



INTELLECTUAL
PROPERTY INDIA

Patents/Designs/Trademark
GEOGRAPHICAL INDICATIONS



सत्यमेव जयते

GOVERNMENT OF INDIA
MINISTRY OF COMMERCE & INDUSTRY

Intellectual Property Office Building

Plot No.32, Sector – 14, Dwarka

NEW DELHI - 110 075.

E-mail : delhi-patent@nic.in

<http://ipindia.nic.in>

☎ 28034304, 05, 06

☎ 28034322-28034320

Fax No.28034301/302

No. POD/Tenders/2010-2011/-

Dated: 01.11.2010.

Tender notice for supply, installation & configuration of Enterprise Antivirus solution

The sealed Tenders are invited by the Patent Office, New Delhi for supply of Enterprise Antivirus solution at the address as mentioned above and as per the specifications and quantity given below for Servers & Desktops in two bid system.

Requirement:

Enterprise Antivirus Solution for:

Servers (Windows based o/s)	10
Desktops (Windows based o/s)	245

1. Eligibility Criteria of Bidders:

- Vendor should attach the Balance Sheet showing at least Rs. 2 crores annual turnover in each financial year for the last three financial years.
- Bidder should be Original Equipment Manufacturer (OEM) / Authorized Partner of Principal Antivirus Vendor and a letter of Authorization from OEM, specific to the quotation should be enclosed.
- The Bidder should be an ISO certified company.
- The Bidder should have professionals certified on the antivirus solution they propose against this quotation. Proof of the same shall be enclosed.

- e) The OEM must enclose a certification of having successfully executed at least two enterprise Anti Virus solutions for minimum 250 nodes each in any of the last 3 financial years for any Educational Institute/University/Govt. entity/PSU.
- f) An undertaking from the manufacturer is required in this regard stating that they would facilitate the bidder on a regular basis with technology/product updates and extend support for the warranty as well.
- g) Latest Income Tax Certificate should be enclosed.

2. Obtaining Bid Documents:

- The tender can be obtained on request from administrative officer on payment of Rs. 500/- (Rupees Five hundred only) (Non refundable), payable through cash / crossed demand draft drawn on nationalized bank in favour of “controller of patents” payable at New Delhi
- The tender document can also be downloaded from the website of IPO but should be accompanied with the cost of tender document of Rs 500/ in cash (to be deposited at counter) or crossed demand draft drawn on nationalized bank in favour of “controller of patents” payable at New Delhi at the time of submission.

3. Submission of Proposals:

- (i) The bidder shall go through the entire document and must comply with all the terms and conditions. A Compliance statement in the form of ‘Complied’ or ‘Not Complied’ shall be given against each item and specification of the Tender (Annexure-I). The compliance statements should be supported by authentic documentation. Please note that any deviation from the laid down requirements / specification shall be brought out separately in deviation sheets to be attached with concerned section of the Tender document. Failure to comply with this requirement may result in the bid being rejected. Each page of the bid and cuttings / corrections shall be duly signed and stamped by the bidder. Failure to comply with this requirement may result in the bid being rejected.
- (ii) The proposals shall be submitted in two parts and should be super-scribed as “PART-I: COVER FOR TECHNICAL BIDS” and “PART-II: COVER FOR COMMERCIAL BIDS”.

- (iii) **Part-I** shall be a Company Profile covering all the documents specified in the 'Eligibility Criteria of Bidders' as per para 1 above as well as a Technical Offer with full details including description of product so as to enable technical assessment of the proposal and categorical clause wise compliance statement as per Annexure-I.
- (iv) The Technical bid must be submitted in an organized and structured manner. No brochures/leaflets etc. should be submitted in loose form. The Technical Offer should comprise of the following:
- a.) A letter of authority duly signed by an authorized signatory.
 - b.) Complete Information of Commercial bid with Product Name, Version & Manufacturer quoted for.
 - c.) Commercials must not be given in Part I.
 - d.) Technical Documentation [Product Brochures, leaflets, manuals etc.]
 - e.) Delivery and implementation schedule.
 - f.) Compliance of terms with any deviation clearly indicated in remarks & brought in separate deviation sheets.
 - g.) Warranty details etc.
- (v) **Part –II** should contain The Commercial Bids for the entire proposal. The bidders are requested to quote:
- a.) Name and Version of Enterprise Antivirus solution with charges for installation & configuration in Indian Rupees.
 - d.) Prices quoted shall be inclusive of escalation of any description. The rates must be quoted including the following:
 - I. All costs should be given in Figures and Words.
 - II. Govt. Levies like Sales Tax, Octroi, Excise Duty, Work Contract Tax (WCT) and Educational cess etc., if any, shall be paid at actual rates applicable on the date of delivery. Rates should be quoted accordingly giving the basic price, duties and taxes etc., if any.
- (vi) Both the covers should first be sealed separately, and then both the covers should be kept in a single sealed bigger cover. This envelope should be duly signed by an authorized signatory and should bear the inscription as under:
"Supply, Installation & Configuration of Enterprise Antivirus Solution for IPO"
"Tender document Enquiry No.": Dated.....

- (vii) Bids Acceptance: The Bids must reach the Patent Office, Delhi addressed to The Administrative Officer, Patent Office, Boudhik Sampada Bhawan, Plot No. 32, Sector-14, Dwarka, New Delhi – 110 078, on or before the due date, i.e., on 09th November 2010 by 3.00 P.M. In the event of due date being a closed holiday or declared Holiday for Central Government offices, the due date for submission of the bids will be the following working day at the appointed time & venue. Bids will not be accepted after the due date & time.
- (viii) Validity of bids: Bids should be valid for a minimum period of 90 days after the due date.

4. The important dates:

- a) Last Date and time for Submission of Tender document: The last date to submit sealed Tender is 10.11.2010 till 3.00 pm.
- b) Opening date of Technical Bid: .10.11.2010 at 4.00 P.M.
- c) Opening date of Commercial Bid: .12.11.2010 at 3.00 P.M.
- d) Address and place for submission of bids: The bids may be submitted in sealed envelope in the prescribed format super scribing 'Tender for supply of Enterprise Antivirus Solution for IPO, addressed to The Administrative Officer, Patent Office, Boudhik Sampada Bhawan, Plot No. 32, Sector-14, Dwarka, New Delhi – 110 078.

5. Terms & Conditions:

1. Price quoted should be inclusive of all applicable taxes and levies.
2. The office reserves the right to change the quantity as per its requirement at any stage. Further the Office reserves the right to place order either of all the items or only some of above items. The supplier shall have no right to claim any compensation in such case.
3. The Office reserves the right to reject any or all Tenders without specifying any reasons thereof.
4. If the technical offer contains any price information the offer will be summarily rejected.
5. Incomplete Tenders are liable to be rejected.

6. Canvassing in any form in connection with the tenders is strictly prohibited and bids submitted by the bidders who resort to canvassing are liable for rejection.
7. IPO shall not pay any costs incurred towards preparation and submission of the bid or any other expenditure in this regard.
8. Unsigned bids, unattested corrections and over writings by bidders are also liable for rejection.
9. Bids not adhering to the specifications will be out rightly rejected.
10. Conditional bids will be summarily rejected.
11. Delivery should be within 1 week from the date of receipt of order for supply.
12. Sealed Tender should reach on or before date as mentioned above.
13. In case of delay, penalty at the rate of 0.5% per day of the ordered value shall be charged (maximum penalty up to 5 % of the order value can be deducted). If the delay is more than ten days the order shall stand cancelled.
14. Payment will be done after installation.
15. All disputes should be within the jurisdiction of Delhi.
16. The Vendor has to submit documentary proof of Sales Tax/PAN etc.
17. No Advance payment shall be made by the office.
18. The Vendor has to submit an EMD of Rs10,000/- in the form of Demand Draft in favour of 'Controller of Patents' payable at New Delhi.
19. Tenders submitted without EMD shall be rejected out rightly.
20. The Vendor has to submit performance security for Rs. 50,000/-, if the tender is awarded.
21. If vendor does not supply the product as per the configuration no payment will be made and performance security will be forfeited.
22. Rates once submitted cannot be changed & should be valid for at least 90 days from the date of contract.

(Dr.K.S.Kardam)
Deputy Controller of Patents & Designs
(Head, Patent Office Delhi).

TECHNICAL SPECIFICATIONS:**Compliance Requirement Description**

Sr no.	Description	Compliance (Complied/Not Complied)	Remarks
(a)	End Point Security Protection Features capabilities		
1	Solution should able to Detects and blocks malicious software in real time, including viruses, worms, Trojan horses, spyware, Adware, and RootKit.		
2	Endpoint solution technology should include a behavioral based technology apart from providing the signatures for known threats, vulnerability add heuristic based approach. It should be able to score both good and bad behaviors of unknown applications, enhancing detection and reducing false positives without the need to create rule-based configurations to provide protection from unseen threats i.e. zero-day threats.		
3	Solution firewall engine should have option to allow or block support of network protocols, including Ethernet, Token Ring, IPX/SPX, AppleTalk, and NetBEUI. Can block protocol drivers (example: VMware, WinPcap) and should have Adapter specific rules – e.g. Ethernet , Wireless, VPN		
4	Proposed IPS solution should allow customer to edit and create the IPS signature using snort/custom based format if required.		
5	Solution should able to block devices based on Windows Class ID and should include USB, Infrared, Bluetooth, Serial, Parallel, fire wire, SCSI and PCMCIA. Solution should also be able to block and give read/write/execute permission for mentioned devices.		
6	Solution should provide application analysis, process control, file and registry access control, module and DLL control.		
	Proposed Solution should be able to deploy flexible and different security policies depending upon the AND/OR		

	relationship of following network triggers -		
	- IP address (range or mask)		
	- DNS Server		
	- DHCP Server		
	- WINS Server		
	- Gateway Address		
	- TMP Token Exists (hardware token)		
	- DNS Name Resolves to IP		
	- Policy Manager Connected		
	- Network Connection (wireless, VPN, Ethernet, dialup)		
7	Proposed IPS solution should combines NIPS (network) and HIPS (host) both with Generic Exploit Blocking (GEB) for one signature to proactively protect against all variants, Granular application access control and behavior based technology mentioned above.		
8	Proposed solution should be able provide superior root kit detection and removal. This should have access below the operating system to allow thorough analysis and repair.		
9	System Lock Down - it should be able to “Locks down” the system by fingerprinting every executable file on the system. It can then monitor all running applications and terminate any application for which the agent does not have a matching fingerprint.		
10	Denial of service detection and protection - Should Protects the system from multiple forms of anomalous network behavior that is designed to disrupt system availability and/or stability.		
11	Anti-spoofing - Should Protects the transmission of data from being sent to a hacker system who has spoofed their IP or Mac Address		
12	Agent has the ability to detect and block process execution chains. It is able to detect when a malicious application tries to execute a trusted application, and then use the trust privileges of that application to access the network.		
13	Anti-application hijacking - Should prevent hackers and web sites from identifying the operating system and browser of individual computers.		

14	Code insertion attack prevention - Prevent malicious applications from inserting code into trusted application to bypass outbound application fire walling.		
15	Protocol adapter attack prevention - Prevent malicious applications from using their own protocol adapter to bypass outbound fire walling.		
16	Antivirus and Antispyware policy can have options by default to choose High Security and High performance to have a right balance while deployment in the production network.		
17	Antivirus schedules scans should get delayed/rescheduled while laptops are running on batteries.		
18	Antivirus should have behavior based technology to scan for Trojans, worms and key stroke loggers to protect from zero day threats. Sensitivity level of this should get adjusted with customized scanning frequency.		
19	Antivirus Solution should have internet browser protection and home page should be configurable if security risk changes that.		
20	Antivirus solution should be able to Scan POP 3 email traffic including email clients Microsoft outlook , lotus notes and outlook express.		
21	Desktop Firewall rules should be configurable depending upon the adapters including Ethernet, wireless, Dialup, VPN (Microsoft PPTP, Nortel, Cisco).		
22	Desktop Firewall rules should be configurable depending upon the state of screen saver "ON" & "Off".		
23	Desktop Firewall Policies should be configurable depending upon the time and day.		
24	The solution must have readymade policies including –		
	a) To Make all removable drives read only ,		
	b) To block program from running from removable drives ,		
	c) Protect clients files and registry keys ,		
	d) Log files written to USB drives ,		
	e) Block modifications to host files		
25	Solution must be able to display and customize warning messages on infected computers. For example, if users have a spyware program installed on their computers, you can notify them that they have violated your corporate policy.		

26	Management server should have the capabilities to add multiple domains if required for the different locations to assign the different administrators for other locations. Each domain should shares the same management server and database & This separation prevents administrators in one domain from viewing data in other domains. These administrators can view and manage the contents of their own domain, but they cannot view and manage the content of other domains.		
27	Solution must provide a group updater for remote site and must have bandwidth throttling option to streamline updates and there by reducing load on the bandwidth		
28	To conserve the network bandwidth clients should be configurable to upload the maximum records of logs to the management server.		
(b)	Compliance enforcement and validation options		
1	The Host-based, self-enforcement - It should use a desktop firewall (built into the agent) to permit or deny managed endpoints access to the network. This method should offer the fastest and easiest implementation as it requires: No infrastructure changes and No additional deployment efforts.		
2	Solution should have the integration with various client management & patch management solution		
3	It must have compliance check policy templates for client management agent to ensure that agent is always installed, running and updated.		
4	Solution must have the ability to validate the users connecting to the Enterprise network by determining the following:		
	a) Their host-firewall policy matches the policy defined on the management server.		
	b) Host-IPS is running. And HIPS signature files are up to date		
	c) Anti-Virus is running and Anti-Virus definitions/.DAT files are up-to-date according to enterprise security policy.		
	d) Custom or third-party security applications are running.		
	e) The patch level of the operating system meets enterprise security policy.		
	f) The patch level of applications meets enterprise		

	security policy.		
	g) Registry values are present.		
	h) The password strength meets minimum requirements.		
	i) Windows Update tool is enabled and running.		
	j) They are permitted to alter their network configuration settings.		
	k) Minimum service pack requirements are met.		
	l) Anti-Spyware is running.		
	m) The agent is a valid agent		
	n) Determine if a custom or third-party files are present..		
	o) Add/Remove Programs is enabled for the user		
	p) Enforce the presence and update status of Anti-Spyware products.		
5	Solution should have following policies templates to check & enforce the security of workstations –		
	a) Minimum password age, password length, complexity and history.		
	b) To Disable Guest account, registry editing, add or remove program, remote desktop, IP change, windows CD and windows auto play.		
6	Host Integrity rule priorities and conditions enable administrators to create interdependencies between rules such as “if/then/else” conditions and determine the order in which rule are executed. For Example, rule conditions allow administrator to create policies such as “the host must be running either anti-virus 1 or anti-virus 2.” Rule priorities ensure the Host Integrity rules are run in the correct order. For example, Agent could download and install a required operating system patch before initiating the update of a hot fix.		
	(d) Automatic remediation in case compliance level of machines fails		
1	If the host is non-compliant with security policies, Agent can automatically initiate a restoration action, which can include running command line, downloading and executing/inserting a file, rechecking the host for compliance, and ultimately granting access for the compliant host to the network.		

	Common usages of remediation include:		
	a) Remediate by executing a file - The ability to bring a system back into compliance after a failed Host Integrity check by running an executable on the local system, such as an Anti-Virus engine.		
	b) Remediate by downloading a file - the ability to bring a system back into compliance after a failed Host Integrity check by downloading a file to the local system, such as an Anti-Virus dat file.		
	c) Remediate by running a script - The ability to bring a system back into compliance after a failed Host Integrity check by running a script that is included in the policy on the local system, such as a cscript or perl script.		
	d) Remediate by setting registry key- The ability to bring a system back into compliance after a failed Host Integrity check by setting a registry key to a specific value.		
2	Solution must be scalable to incorporate the following with no installation of component on clients should need be in future:		
	a) Network access control solution should be able to provide flexible options to enforce the security policies at different network entry points and user scenario. It should include:		
	i) 802.1x standards-based approach for LAN and wireless networks , DHCP-based approach for LAN and Wirelessover any infrastructure,		
	ii) Gateway enforcement for in-line enforcement on any network,		
	iii) Guest Access for unmanaged nodes connected locally,		
3	The Solution must provide security for MS Exchange, Domino and at Mail Gateway		
(e)	Backup and Restore Management		
1	System Recovery solution should support for Dissimilar Hardware recovery in case of a complete system crash.		

2	It should support conversion to and from virtual environments like VMware, Microsoft Hyper & Microsoft Virtual Server		
3	It should support scheduling of recovery points		
4	It should auto-detect hardware and install appropriate drivers while recovering a system from complete crash situation.		
5	Solution should support saving of recovery points at FTP locations, DAS, NAS, USB Drive, DVD drives		
6	The solution must be able to initiate automatic threat con driven backups as soon as the threat landscape increases.		
7	The solution should provide a complimentary disaster recovery for critical servers and clients.		
8	The solution must provide bare metal recovery to the existing or dissimilar hardware possible in minutes		
9	The solution must provide physical to virtual and virtual to physical conversion. With this functionality, administrators can have can follow best-practices, such as testing deployments in virtual environments or using virtual environment as an immediate disaster recovery site.		
12	An optional Granular Restore should also be part of solution.		
13	Should support for windows 2000, 2003, 2008 R2 (servers), Red Hat and SUSE Linux		
14	Should support for 32 bit & 64 bit windows (incl. xp, vista, 7)		

COMMERCIAL BID FORMAT:

Sub: Tender for “Supply, installation & configuration of Enterprise Antivirus solution”

a) Enterprise Antivirus Solution

Sl.No	Name of the manufacture(Brand)	Rate per license	Total (in Rupees incl. Taxes etc.)	
			In Words	In Figures

(Signature of vendor/supplier with stamps of the firm/Company)

Dated :

At :