The executant has the power to issue this guarantee and executants on behalf of the Bank and hold full and valid Power of Attorney granted in their favour by the Bank authorising them to execute this guarantee.
Notwithstanding anything contained here in above, our liability under this guarantee is restricted to Rs. _____ (Rupees _____ only). Our guarantee shall remain in force until _____. Our liability hereunder is conditional upon your lodging a demand or claim with Bank (Bank Name and Details) on or before _____. Unless a demand or claim is lodged with Bank (Bank Name and Details) within the aforesaid time, your rights under the guarantee shall be forfeited and we shall not be liable there under. This guarantee shall be governed by and construed in accordance with the laws of India. All claims under this guarantee will be made payable at Bank (Bank Name and Details). This Guarantee will be returned to the Bank when the purpose of the guarantee has been fulfilled or at its expiry, which ever is earlier.

We, Bank (Bank Name and Details) lastly undertake not to revoke this guarantee during its currency except with the previous consent of the Corporation in writing.

In witness where of we ..... have set and subscribed our hand and seal this .....day of .....2015 .

SIGNED, SEALED AND DELIVERED.
BY
AT
IN THE PRESENCE OF WITNESS :

1) Name .....
Signature.....
Designation.....

2) Name.....
Signature.....
Designation.....

END OF RFP