

**Tender Document**  
**For**  
**Rate contract for Supply and Installation of**  
**AntiVirus & Content Security S**  
**oftware for Desktop, Server & Network**

**Tender no. MPSEDC/MKTG/2010/175**

(All pages of this document except for Commercial-bid to be submitted in original duly signed on each page along with the technical bid envelope. The Commercial bid in original is to be enclosed in a separate sealed envelope)

**M.P. State Electronics Development Corporation Ltd.**  
**147, Zone-I, M.P. Nagar, Bhopal-462011 (M.P.)**  
**Ph. No. 0755-2769816/23, Fax: 0755-2769824**

Signature of the Tenderer  
with stamp and date

[www.mpsedc.com](http://www.mpsedc.com)

Signature of the Tenderer  
with stamp and date

**M.P. State Electronics Development Corporation Ltd.**  
**147, Zone-I, M.P. Nagar, Bhopal-462011 (M.P.)**  
**Ph. No. 0755-2769816/23, Fax: 0755-2769824**  
**www.mpsedc.com**

## **Technical Bid**

### **INVITATION FOR BIDS**

Addl. Chief General Manager, MPSEDC Ltd., Bhopal invites sealed bids, under two envelopes system, from the bidders for Rate contract for Supply and Installation of AntiVirus & Content Security Software.

Interested bidders may obtain further information from the office of MPSEDC Ltd., Bhopal Bids are invited for the work mentioned hereunder:

<b>Sl. No.</b>	<b>Items</b>	<b>Description</b>
A	Scope of Work	Rate contract for Supply and Installation of AntiVirus & Content Security Software
B	Cost of bid document	Rs.1000/- (non-refundable) by Demand Draft/Cash
C	Postal charges	Rs.100.00(MPSEDC Ltd. shall not be responsible for any postal delay)
D	Sale of bid documents	02.03.10 to 23.3.10(Between 10.30 a.m. to 5.30 p.m.)
E	Last date of submission of bid	26.03.10 up to 3.00 p.m.
F	Date of opening of Technical bid	26.03.10 at 4.00 p.m.
G	Pre bid meeting	10.03.10 at 12 Noon at MPSEDC office
H	EMD	Rs.1,00,000 in the form of Demand Draft payable to MPSEDC Ltd. payable at Bhopal
I	Place of opening of bids	MPSEDC Ltd., 147, Zone-1, Maharana Pratap Nagar, BHOPAL-462 011 (M.P.)
J	Address for communication	MPSEDC Ltd., 147, Zone-1, Maharana Pratap Nagar, BHOPAL -462 011 (M.P.)

**Note** - Tender Document can be downloaded from the website [www.mpsedc.com](http://www.mpsedc.com). In case tender form has been downloaded from the website, the tenderer will have to enclose a Demand Draft of Rs.1000/- (Rupees One Thousand only) of any scheduled bank in favor of MPSEDC Ltd. payable at Bhopal along with the tender.

**\*Any future Corrigenda/Information shall be posted only on our website [www.mpsedc.com](http://www.mpsedc.com)**

Signature of the Tenderer  
with stamp and date

## Letter for Submission of Tender

To  
MPSEDC  
147 Zone I, M P Nagar  
Bhopal (M P)

Dated ----- ,2010

Ref: "Tender for Rate contract for Supply and Installation of AntiVirus & Content Security Software against Tender no. MPSEDC/MKTG /2010/ 175 due for opening on 26.03.10

Dear Sir,

Having examined the tender document relating to the Supply of AntiVirus & Content Security Software as detailed in your tender, Conditions and scope of work etc. and having understood the provisions and requirements relating to the Supply and all other factors governing the tender, We hereby submit our offer for the Supply of the proposed software in accordance with terms and conditions and confirm our acceptance to execute the order within the time period specified in the tender document, at the rates quoted by us in the accompanying Technical & commercial Bid.

If, after the tender document is accepted, we fail to complete the Rate contract for Supply and Installation of AntiVirus & Content Security Software as per the order. We agree that, M/s. MPSEDC LTD. Bhopal shall have full authority to forfeit the earnest money and cancel our order with no obligation on their part.

We confirm having deposited earnest money of Rs 1,00,000/- (Rupees One lakh only) by Demand Draft No.....dated ..... drawn on .....Bank ..... Branch attached here to, and general information required is as per annexure attached.

We further confirm that –

- i. We have successfully executed orders of similar nature and we have sufficient experience and financial strength in handling orders of this value.
- ii. We have sufficient qualified manpower and after sales support to execute the order efficiently in the specified time schedule.
- iii. The quoted rates shall be valid for one from the date of agreement with MPSEDC Ltd .
- iv. We further confirm that all chapters of the tender documents have been read, understood and signed and there is no deviation/discrepancy

Signature of the Tenderer  
With stamp and date

Signature of the Tenderer  
with stamp and date

## GENERAL INFORMATION AND EMD DETAILS

1	EMD Details DD No and date: Amount in Rs. Name of the Bank:	
2	Name and Address of the Tenderer	
3	Contacts:	
4	Telephones:	
5	Fax:	
6	E-mail:	
7	Mobile No:	
8	Category of the tenderer (Whether company, partnership firm or Proprietary concern)	
9	Name of Chief Executive Officer and Telephone No.	
10	Year of Establishment	
11	Sales Tax / Commercial Tax / CST no. / TIN no.	
12	Income Tax PAN / GIR No.	
13	Yearly Turn over of the Last 2 years.	
14	Name and Address of the Banker	
15	List of major Clients and the size of orders executed	

Note: Separate sheets may be attached wherever necessary.

Signature of the Tenderer  
with stamp and date

## Terms and Conditions

Contents of Bidding Documents for Rate contract for Supply and Installation of AntiVirus & Content Security Software the bidding procedures and the terms of contract are prescribed here in under:

1 **Eligibility Criteria:**

- Bidder must have executed at least 3 software orders for the projects in the government sector (attach order copy) and at least two single order worth of Rs. 2 lakhs of software supply to the government sector must have been executed by the bidder's order should be related to supply of AntiVirus software. (Attach order copy)

2. **Amendment in Bidding Document by the Competent Authority**

At any time prior to the deadline for the submission of bids, the competent authority may, for any reason, whether on its own or in response to a clarification requested for by a prospective bidder, modify the bidding document by way of amendment(s).

The prospective bidders having received the bidding documents will be notified of the amendment(s) so made in writing or by Fax and such amendments shall be binding on them.

In order to allow reasonable time to the prospective bidders for taking into account such amendment(s), in the preparation of their bids, the competent authority, at its discretion, may extend the deadline for the submission of bids.

3 **Bid Price**

The bidders shall indicate on the prescribed Price Schedule. Prices quoted by the Bidder shall be fixed during the Bidder's performance of the contract and shall not be subject to variation on any account.

A bid submitted with an adjustable price will be treated as non-responsive and rejected.

4. **EMD may be forfeited:**

If a Bidder withdraws its bid during the period of bid validity specified by the bidder on the bid Form or In case of a successful Bidder, if the Bidder fails:

- i. To accept the order
- ii. To furnish performance security
- iii. If the Vendor, after accepting the purchase order fails to deliver the material/services as per the order.

5. Any alterations, erasures or overwriting shall be valid only if the person or persons signing the bid initial them.

Signature of the Tenderer  
with stamp and date

## 6. **Scope of Work**

### **Purpose**

Government of Madhya Pradesh having their capital at Bhopal consists of 50 districts which are fully or partially computerized having different make and models of Desktop, Servers with different Operating Systems.

Government felt to implement a comprehensive security solution which safeguards enterprise assets and ensures total protection of geographically distributed Desktops, Servers and clients from all types of malicious software i.e. Virus, Worm, Trojans, Spam, Adware, Spyware etc. which can infiltrate and damage them. This tender is for Rate Contract for Suitable software as per need of the required computer environment. Since Government has kept data security in his paramount importance, the quotations are invited from the established vendors for providing Rate Contract for their Software & Solutions to achieve the above needs.

The Government of Madhya Pradesh has reserves the right to modify the scope of work / quantity of any item quoted against this tender enquiry as well as reserves the right to cancel the Rate Contract without assigning any reason.

### **SUBMISSION OF BIDS**

#### 7. **Sealing and Marking of Bids**

The bidders shall submit EMD, technical bid (containing the technical competence offered, etc and original copy of commercial bid in separate sealed, envelopes all the above envelopes shall be sealed in one main envelope. All the envelopes should be distinctly marked EMD, technical bid, and commercial bid.

#### 8. **Deadline for Submission of Bids**

Bids must reach to the competent authority at the address specified but not later than the time and date specified in the invitation of Bids. In the event of the specified date for the submission of bids being declared a holiday for the office of the competent authority, the bids will be received up to the appointed time on the next working day.

#### 9. **Late Bid**

Any bid received after the deadline for submission of bids prescribed by the competent authority, will not be accepted and returned unopened to the bidder.

### **BID OPENING AND EVALUATION OF BIDS**

#### 10. **Opening of Bids**

Since it is a Two-bid system, Technical and EMD envelope will be opened first by the Committee constituted for this purpose. If the technical bid specifications offered, EMD and deviations asked (if any) are found in order, the Committee will open commercial bid only for the eligible bidders.

The Committee will open the bids, in the presence of Bidders' representatives who choose to attend on the date specified at the following location:

Additional Chief General Manager  
M.P. State Electronics Dev. Corpn. Ltd.  
147, Zone-I, Maharana Pratap Nagar, BHOPAL-462011

Signature of the Tenderer  
with stamp and date

Prospective Bidder representatives shall sign a register evidencing their attendance.

In case, the commercial bid is not opened on the same or next day of opening of technical bid the Committee may decide to open the commercial bid on subsequent dates. In such case the date, time and place of opening of commercial bid will be intimated to the bidders or their representatives.

**11. Preliminary Examination**

Before starting evaluation, the bids will be examined to determine whether they are complete, whether any computational errors have been made, whether required sureties have been furnished, whether the documents have been properly signed, and whether the bids are generally in order. In case of computational error the basic price will prevail.

If bid is determined as not substantially responsive, the competent authority will reject it and only the substantially responsive commercial bids will be considered.

The process of evaluation of bid is as follows:

- (i) The Committee, appointed by the MPSEDC LTD. will first verify that the Bank Draft for Bid Security is in order and as per requirement of the bid. The Committee will examine the bid on Eligibility Criteria as specified. The scrutiny of technical proposals will be based on the Evaluation Criteria determined.
- (ii) The commercial bid will be opened only for the proposals, which are found eligible and technically acceptable by the Committee and approved. On the day specified for the opening of bid, the Committee, appointed by the MPSEDC LTD., will open the commercial bids of eligible bidders and scrutinize the same minutely.
- (iii) After scrutiny, the MPSEDC LTD. after having examined the proposal may accept the same or accept the bid price of any other bidder found suitable or reject all or any proposal. The decision of the MPSEDC LTD. in this regard shall be final and binding.
- (iv) The scope of work mentioned in the tender document is as per our estimate. However, software Supply is depending on the actual requirement of the deptt.

**12. Contacting the Competent Authority**

Any effort on part of a Bidder to influence the Competent Authority or members of Technical/Monitoring committee, in its decisions on bid evaluation; bid comparison or contact award may result in rejection of the bidder's bid.

**13. Statutory Obligations**

The agency has to ensure that the statutory obligations as per requirement of different rule and regulation. Any expenditure required shall be to the vendor's account. The agency shall submit the related documentary proof as and when required by MPSEDC.

**14. Applicable Law:**

The contract will be interpreted in accordance with the Laws of the union of India and Govt of MP.

**15. Rate Contract Agreement**

Offer for Agreement: After finalization of the rates by the Committee of MPSEDC on the basis of offers/tenders received, the rates will be offered to selected bidders for entering into Rate Contract Agreements. They have to sign the agreement within 10 days of the receipt of the communication

Signature of the Tenderer  
with stamp and date

failing which the earnest money may be forfeited. Agreement has to be executed on Non-judicial stamp paper of appropriate denomination, applicable as per rules.

16. **General**

- (i) Bid form shall be duly filled in, signed and complete in all respects.
- (ii) The price should be inclusive of all taxes.
- (iii) The rates should be free from all escalation.
- (iv) Supply and Installation period should not exceed 45 days from the date of order under any circumstances. The MPSEDC LTD. reserves the right to extend the delivery period, in the interest of the concerned deptt.
- (v) Antivirus should invariably be maintained and supported for a period of one year from the date of successful installation and commissioning.
- (vi) **Penalty** - In case of delay in execution of the order, the concern deptt. may as its option either:

Recover from the developer towards liquidated damages a sum @ ½% (half percent) of the price of software not delivered for a week, or Part thereof subject to maximum of 10% (ten percent). OR purchase from elsewhere on account and at the risk of developer, the Antivirus software not installed.

OR

Cancel the contract reserving concern deptt right to recover damages.

- (ix) The inner and outer envelopes shall be addressed to the competent authority at the following address:  
  
Additional Chief General Manager  
M.P. state Electronics dev. Corpo. Ltd  
147, Zone-I, Maharana Pratap Nagar, BHOPAL-462011
- (x) The envelopes shall also indicate the name and address of the Bidder to enable the bid to be returned unopened in case it is declared "late."
- (xi) If the outer envelope is not sealed and marked, the competent authority will assume no responsibility for the bids, misplacement or premature opening.
- (xii) Telex; cable facsimile or fax bids will be rejected.
- (xiii) Conditional bids are liable to be rejected.
- (xiv) MPSEDC Ltd.. does not bind themselves to accept the lowest or any other tender and reserve the right to accept or reject any or all the tender in full or in part without assigning any reason.

Signature of the Tenderer  
with stamp and date

## Financial Bid

Financial Bid must be submitted strictly under the given format

S.No.	Details	Cost (Rs.) Per box / Users	Taxes (Rs.)	Total Cost (Rs.)
01	<b>Desktop licence ( Box Pack/ Slim DVD)</b>			
02	<b>Network Version ( Box Pack)</b>			
	5 Users			
	10 Users			
	25 Users			
	50 Users			
	5000 Users			
03	<b>Network Version</b>			
	Network Version above 50 to 200			
	Network Version above 201 to 500			
	Network Version above 501 to 1000			
	Network Version above 1001 to 5000			

			Cost	Taxes	Total Cost
04	Annual up gradation and maintenance charges	1 <sup>st</sup> Year - .....% of quoted price 2 <sup>nd</sup> Year - .....% of Quoted Price			

Signature of the Tenderer  
with stamp and date

**Annexure 1**

**Enterprise Antivirus solution for Servers and Desktops**

<b>S/N</b>	<b>Requirement</b>	<b>Your Offer</b>
1	Software must provide Virus protection at Server and Desktop level and also regulated access control with Centralized Management through command centre	
2	Solution must provide automatic downloads of latest virus signature updates from the Internet to state windows desktops and servers. The distribution should happen seamlessly from a single management console	
3	Software must include audit trail logging and reporting capability. It should provide centralized log of all virus events on desktops and servers, including files checked, viruses found and responses taken	
4	Solution shall able to perform script filtering on JavaScript, Java Applets, ActiveX Controls or VB Script. Must protect against all kinds of viruses, trojan horses and worms including: boot sector, master boot sector, memory resident, file multipartite, macro etc.	
5	Must protect against spyware and adware	
6	Must support exclusion list by file extensions	
7	Must have quarantine capabilities so as to quarantine a system that has been infected	
8	Must scan USB pen drive, Floppy disks, CD ROM and Network Drives automatically in real-time when accessed	
9	Must scan compressed file archives in ZIP, ARJ and Microsoft Compressed formats. It should also protect from viruses hiding in compressed files, such as Internet downloads and e-mail attachments	
10	Must provide a variety of ways to handle viruses, including: cure, rename, move, report, delete or purge	
11	Must have the capability to automatically copy a file before curing - creating a temporary backup	
12	Must have heuristic scanning to allow rule-based detection of unknown viruses	
13	Shall support the following – Windows XP / Vista/ Windows 2003 (Standard / Enterprise Edition) and latest edition	

Signature of the Tenderer  
with stamp and date

14	Must be industry standard and with atleast one of the certifications like Tucows/ Check Mark/ CheckVir/ VB 100%	
15	Must be of latest technology like scanning for viruses before the Transport Layer without allowing the viruses to reach the system / application layer	
16	Solution must provide live alerts to Centralized Management Console about the critical activities being carried out on Client system	
17	Solution must provide Proactive scanning to detect unknown viruses on the fly.	
18	Solution must have a quarantine directory from where system administrator can collect samples and will be able to submit to the vendor.	
19	Solution must be able to deploy Endpoint Security to the clients	
20	Should support Integrated anti-virus/anti-spyware agent delivering real-time protection	
21	Should support feature to scan data as soon as it is accessed from the file system	
22	Should support static analysis and code emulation for addressing threats such as packers	
23	Should support tunneling signatures for detecting and removing rootkits: To Avoid evasion by relying on Tunnels rather than OS API	
24	Should support Event Flood Protection	
25	Should support Integrated and Single foot printed State Assessment Scans to detect Vulnerabilities	
26	Should support Dynamic Translation to Allow the anti-malware engine to generically decrypt malware that has tried to scramble its contents	
27	Should support In-depth scanning of unknown malware: By Dynamic Translation	
28	The solution should stop remote users from modifying system files	
29	It should stop remote users from creating executable files	
30	The solution should have incremental updates for dial-up users	
31	It should have the facility of scheduled scanning.	
32	It should give a pop-up alert box to the user to disinfect, delete, quarantine or block access to that file whenever an infection is found in it (user defined)	

Signature of the Tenderer  
with stamp and date

33	Have Centralized reporting system, both text and graphical	
34	Have detailed system information of all clients on the console	
35	Be able to be installed on Notebook Computers	
36	Be able to force an update (PUSH) to client	
37	Be able to detect clients in the network which DOES NOT have an AntiVirus and automatically install the same	
38	Be able to schedule a scan and clean clients from the Management console	
39	Must ensure real time protection even during the signature and engine updating process	

### Enterprise Anti-Virus for Email anti-virus and anti-spam

	<b>General Capabilities</b>	
	Software should provide capabilities such as anti-spam & content filtering (eg. Email), malicious code defence in addition to AntiVirus.	
	Should keep viruses and other web based threats out of the network, stopping them before they enter at the internet gateway. Should also provide integrated content filtering messages to prevent inappropriate content from reaching users	
	The solution should provide protection at multiple levels and at multiple checkpoints in the messaging infrastructure, including messaging SMTP gateway and Mailbox servers, helping to stop viruses, worms, and spam before they impact the network or user productivity.	
	The solution should have the ability to provide protection (ability to detect and correct) against Line Feed and Carriage Return, illegal MIME header attacks in email headers.	
	Should a zip archive file carrying multiple files have some malicious files, only the malicious files should be removed/cleaned and the rest should be passed on as it is to the intended recipient(s).	
	The solution should support uuencoded and compressed file integrity checks ; It should also have the capability to detect encrypted files and take appropriate action according to organization policy.	
	It should also be able to detect and restrict the number of nested attachments in a message and the number of nested compressed files.	
	Facility of blocking e-mail addresses from where we do not want to receive e-mails	
	<b>Antivirus protection</b>	
	Should provide comprehensive Antivirus protection against the latest threats and viruses by using multiple	

Signature of the Tenderer  
with stamp and date

	technologies like heuristics, signature, scan engines, etc.	
	The solution should provide functionality to run manual & quick scans on email message mailboxes on predefined schedules, in addition to realtime checks on incoming messages.	
	Scanning of emails should be supported in any of the following configurations:	
	Scanning of inbound mails ; Scanning of outbound mails; Scanning of internal mails ; Mailbox scanning ; On access scanning	
	It should be possible to quarantine messages with malicious code and provide notification to appropriate sender or receiver and the administrator.	
	In an outbreak scenario, it should be possible to scan email messages when they are accessed from the mailboxes with latest updated signature.	
	There should be a provision to scan messages in the mailboxes with the latest signatures which had been scanned earlier (1 day before or 5 days before, 1 week before, etc).	
	More than three Scan engines supported by independent labs should provided with the solution.	
	<b>Anti-Spam</b>	
	The solution should be a multi-layered spam protection leveraging different filtering technologies, including spam signatures, heuristics, reputation filters, language identification etc.	
	The solution should allow multiple allow and deny lists to provide flexible protection; The solution should support domain-level black and white lists.	
	The solution should proactively target patterns common in spam campaigns.	
	The solution should support DNS Based Distributed black lists.	
	The solution should provide IP based block-and-allow list based on sender reputation. These lists should be automatically updated as new versions become available. It should also allow administrators to configure additional IP allow-or-deny lists as needed.	
	It should support Tagging and forwarding of SPAM or likely SPAM messages.	
	It should be possible to tag email by insertion of tags either into the Email X-Header or the subject line so that the end user can be indicated of its possible contents.	
	It should employ checks based on Sender ID.	
	The solution should provide a choice of actions to be taken on Spam Mails. The action may be to just identify a type of message, tag a message, delete and or quarantine/archive a message or a combination of the above.	
	The solution should provide protection from Directory Harvest Attack.	
	It should be possible to detect and delete mails addressed to mails ids nonexistent in the organization.	
	<b>Filtering</b>	
	The solution should allow Administrators to quickly create	

Signature of the Tenderer  
with stamp and date

	custom organization-wide content filters to handle messages based on content, sender information, or other criteria.	
	It should allow File Filtering to block files based on the following parameters.	
	Type (true type); Size; Direction (inbound or outbound); Nested zip archives; Container documents	
	The solution should provide for keyword (body text) based filtering. It should filter messages based on a variety of words, phrases, and/or sentences. Also, a provision for administrators to download filter lists for profanity, racial discrimination, sexual discrimination, and spam should be made available.	
	<b>Performance</b>	
	The mail flow should not be affected/stopped/ or queued during definition updates	
	Should provide Multi-threaded and In-memory scanning to increase performance of the messaging server	
	<b>Reporting</b>	
	The solution should offer consolidated reporting which gives administrators visibility into aggregated filtering performance for deployed servers.	
	The solution should allow administrator to create E-Mail Notifications based on disposition or category of message.	
	<b>Management</b>	
	The solution should have provision for configuration backup and restore.	
	The solution should support quarantining of SPAM & virus emails	

## Secured & Fast Internet Access

It is desired to provide a Proxy, Caching, application layer filtering functionality and reduce bandwidth consumption on the Internet/WAN links and improving responses to a client accessing web based applications by the following methods.

1	<p><b>Secure Proxy:</b></p> <ul style="list-style-type: none"> <li>• The solution should provide for both, forward and reverse proxy capabilities.</li> <li>• It should provide for one or more networks to be configured, each with distinct relationships to other networks.</li> <li>• It should be possible to configure unique access policies per network.</li> <li>• The solution should be able to define routing relationships (Route and NAT network) between networks, depending on the type of access and communication required between the networks.</li> <li>• The proxy solution should provide for HTTP filtering on a per-rule basis along with deep HTTP stateful inspection</li> </ul>	
---	--	--

Signature of the Tenderer  
with stamp and date

	<p>(Application layer filtering)</p> <ul style="list-style-type: none"> <li>• The proxy should provide for ways to block/ control access to all executable content</li> <li>• The solution should provide granular access control to file downloads through file extension</li> <li>• The solution should provide inbound and outbound access control on User-based or group-based access policy</li> <li>• The solution should provide deep HTTP inspection that can help create "HTTP Signatures" that can be compared to the Request URL, Request headers, Request body, and Response body to get precise control over what content internal and external users can access</li> </ul>	
	<p><b>Advanced Caching:</b> is widely used as a method of improving network performance by serving content locally instead of retrieving it from the original with every request following are the desired specifications of the Web Caching functionality of the proposed solution:</p> <ul style="list-style-type: none"> <li>• The solution should support both in memory and fast access disk Caching. The proposed solution should be capable of caching large amount of content both on the disk as well as in the Random Access Memory (RAM). Objects that are frequently accessed should be stored on the RAM so that the time to retrieve such content from the Cache is considerably lower.</li> <li>• The solution should support both forward as well as Reverse Caching so that it offers flexibility of being placed either at the server or at the client end.</li> <li>• The solution should support scheduled download of content so that it can be stored in the cache even without a user requesting for it. This scheduling should be possible based on time, URL, Levels to download etc.</li> <li>• The proposed solution should support caching of The Background Intelligent Transfer Service (BITS) which helps you transfer large amounts of data without degrading network performance.</li> <li>• The solution should be capable of</li> </ul>	

Signature of the Tenderer  
with stamp and date

	<p>Caching objects that have an unspecified last modification time.</p> <ul style="list-style-type: none"> <li>• The solution should also be in a position to Cache Dynamic content, Content for Offline browsing and content requiring user authentication for retrieval.</li> <li>• The proposed solution should be capable of caching SSL responses</li> <li>• The solution should offer administrator configurable Time to live (TTL) for content in the cache. TTL should be specified as a percentage of the content age and should also support TTL boundaries even if the content doesn't have an expiration period specified.</li> </ul>	
	<p><b>HTTP compression:</b> reduces file size by using algorithms to eliminate redundant data. Most common Web-related file types can safely be compressed following are the details of the compression requirements of the proposed solution:</p> <ul style="list-style-type: none"> <li>○ The proposed solution should be capable of compression of HTTP traffic. The compression should be based on Open standards and should not use proprietary methods of compression. Open Standard should be preferably GZIP and deflate algorithms so as to ensure interoperability with different web applications.</li> <li>○ The proposed solution should be capable of requesting and responding with compressed HTTP traffic from web servers.</li> <li>○ The proposed solution should be lossless such that no content is lost in the compression or decompression process.</li> <li>○ The solution should provide flexibility to decide whether the compression is done on the following parameters: <ul style="list-style-type: none"> <li>▪ Source and/or Destination Networks</li> <li>▪ Specific Computer sets</li> <li>▪ Specific Content Type such as: <ul style="list-style-type: none"> <li>• Image Files (jpg,tiff,bmp etc)</li> <li>• Documents such as doc,xls ppt pdf etc</li> <li>• HTML</li> </ul> </li> </ul> </li> </ul>	

Signature of the Tenderer  
with stamp and date

	<ul style="list-style-type: none"> <li>• Text</li> <li>○ The solution should not compress video and audio traffic as these are already compressed and the compression and decompression exercise could introduce additional latency.</li> <li>○ The compression and decompression should be done on the application layer so as to provide granular control on content types to be compressed.</li> <li>○ The solution should be capable on compression of static as well as perform on-demand compression of dynamically generated responses before sending them over the network.</li> <li>○ The solution should support range compression which is the compression of a specific portion of Web content. Range compression is required to support legacy Portable Document Format (PDF) file readers that do not have built-in compression support.</li> <li>○ The solution should support caching and inspection of traffic which is compressed. It should do so by decompressing the content, followed by inspection and caching (if required) and should allow flexibility of sending the decompressed content to the end user. The solution should also support send the compressed content to the end user.</li> </ul>	
	<p><b>Traffic Prioritization:</b> should help the highest priority applications get precedence over other network traffic through Diffserv IP settings, providing better bandwidth utilization and response times for critical Web resources, the proposed solution should support Packet Prioritization (using Diff Serv).</p>	
	<p><b>Authentication Features and session management:</b> The proposed solution should support delegation of authentication in the following methods:</p> <ul style="list-style-type: none"> <li>• The solution should supported Directory integrated as well as Basic Authentication</li> <li>• The solution should support RADIUS for Web Proxy client authentication</li> <li>• The Solution should support Delegation of Basic authentication</li> <li>• The solution should support Single sign</li> </ul>	

Signature of the Tenderer  
with stamp and date

	<p>on for URL in a specified DNS domain.</p> <ul style="list-style-type: none"> <li>• The Solution should support Forms-based authentication; it should also offer the flexibility to administrators to define custom forms.</li> <li>• The solution should offer cookie-based as well as idle-time based session management.</li> <li>• The Solution should support LDAP authentication</li> <li>• The solution should also support One Time Passwords (OTPs)</li> <li>• The solution should support digital certification based authentication and the certificate revocation settings should be configurable by the administrator.</li> </ul>	
	<p><b>Application Layer filtering:</b> for Web protocols offers an enhanced level of security to web applications that are accessed through a browser. In this regards the proposed solution should support the following functionality.</p> <ul style="list-style-type: none"> <li>○ HTTP Policy: block applications, such as messaging applications or peer-to-peer file sharing applications, that tunnel over HTTP. HTTP policy should encompasses the following settings: <ul style="list-style-type: none"> <li>▪ Request header maximum length</li> <li>▪ Request payload length</li> <li>▪ URL Protection</li> <li>▪ Executable Blocking</li> <li>▪ Denied Methods</li> <li>▪ Specified actions for specific file extensions</li> <li>▪ Deny specific headers</li> <li>▪ Modify Server and Via headers</li> <li>▪ Deny specific signatures</li> </ul> </li> <li>○ The proposed solution should be capable of inspecting SSL traffic; it should also support pass through of SSL traffic.</li> <li>○ The solution should provide application layer filtering</li> </ul>	
	<p><b>Advanced Firewall Protection</b></p> <p>The solution should also support a multi layer firewall capabilities such as:</p> <ul style="list-style-type: none"> <li>• Packet filtering (circuit-layer filtering)</li> <li>• Stateful filtering</li> <li>• Application layer firewall (with built in</li> </ul>	

Signature of the Tenderer  
with stamp and date

	<p>filters)</p> <p>The solution should provide for:</p> <ul style="list-style-type: none"> <li>• Block access to all executable content</li> <li>• Control HTTP file downloads through file extension</li> <li>• Control HTTP access based on "HTTP Signatures"</li> <li>• Control allowed HTTP methods</li> <li>• Extensive protocol support</li> <li>• Support for complex protocols requiring multiple primary connections</li> <li>• Granular control over IP options</li> <li>• Port redirection for FTP server publishing rules</li> <li>• Flood Resiliency</li> </ul> <p>Enhanced remediation during attack (worm attacks)</p>	
--	---	--

Signature of the Tenderer  
with stamp and date