Government of India
Ministry of Science and Technology
Department of Science and Technology
NRDMS & NSDI Division
East block -7, Level-5, Sector-1, R.K. Puram New Delhi-110066

Open Tender No.2/9/2016-NSDI Dated: 13 October, 2017

To

All Eligible Vendors

SUBJECT: SUPPLY AND INSTALLATION OF ROUTER, FIREWALL,IDPS and LAN SWITCH ETC. AT NSDI, DST

National Spatial Data Infrastructure (NSDI), DST on behalf of the President of India invites on-line quotations on CPP website (https://eprocure.gov.in) from eligible vendors for supply and installation of items like Router, Firewall, IDPS and LAN switch etc. as a comprehensive networking and security solution for its Geo-portal Infrastructure and Geo Web Services. Details of the equipment are given at Annex–I and item-wise related specifications are given at Annex-II. All the eligible vendors are requested to submit quotations for the items mentioned in Annex-I as per the specifications given at Annex-II.

2. The General Terms and Conditions for submitting the quotations are available overleaf. The biding procedure shall be a single stage - two bid system and bid documents are to be prepared in two parts as under: -
Part-1 (Technical Bid)
Part-II (Price Bid)

3. Part-1 (Technical Bid) - The technical bid shall comprise of the following: -
3.1 Name of the Firm, Address, and its registration and taxation details with all credentials
3.2. Details of credentials in support of qualification criteria as mentioned in General Terms and Conditions
3.3 Technical details as per Annex I and II
3.4 Scanned copies of Tender Fee and EMD
3.5 Authorised Dealership certificate, if the firm is an authorised dealer of the items.
3.6 Methodology and Implementation Plan at NSDI
3.7 Any other relevant information that the firm deems it fit to provide.

4. Part-2 (Price Bid) The price bid should be submitted in an Excel file as per the enclosed BOQ format with the tender document in the CPP Portal.

5. Firms or their authorized representatives can attend the opening of the bids at NSDI office at the specified time of opening of the tender. The authorized representative attending the process of opening of tender should carry with him/ possess the authorization letter from the firm. They could also view the on-line quotation opening process at their premises.

6. The Tender will be evaluated as per the Terms and Conditions mentioned herein.

7. The Tender fee is Rs. 1000/- (Rupees One Thousand only) which is required to be submitted

by post/ through Firm Representative preferably before the date fixed for opening of the quotations in the form of demand draft in favour of DDO (Cash), Department of Science and Technology payable at New Delhi.

8. The Tender can be obtained from the NSDI Office without cost before the due date of submission. The Tender document can also be downloaded from DST website www.dst.gov.in or NSDI website www.nsdiindia.gov.in or the CPP website.

9. EMD: Earnest money amounting to Rs.1,00,000/- (Rupees One Lakh Only) in the form of Bankers Cheque/ Account Payee Demand Draft of Nationalized Bank/ Commercial Bank drawn in favour of D.D.O (Cash), Department of Science & Technology is required to be submitted by post/through representative preferably before the date fixed for opening of the quotations.

10. SECURITY DEPOSIT: The successful Tenderer shall furnish the security deposit to DST within 2 weeks after placement of order at the rate of 10% of the order value, failing which the EMD will be forfeited automatically, without any notice. Detailed information on security deposit may be seen at the General Terms and Conditions of the Tender.

11. NSDI, DST reserves the right to amend or withdraw any of the Terms and Conditions contained in the Tender Document or to reject any or all the tenders as a whole or in part without giving any notice or assigning any reason thereto.

12. The Addendum/ Corrigendum if any will be uploaded on the aforesaid websites of the Department or the CPP. NSDI may arrange pre-bid meeting(s), if necessary, on the basis of requests received from interested vendors within 7 working days of the publication of this tender. Date of pre-bid meeting will be announced on the NSDI website. No individual communication will be made with the vendor for this purpose.

Note:

The Last date of submission of Tender – 16 November, 2017
The Date of Opening of the Tender – 1100 hrs on 20 November 2017

Sd/-
(Agusthia Minj)
Under Secretary to Government of India
National Spatial Data Infrastructure (NSDI)
Department of Science and Technology, New Delhi
Phone: 011- 26182973, 011-26177249
Fax: 011- 26169135

Copy to:
DST/NSDI: For posting the complete Tender Document on Department's website www.nsdiindia.gov.in or www.dst.gov.in or www.eprocure.gov.in and participating firms may download the complete document and the same may be used for submission of bids along with the tender cost of Rs.1000.

GENERAL TERMS AND CONDITIONS

SUPPLY AND INSTALLATION OF ROUTER, FIREWALL, IDPS & LAN SWITCH ETC. AT NSDI, DST

A. The online quotation should be submitted on or before the specified date in the enquiry letter addressed to the Under Secretary, NSDI, Level-5, East block -7, Sector-1, R.K. Puram, New Delhi-110066.

THE COVER SHOULD BE SUPERSCRIBED WITH THE FOLLOWING

"SUPPLY AND INSTALLATION OF ROUTER, FIREWALL, IDPS and LAN SWITCH ETC."

B. This office takes no responsibility for delay, loss or non-receipt of quotations/ documents sent by post whereas reserves the right to accept or reject any part of the tender without assigning any reason.

C. Corrections if any must be attested. All rates shall be indicated both in words as well as in figures, where there is a difference between rates quoted in words and figures, rate quoted in words will prevail. The firm has to submit the signed copy of the Terms and Conditions along with the quotation. The submission is for the acceptance of the general terms and conditions without which the quote would be rejected.

D. EMD: Earnest money amounting to Rs.1,00,000/- (Rupees One Lakh Only) in the form of Banker's Cheque/ Account Payee Demand Draft of Nationalized Bank/ Commercial Bank drawn in favour of D.D.O., Department of Science & Technology should accompany the tender. Tender without EMD shall be summarily rejected (EMD exemption is applicable for those who are registered with DGS&D for the said items). The earnest money should initially be valid up to 60 days beyond period of bid validity. The earnest money of unsuccessful bidders will be returned on finalization of tender. The earnest money of successful bidders will be returned on receipt of Security Deposit or it may be adjusted in the security deposit if requested by the tenderer.

E. SECURITY DEPOSIT: The successful tenderer shall furnish the security deposit within 2 weeks after placement of order at the rate of 10% of the order value, failing which the EMD will be forfeited automatically, to DST, without any notice. The security deposit shall be furnished in the form of Demand Draft/ Bank Guarantee drawn in the favour of DDO, Department of Science & Technology and should be valid for 27 months. The security deposit will be returned in full on completion of successful guarantee/ warranty period.

F. RIGHT OF ACCEPTANCE: This office reserves the right to reject the lowest tender or any or all the tenders without assigning any reason whatsoever.

G. QUOTATIONS VALIDITY: Quotation should be valid for a minimum period of six months after the date of publication of tender.

H. QUALIFICATION CRITERIA FOR VENDOR

- Vendor should be either original equipment manufacturer or authorized dealer of reputed and established brand manufacturer. The original manufacturer/ authorized dealership certificate duly should be signed and submitted by post/ through representative before fixed date of opening of quotation. Organisation details may also be provided as per the format of FORM-4 enclosed at Annexure V.
- Vendor/ OEM should have been dealing in the Networking and Security Solutions for the past five years and should have supplied the same to any Ministry/Govt. Department/Autonomous bodies. (Work order is to be attached). details may also be provided as per the format of FORM-1 & FORM-2 enclosed at Annexure V.
- Vendor/OEM should not have been debarred or blacklisted by any Central / State Government Departments in India. A self-declaration is to be attached.
- Details of Technical and Administrative manpower may be provided as per the format FORM-3 enclosed at Annexure V.

I. EVALUATION CRITERIA .

The Solution proposed by the pre-qualified vendors will be technically evaluated by NSDI Technical Evaluation Committee. The Technical Committee has full rights to set the Technical Evaluation Criteria as per the national standards. The Committee also have the full rights to accept/ overrule any deviation in the technical specifications mentioned in Annex-II.

The Committee may ask the vendors to demonstrate the Proof of Concept(PoC) of the proposed network Security Solution. The vendor is responsible for creating virtual or real environment to demonstrate the technical capability of his solution proposed. For the evaluation purposes , the marking scheme will be as per the details enclosed at Annexure- IV . On completion of the technical evaluation, financial bids of the technically- qualified tenders who secure more than 70% cut off marks, will be eligible for opening and evaluation for selection of the final bidder.

J. QUALIFYING BID: The technically qualified tender who quotes the lowest bundle cost will be declared as qualifier on the basis of L1 provided the bidder has submitted all the required documents mentioned in the tender document.

K. GUARANTEE TERMS: The tenderer should provide warrantee/guarantee for minimum THREE YEARS with on-site training and support. Any part failing during the warranty/ guarantee period shall be repaired /replaced/installed free of charge by the supplier at the installation site.

L. PRICE & STATUATORY DUTIES:

1. The price quoted in BOQ should exclude all taxes.

2. No additional/separate cost for installation, commissioning, licensing, maintenance etc will be considered. The tender will be evaluated on the basis of the lowest bundle of cost amongst the technically qualified bidders.

3. GST/ Sales tax and / or other duties and levies where legally leviable and intended to be claimed should be distinctly and separately mentioned in the quotation. Where it is not done, no claim for Sales Tax / Service Tax will be admitted at any later stage and on no ground whatsoever.

4. GST/VAT/CST registration No. and date of its validity should be mentioned.

5 This office will not issue any Form such as ‘C’, ‘D’ etc.

M. DESPATCH INSTRUCTIONS: The firm will dispatch the materials by road under insurance cover and freight paid by tenderer.

N. DELIVERY PERIOD: Materials should be supplied by the tenderer within 2 weeks from the date of issue of purchase order at NSDI, Level 5, East Block 7, Sector 1, R.K.Puram, New Delhi - 110066.

O. LATE DELIVERY CHARGS: If the delivery of the material is delayed by more than the specified time, 0.5% of the total amount will be charged per week subject to maximum of 10% of the ordered value.

P.PAYMENT TERMS:

1. Payment will be made after completion of supply, installation & testing of the items and submitting the invoice. No advance payment will be made.

2. Payment will be in Indian Rupees.

3. Payment will be made in the name of the Company.

Q. ADDITIONAL/REDUCED QUANTITY: NSDI reserves the right to place order for additional/ reduced quantity of the ordered quantity at the same rates and terms and conditions till the validity of the quotation.

R. The tender should have valid Sales Tax/Service tax number. It is required to mention Sales Tax/Service tax Numbers and enclose a copy of the registration.

S.DOCUMENTATION: One copy each of operational and service manuals shall be supplied along with the equipment in the event of order being placed. All associated software should be supplied in original CD/DVD licensed to NSDI along with one set of Hard copy document on operational methods.

T. ENCLOSURES:

The firm must submit the following enclosures along with the tender.

1. Financial bid with all quoted items as per excel format enclosed.

2. Technical manuals/ detailed technical literature/ catalogues for all the offered products.

3.Signed copy of General Terms & Conditions and Vendor’s certificate for compliance with General Functional Requirement for Networking & Security Solutions at NSDI as per Annex-II by the authorized person. Printed terms and conditions of tendering firms will not be considered as forming a part of their tender.

5. Any other document mentioned elsewhere in the tender document.

6. The tender is liable to be rejected in the absence of the above enclosures with the sole responsibility of the tenderer.

U. The tender document can be obtained from the Section Officer (NSDI)/ Surveyor (NSDI), R. K. Puram, New Delhi on any working day between 10.30 AM to 04:30 PM. before the tender closing time. Tender documents can also be downloaded from the NSDI's website www.nsdiindia.gov.in or Department's website www.dst.gov.in or the CPP website and used for submitting the bids along with the fee of tender cost.

***

SUPPLY AND INSTALLATION OF ROUTER, FIREWALL, IDPS & LAN SWITCH AT ETC. NSDI, DST

CHECK LIST

Please ensure to check the following before submitting the quotations as otherwise the quotations are liable to summary rejection.

1	PRICE	Prices quoted both in figures and words are correct. However prices quoted in words will prevail, if there is any difference
2	VALIDITY	For a minimum of six months
3	PAYMENT TERMS	No advance will be provided, payments will be made after receipt of the materials in good working condition and satisfactory performance after installation as acceptable to this office.
4	DELIVERY PERIOD	Material should be delivered within 2 weeks from the date of supply order
5	PAKAGING/FORWARDING CHARGES	Should be clearly indicated. Mentioning "EXTRA" will not be acceptable. Delivery is to be made at NSDI, RK Puram, New Delhi – 110066.
6	LAVIES/TAXES	Levis/Taxes if any are to be clearly mentioned.
7	TRANSIT INSURANCE	Clearly indicate as per clause "L" of GTC
8	ENCLOSURE	As per clause "S" of GTC
9	PAN/TIN	REGISTRATION COPY OF GST, PAN, TIN, ST TO BE ENCLOSED
10	DUE DATE	16.11.2017
11	OPENING DATE/TIME	20.11.2017

Annex-I

Quantity, Scope of Work for Networking & Security Solutions at NSDI, New Delhi

A. Supply , installation and commissioning of Router, Firewall, IDPS , Database Security and Server Security Solutions along with Lan Switch as a bundle of security solutions for NSDI as per format given below:

S. No.	Item	Description (Make, Model Number, Brochure & data sheet may	Qty.	Remarks
1	Router	As at Annex II	2	
2	Firewall	As at Annex II	2	
3	IDPS	As at Annex II	2	
4	LAN Switch	As at Annex II	2	
5	Database Security Solution	As at Annex II	2 User	
6	Endpoint Threat Protection solution for Servers and Desktops	As at Annex II	6 User	
7	Server (Quadcore 3 GHz CPU, 16GB RAM, 500GB Hard- disk, Windows 2012) with all necessary peripherals i.e TFT Screen,Key Board, Mouse	As at Annex II	1	

B. One time configuration and operationalization of all the equipment as per the requirements of NSDI.

C. Supplied equipment shall be configured and integrated to work for all functions as mentioned above, with the existing equipment in the network. Therefore bidder will specifically ensure the interoperability before quoting a particular model of any equipment.

D. Implementation of controls network traffic & security with advanced features.

E. Customization of existing security policies with all new enhanced security features of supplied equipment.

F. Intuitive Browser based tools for easy setup and management and consistent features across all equipment to simplify setup and configuration.

G. Operational Training to NSDI officials.

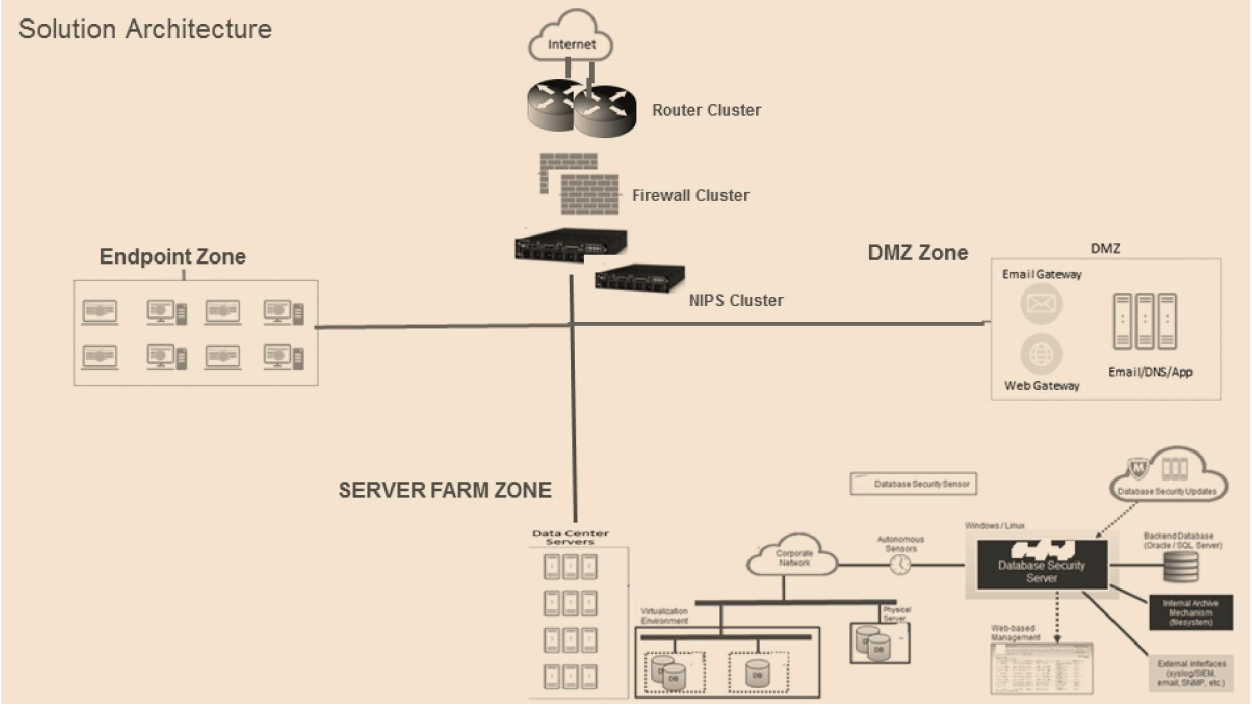
H. Once the integrated setup is functional and tested for all features, the complete layout document will be prepared and submitted by the bidder. The agency or its representative will provide all the data/configuration files necessary for integration with the existing Network with respect to the above scope.

I. The OEM warranty of the Equipment supplied shall be for 3 Years (on-site) from the date of commissioning of the complete network. The warranty shall include all software licenses, subscription, updates and upgrades for 3 years.

J. OEM shall provide incident response services for 3 year along with solution proposed.

<u>System Integration:</u> The layout drawing of the system integration is as detailed below for reference of the tenderer/bidder and it shall be the responsibility of the tenderer/bidder to provide all the equipment and related accessories at his own cost for the required system integration.

<u>Proposed Solution Architecture-</u>



a) Proposed solution architecture should consist of Router, Firewall and NIPS in cluster active-active configuration.

b) Proposed architecture should have 3 zones- DMZ Zone, Server Farm Zone (presently 6 Windows 2012 servers and one database instance) and Endpoint Zone.

c) Proposed solution for Server & Database security management should consist of single separate management hardware with minimum below mentioned configuration- Quadcore 3 GHz CPU, 16GB RAM, 500GB Hard-disk, Windows 2012 OS with SQL2008/oracle 11g/12c database

Annex-II

A. General Functional Requirement for Networking & Security Solution at NSDI

S.No.	Details	Compliance (Yes/No)	Deviation (If Any)/Remarks
1	Proposed solution must provide comprehensive visibility into and control over activity within the network. Such visibility includes users, devices, vulnerabilities, threats, client-side applications, files, and web sites. Holistic, actionable indications of compromise (IoCs) correlate detailed network and endpoint event information and provide further visibility into malware infections. Should also provide content awareness with malware file trajectory that aids infection scoping and root cause determination to speed time to remediation		
2	Proposed solution must have on device Management Center that continuously monitors how the network is changing over time. New threats are automatically assessed to determine which ones can affect business continuity. Responses should be focused then for remediation and network defenses should be adapted to changing threat conditions. Critical security activities such as policy tuning should be automated, to save time and effort, while protections and countermeasures must be maintained in an optimal state.		
3	Must support advance malware protection, detection, blocking, tracking,analysis, and remediation to protect the enterprise against targeted and persistent malware attacks. Additional services from OEM for incident response should also be part of solution offered		
4	Must support full contextual awareness policy enforcement based on complete visibility of users, mobile laptop devices, client-side applications, vulnerabilities, threats, and URLs		
5	Must support Application control and URL filtering, Application-layer control (over applications, geolocations, users, websites) and ability to enforce usage and tailor detection policies based on custom applications and URLs		

6	Should support Enterprise-class management Dashboards and drill-down reports of discovered hosts, applications, threats, and indications of compromise for comprehensive visibility		
7	Should support threat correlation, impact assessment, automated security policy tuning, and user identification and incident response services should also be build from OEM directly for any security incident		
8	Proposed solution must be Highly scalable security appliance, architecture that performs at up to multigigabit speeds; consistent and robust security across small office, branch offices, Internet edge, and data centres in either physical and virtual environments		
9	Proposed solution must extends secure corporate network access beyond corporate laptops to personal mobile devices, regardless of physical location; support for Secure Mobility Solution, with granular, application-level VPN capability		
10	Proposed solution must protect traffic, including VoIP and client-server application data, across the distributed enterprise and branch offices		
11	All the subscription & licences with warranty for the proposed solution should be for three(3) years.		
12	Implementation vendor should be responsible for technical training to NSDI IT persons.		

B. Router Technical Specifications (Redundant configuration)

S.No.	Details	Compliance (Yes/No)	Deviation (If Any)/Remarks
1	Aggregate Throughput : 2 Gbps		
2	Total On Board WAN/LAN : Min 4 (with at least 2 Fibre Module)		
3	BGP Routing		
4	VRRP (Redundancy Protocol) for 2 Routers		
5	Dual Power Support		

6	RAM : 16GB, FLASH MEMORY: 32 GB		
7	Minimum 2 input & 6 output ports to connect the standardized connection. (No of ports must enough to synchronize & function the whole setup)		

C. Firewall Technical Specifications (Redundant configuration)

S.No.	Details	Compliance (Yes/No)	Deviation (If Any)/Remarks
1	8 Gigabit Ethernet (GE) copper Ports scalable to 6 GE copper or 6 GE SFP Ports , 2 Nos of 2.0 USB Ports, 1 RJ-45 console Port and dedicated 1 GE Management Port or better		
2	Must support 10,000 or more concurrent sessions		
3	Support for 5,000 or more new connections per second		
4	Internet Secured Gateway should have Stateful Inspection throughput of 4 GBPS with multiprotocol should support 2 GBPS or higher throughput		
5	Must support Triple Data Encryption Standard & Advance Encryption Standard (3DES/AES) VPN throughput of 700 MBPS or higher		
6	Should support unlimited user nodes and should support 50 or more Virtual Interfaces (VLANS)		
7	Must be able to support IPSec site to Site VPN peers for 50 Nos.		
8	Should be able to categorize URL		
9	Should support on - device management		
10	Must support Centralized configuration, logging, monitoring, and reporting		
11	Aggregate Throughput : 4 Gbps		

D. IDPS Technical Specifications (Redundant configuration HA)

S.No.	Details	Compliance (Yes/No)	Deviation (If Any)/Remarks
1	The device should support following modes of deployment:- a.) IDS (Inline detection mode), Inline b.) IDS and inline together/simultaneous in same appliance c.) NIPS should be available as hardened plug n play dedicated appliance (NOT ANY UTM or open functionality from first day. e.) 4*10Gbps ports with fail open functionality from first day. f.) NIPS should provide maximum concurrent connections of 3,000,000		
2.	NIPS should be in Gartner leadership quadrant since last 3 consecutive years and the device should perform traffic inspection based on Signatures, Protocol anomaly, Behaviour anomaly and Reputation.		

3	The device should accurately detect the following Attack categories:- a.) Malformed traffic, Invalid Headers, DoS,Ddos b.) Vulnerability exploitation by integration through 3rd party VM solutions c.) Zero-day and unknown attacks through signature less engine or integrating with sandbox solution d.) URL obfuscation e.) The device should employ full seven-layer protocol analysis of over internet protocols/applications like HTTP, FTP, SMTP, Facebook, Gmail, etc. f.) The device must support vulnerability based and exploit based signatures. It should detect and block all known high risk exploits and the underlying vulnerability (not just one exploit of that vulnerability) g.) NIPS should support management console (policy management /reporting) in HA and it should be custom appliance based which should be proposed in solution BOQ.		
4	The device should handle following traffic inspection& support: a.) IPv6, IPv4, MPLS, Tunneled: 4in6, 6in4, 6to4 b.) Bi- directional inspection, Detection of Shell Code, Buffer overflows, Advanced evasion protection c.) Application Anomalies, P2P attacks, TCP segmentation and IP fragmentation. d.) Rate-based threats, Statistical anomalies e.) The device should have the ability to identify/block individual applications (e.g. HTTP or HTTPs) f.) Layer 7 DOS attack protection g.) The device should identify SSL protocol based attacks. h.) NIPS engine should provide shell code analysis for protection from advanced threats.		

5	NIPS should provide SSL throughput of 1.5Gbps with 2048bit key length and should support browser script analysis.		
6	The device should support Block attacks based on IP reputation, DNS Inspection, Geo-location, URL Inspection. NIPS should provide 1000 virtual NIPS systems in solution proposed		
7	NIPS should support pdf, flash and office document analysis capability and proposed NIPS should provide OS profiling for hosts		
8	Should support active-passive and active-active for the appliance, the HA should be out of box solution and should not requires any 3rd party or additional software for the same		
9	NIPS should support stateful packet inspection, Inbound& outbound SSL inspection without adding any latency.		
10	NIPS should provide real world throughput of 1.5Gbps and maximum UDP throughput of 5Gbps		
11	The device should protect against DOS attacks based on: a.) Heuristic-based detection b.) Self-learning profile-based detection / Network Behavior Analysis c.) The solution should be able to provide Layer 7 DOS protection like HTTP challenge-response approach based on the traffic volume anomaly. d.) The device should have the feature for integrating SNORT signatures. e.) The device OEM must have its own threat intelligence analysis center.		

E. Switch Technical Specifications

S.No.	Details	Compliance (Yes/No)	Deviation (If Any)/Remarks
1	Switch should offer Wire-Speed and Non-Blocking Switching.		
2.	Switch should have 24 10/100/1000 PoE+ RJ45 Ethernet with minimum 370 PoE wattage.		
3	Switch should have 2 ports of 10G SFP+ from day 1 for Stacking over 10GE between floors. Must include one optic, cable for stacking on 10GE with stack distance of 10 meters to adjacent floor and one SR SFP+ to complete stack of top-to-bottom hub room's.		
4	Switch should have 2 additional 10G SFP+ ports from day 1 loaded with two SFP+ for uplink to core.		
5	Switch should have 2 additional 10G SFP+ ports from day 1 for adding high capacity endpoints as and when required		
6	Should have Flash ROM of 128MB and DRAM of 512MB or more.		

F. Database Security Solution

S.No.	Details	Compliance (Yes/No)	Deviation (If Any)/Remarks
1	The solution should be software based which monitors & manage activity on at least the below mentioned databases and its spatial data components . Oracle 8i, 9i, 10g, 11g,12C SQL Server 2005, 2008, 2012 Sybase ASE 15.0.3 or Higher MySQL (specify Version) IBM DB2 (specify Version) Postgres and Post GIS Other (specify) (No custom appliance based solution shall be proposed for database security)		
2.	Solution does not require changes in the database application (e.g. turning audit or trace on)		

3	Solution should be a non-intrusive agent installed on the server. The agent should read the data from shared memory and should process it locally and without sending it to any of the network appliance for processing		
4	Solution should protect itself from tampering and attacks through pre- defined policies and rules which should get updated through new updates for new vulnerabilities and exploits in database		
5	Solution allows easy translation of actual database activity into monitoring / audit policy direct from alerts		
6	Solution should be capable of capturing the alerts which will include the following metadata: Originating IP Address DB User OS User Full SQL Statement Accessed tables Application Name Module Name Host Name/Terminal name Command Type		
7	The solution should be capable of sending alerts can be sent to external applications at least through: via e-mail via syslog via snmp traps Other (specify)		
8	Solution should easily integrate with SIEM and other management products		
9	Solution should be capable of monitoring of all database activities and protect against insiders with privileged access		
10	Solution should offer granular monitoring of database transactions with real- time alerts and prevention of breaches		

11	Solution should offer granular monitoring of queries, objects and stored procedures with real-time alerts and prevention of breaches		
12	Solution should provide protection against newly discovered database vulnerabilities, providing immediate protection with no DBMS downtime and without having to update the patch itself.		
13	Solution should offer flexible audit and reporting capabilities suitable for PCI DSS, SOX and HIPAA		
14	Solution should provide multiple user roles that facilitate separation of duties		
15	Solution should capable of monitoring and alerting unauthorized access to sensitive data on the Database, like credit card tables etc.		
16	Solution should have the ability to independently monitor and audit all database activity , including administrator's activity and select transactions.		
17	Solution should record all SQL transactions : DML, DDL , DCL and Selects and The ability to store this activity securely outside the database		
18	Solution should have the ability to enforce separation of duties on Database Administrators. Auditing should include monitoring of DBA activity and solutions should prevent DBA manipulation or tampering with logs or recorded activity.		
19	Solution should have the ability to generate alert on policy violations and provide real time monitoring and rule based alerting.		
20	Solution should have the ability to ensure that a service account only accesses a database from a defined source IP and only runs a narrow group of authorized queries		

21	Solution Should capture and report on SELECT statements made on Databases		
22	Solution Should report on detailed SQL, including the source of the request, the actual SQL commands, the database user name, when the request was sent and what database objects the command was issued against.		
23	Solution Should report on database access including logins, client IP, server IP and source program information.		
24	Solution Should track execution of stored procedures, including who executed a procedure, name of the procedure and when, which tables were accessed as a result		
25	Solution Should track and audit administrative commands such as GRANT,		
26	Solution Should track and report all failed logins.		
27	Solution Should support creation of specific rules on observed events, sending SMTP alerts when the rules are violated.		
28	Solution should Capture and report on non-administrators executing DDL.		
29	Solution Should support architecture where application has pooled connections, the original IP address and user name should be monitored.		
30	The solution deployed should not require any change in the DBMS binaries		
31	The agent should not demand for restart of the database while installing or While upgrading or While uninstalling the solution		

32	Solution should be able to monitor inter and intra DB activities and attacks		
33	Solution should be able to monitor activities done by administrator or any DB admin sitting directly on the database server console		
34	Solution Should be able to scan databases for vulnerability		
35	The solution should have a single console to manage and monitor database activity monitoring and the vulnerabilities inside the database		
36	Solution should be capable of detecting weak passwords		
37	Solution Application comes with predefined reports, allows for customizing and Ad-hoc reports		
38	The solution should provides Sarbanes-Oxley module, PCI DSS and any others(Specify)		
39	The OEM should take ownership of deployment and directly provide highest premium support offering 24 * 7 for the solution during the contract period. NIPS, Database security and Server security solution should be offered from the same OEM.		
40	The proposed solution should be capable of detecting and preventing advance database attacks such as SQL Injection, TNS Poisoning, Buffer Overflow etc. A. An interactive graphical representation of database access activity B. Automatic scheduled data export and archiving to long-term storage. C. Monitoring local access D. Executive Summary / Dashboard view E. Both Online and Offline Security update capability F. Monitoring of Database Memory at		
41	Solution should provide more than 4700 scans/checks including unsecure PL/SQL code scanning and fast password checking		

42	Solution should provide virtual patching to protect database from potential breaches prior to installing vendor released patch updates		

G. Server Security Solution

S.No.	Details	Compliance (Yes/No)	Deviation (If Any)/Remarks
1	Endpoint security solution should provide integrated anti malware, firewall, device control, web and email security to deliver essential endpoint security defenses with centralized management. It should allow administrators to protect Windows, Mac and Linux environments from malware and 0-day threats and to prevent unauthorized devices, connections and websites from being accessed		
2.	Solution must provide Virus protection at Servers and Desktop level		
3	Should be able to guard all Windows, Mac, and Linux endpoints against system, data, email, web threats and should be managed from a single management console & single agent		
4	Endpoint Security client should create a common service layer— the Endpoint Security Platform. Common services such as logging, installation, data updating, and self-protection should reside on a single layer. Should have the following integrated components like AV ,Firewall, Web Control , Threat Protection etc. ,which can adapt using updated information that can automate workflows to stop future attacks		

5	Endpoint Security product should have a Collaborative Framework i.e Threat Protection defenses should collaborate and share what they see in real time to coordinate identification and block the execution of suspicious fles, websites, and potentially unwanted programs for a higher level of protection. Should fulfill the following use case : A file hash if sent from Web Control part to Threat Prevention module, should trigger an ODS. Malicious files should be detected and blocked before they have full access to the		
6	Should have the ability to detect and remove unwanted joke programs,		
7	Alert / Notify , Clean, Delete / Remove, Move / Quarantine, Prompt for Action		
8	Shall support multiple Windows platforms		
9	Endpoint protection vendor must have scored the highest in a test of protection against evasion attacks in NSS Labs report.		
10	Should support file scan caching to avoid repetitive scanning of files which are unchanged since the previous scan		
11	Proposed solution must automatically scan Compact disks, USB devices and Network shares in real-time when accessed.		
12	Proposed solution should provide multiple policies to lockdown the desktop like – change in registry, Internet Explorer file settings, Exe file execution etc to block unknown zero day attacks and reduce dependency on frequent signatures		
13	Should allow the On Demand Scanner to recognize the last scanned file and resume scanning from that file if an “On demand Scan” is interrupted		

14	Should have the ability to control the amount of CPU resources dedicated to a scan process		
15	The proposed solution should be capable of detecting and preventing buffer overflow vulnerability, irrespective of the exploit that is using the buffer overflow vulnerability. The solution should support buffer overflow detection and prevention on the following minimum applications:		
16	Proposed solution should be capable of blocking TCP/IP ports on the System and also creating exceptions for specified applications to use these blocked ports.		
17	Proposed solution should be capable of blocking read, write, execute, delete & change permissions on specified file(s)/folder(s)/Network Share(s).		
18	The proposed solution should provide Self-protection from modifying or disabling VirusScan		
19	The management server should have a database which supports merging, backups, restoration and replication		
20	Should support protection against POTENTIALLY UNWANTED PROGRAMS		
21	Proposed solution should have integrated URL categorization feature		
22	Should have Web Filtering for Endpoint that provides secured web access for anyone using the Internet for work-related or personal business—in or out of network.		
23	Proposed solution should categories URLs for threats like – Spywares, Trojans, Spam, Adwares etc.		

24	Solution URL category module should provide end user detail threat information about the site		
25	The proposed solution should scan system memory for installed rootkits, hidden processes, and other behavior that suggests malicious code is attempting to hide itself		
26	The proposed solution should allow to configure different policies for different set of Processes		
27	Proposed solution must identify machines plugged into the network and notify the administrator of the presence of a machine without an Antivirus engine running on it.		
28	Heuristic network check for suspicious files		
29	Protection from malware even if no signature file available locally		
30	Should have enhanced tamper protection that guards against unauthorized access and attacks, protecting users from viruses that attempt to disable security measures		
31	It should support heuristic scanning for viruses and worms for which signatures are not released and documented		
32	Infection treatment should support report-only, cure, delete, move and rename file		
33	It should allow to pre-define certain extensions which can be blocked/exempted even without scanning		
34	It should allow scanning specified extensions or exclude certain extensions and allow scanning various types of compressed files		

35	It should allow notifications being sent to the owner, sender and administrator when and infection is detected		
36	Attachment type recognition based on attachment extension, content, file type or file		
37	Should search for keywords in the message content and block and alert the administrator in case found		
38	Facility of blocking e-mail addresses from where we do not want to receive e-mails		
39	Filters should automatically be downloaded from the proposed solution vendor to customer		
40	It should be possible to specify the number and level of detail of logs to keep		
41	Must be able to totally protect from spyware, adware, Trojans, key loggers, P2P Threats, Hackers tools, DDOS Attack Agents, in real time		
42	Must be able to support Interactive scan on demand		
43	Should have centralized management and reporting capabilities to deliver reports like top Spywares, by category, by infected machines, by risk priority etc		
44	Real time Active protection on memory, process termination / file removal of pests in active memory		
45	Must be able to scan from the desktop according to preset or customized configurations		
46	Should have centralized update/download mechanism which should be able to download details of latest Spywares and push the same across all the desktops		
47	The solution must be able to auto-quarantine or auto-delete spyware or adware without end-user interaction		

48	The management tool should provide support for Microsoft Clustering Services. This would ensure that the management server is always available, even if the primary server shuts down for any reason		
49	The centralized management console may be web-based		
50	The centralized management console should be capable of deploying remotely the managed products (such as desktop AV) on a machine		
51	The tool should support hierarchical grouping of machines and policy deployment. The grouping could be based on IP Address of a subnet of machines or a particular site		
52	The Centralized management tool should be capable of deploying Pattern Files, Scan Engines, emergency releases of pattern files, patches, hot fixes and new product versions for all managed products		
53	The centralized management tool should be able to deploy signature files for different products		
54	Centralized management console should provide dashboard with multiple information & these information should also be fetched from database based on different queries		
55	Console should support tagging of information in the database to provide flexible reporting		
56	Administrator should be able to configure the update process as automatic or manual, controlled deployment		
57	Update process should conserve WAN Bandwidth by having a distributed framework for signatures and policy updates		

58	The centralized management console should provide management reports for different managed components like – Top N reports, Trend reports, Outbreak reports, Compliance reports,		
59	The centralized management console should support the way to build custom queries on the database to create custom reports		
60	Central management console should provide automatic generation and delivery of reports to the respective administrators		
61	Central management console should provide actionable reports		
62	Central management console should support granular role based access control		
63	The Centralized Management Console should deliver security threat information including current threats and the DAT and engine files necessary to protect against them		
64	Must have the policy to restrict or permit access to potentially harmful web sites.		
65	Web control Solution should warn employees before they interact with dangerous web sites, and give them the freedom to search and surf online with protection from web-based threats.		
66	Prevent disruption and downtime from rogue systems that do not have agent installed by being able to identify them as they connect to the network		
67	Should have near Zero-impact user scans only run when a device is idle		
68	Policy sharing across servers and roll-up reporting		

69	Should support agent handlers to allow management of end systems ,even off the network		
70	Management server should have the capability to correlate threats, attacks, and events from endpoint, network, data security as well as compliance audits to improve the relevance and efficiency of security efforts and compliance reports.		
71	Proposed Solution should be Recognized for four straight years by Gartner as a leader in Endpoint Security and Mobile Data Protection		
72	Should Shorten the time from insight to response with dynamic and automated queries, dashboards, and responses		
73	Solution should reduce the cost of managing IT security and compliance by more than 60 percent based on survey by agencies like MSI International of more than 450 mid-sized and large enterprises).		
74	The management server should be able to manage/report other vendors' products too		
75	Device Control Solution		
76	Monitor, block and notify user when devices are connected to the machine to prevent data from leaking out. Devices include wireless access, firewire, Bluetooth, serial port, parallel ports.		
77	Monitor and blocking of devices should include parameters such as vendor id, product id, serial number, bus type connection (usb, PCI,IDE), Device class and device name.		
78	Provide a simple way to add new devices not in the default list that is to be monitored or blocked.		
79	Able to make DVD/CD Writers read-only to prevent data leakage.		

80	Able to make usb mass storage devices read-only to prevent data leakage		
81	Able to prevent confidential data from being copied to usb and yet allow other data to be copied.		
82	Able to automatically encrypt confidential data when its being copied to usb. Other data will not be encrypted.		
83	Monitor and prevent data copied to USB storage devices (thumb drives, iPods, etc.) and CD/DVD but not other USB devices e.g. mouse, keyboard, 3G modem.		
84	Pop up user messages can be customised on a per protection rule basis.		
85	Offline agent bypass is allowed based on FIPS compliant challenge- response. Agent is placed in monitoring mode instead of blocking mode. This is required in case of business critical situation such as director needs to send out email urgently.		
86	Agent-based scanning enables parallel scanning of thousands of endpoints		
87	Ability to support global distributed deployments of endpoint machines		
88	Tamper proof agent that cannot be inappropriately disabled; if somehow stopped, a separate service restarts it. The same protection applies in safe mode.		
89	Agent does not appear in “Add/Remove Programs” and System Tray, and obfuscated in Services and Task Manager		
90	Agent uninstallation can be done offline based on challenge-response.		
91	Communications between agent and server are encrypted and authenticated		

92	Filter scans based on tag classification		
93	Scans can be configured to run on schedules by day and/or time of week.		
94	The device control should be upgradeable to full-fledged data leakage protection solution through a license upgrade		
95	Support: The OEM should have bundled 24-7 support via phone, mail &chat .The OEM should have a support and R&D center.		
96	The OEM should have a option of providing a dedicated Support Account Manager (SAM) who delivers proactive account management services at a cost		
97	At an additional cost the OEM should have a option of direct access to product specialists who are technical experts on the solution proposed through the SAM .		
98	The optional OEM Support Account Manager should conduct up to two onsite meetings with the customer team per year		
99	The OEM should provide a Minimum Escalation Requirements Tool to assist OEM technicians to quickly diagnose issues.		
100	Should have new Endpoint Protection Technology features like :		
101	Should get real-time intelligence and actionable threat forensics from defenses that communicate and learn from each other to combat advanced threats. Should have capability to connect to in-house Threat Intelligence Exchange Server .		
102	Should strengthen the defenses with faster scanning, threat updates, maximized CPU, and protection performance that is proven to be effective in third-party tests		

103	Should be able to simplify our defenses and remove the complexity of duplicate technologies, connect other solutions, and enable more of our defenses to communicate with each other using our endpoint security framework.		
104	Should boosts performance by avoiding scans on trusted processes and prioritizing those appearing suspicious.		
105	Should have Functionality de-duplication: The integrated common service layer should eliminate redundancies caused by multiple point product installations on a single machine ,there should be only one firewall, one self- protection, one access protection, and one buffer overflow protection as functionality de-duplication also helps to reduce confusion over what to install.		
106	Should allow administrators to configure on-demand scans in “scan on idle” mode. When this is enabled, on-demand scans will only run when the system is idle. User systems are idle during certain time periods, such as when users take lunch or coffee breaks. The new feature takes advantage of this idle time to perform scans. When the user is active, the scan pauses automatically. Even if a user reboots, the scan will not terminate; rather, it will simply stay paused until idle. With this advancement, users may never notice scans again.		
107	Should be upgradeable for Dynamic Application Containment (no blocking) to take care of the latest threats		
108	Should have an option to integrate with Threat Intelligence Exchange Server to Instantly share patient zero threat insight with all other endpoints to prevent infections and update protection		

Annex-III

Financial Bid

The format for the financial bid should be as per the attached excel table.

Note: Additional/separate cost for installation, commissioning, licensing, maintenance etc. will not be considered.

Annex-IV

Evaluation of Technical Eligibility Criteria

(Subject to revision after vendor interaction during Pre-bid Meet)

- **Financial strength : Maximum 10 marks**
- **Availability of Technical Man Power : Maximum 10 marks**
- **Experience of similar work : Maximum 15 marks**
- **Performance on similar work : Maximum 15 marks**
- **Proposed Network Security Solution : Maximum 50 marks**

  (Methodology, Training, Licensing Policy, Performance, Consistency, Maintainability, Scalability, Advance Security Feature(s) like Machine Learning etc.; Demonstration, PoC(If any) etc)

Note: The Qualifying marks will be Minimum of 70 marks