

Request for Quotation for:

State of West Virginia -Department of Education



INTERNET FILTERING AND REPORTING SOLUTION – RFQ #EDD327891

Prepared by Michael Hartley
michael.hartley@telemate.net

678.589.3630



TeleMate.Net Software
5555 Triangle Parkway, NW
Suite 150
Norcross, GA 30092
Tel: 678.589.7100
Fax: 678.589.7110

www.telemate.net

RECEIVED

2010 MAY 13 A 10:09

PURCHASING DIVISION
STATE OF WV

Attn:

Buyer: Shelly Murray
TELEPHONE: (304)558-8801
State of West Virginia
Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

Dear Ms. Murray,

TeleMate.Net Software would like to thank you for your consideration in response to the Request for Quotation for The State of West Virginia Department of Education for Internet Filtering and Reporting Solution. As an industry leader since 1986 TeleMate.Net Software is confident in our ability to provide the State and Departments the highest quality solution with exceptional customer services. As an organization our goal is to under promise and over deliver in every aspect of a deployment beginning in the sales process, customer acceptance, initial deployment, and in subsequent years of services.

In response to the enclosed proposal, we have provided responses to all Sections. TeleMate.Net Software accepts all statements and conditions to these statements as defined and welcomes and opportunity to participate in the process

As specified in the Notice for Proposal all responses are provided in the format of the request.

Thank you for your consideration.

Regards,

Michael Hartley
District Sales, Federal



www.telemate.net
michael.hartley@telemate.net

Global leader in Network Monitoring and Security Solutions

678.589.3630 Direct / 678.589.7100 Corporate
678.589.7110 Fax

5555 Triangle Parkway, Suite 150
Norcross, Georgia 30092



State of West Virginia
 Department of Administration
 Purchasing Division
 2019 Washington Street East
 Post Office Box 50130
 Charleston, WV 25305-0130

Request for Quotation

RFQ NUMBER:
EDD327891

PAGE
1

ADDRESS CORRESPONDENCE TO ATTENTION OF:
**SHELLY MURRAY
 304-558-8801**

RFQ COPY

TYPE NAME/ADDRESS HERE

VENDOR

**TeleMate.Net Software, LLC
 5555 Triangle Parkway, Suite 150
 Norcross, GA 30092**

PURCHASER


**DEPARTMENT OF EDUCATION
 BUILDING 6
 1900 KANAWHA BOULEVARD, EAST
 CHARLESTON, WV
 25305-0330**

DATE PRINTED: 04/05/2010	TERMS OF SALE	SHIP VIA	FOB	FREIGHT TERMS
------------------------------------	---------------	----------	-----	---------------

BID OPENING DATE: **05/13/2010** BID OPENING TIME **01:30PM**

LINE	QUANTITY	UOP	CAT NO.	ITEM NUMBER	UNIT PRICE	AMOUNT
0001	1	LS		920-45		
<p>THE WEST VIRGINIA PURCHASING DIVISION, FOR THE AGENCY, THE WEST VIRGINIA DEPARTMENT OF EDUCATION, IS SOLICITING BIDS FOR AN INTERNET FILTERING AND REPORTIN SOLUTION PER THE ATTACHED SPECIFICATIONS.</p> <p>TECHNICAL QUESTIONS MUST BE SUBMITTED IN WRITING TO SHELLY MURRAY IN THE WEST VIRGINIA PURCHASING DIVISION VIA MAIL AT THE ADDRESS SHOWN AT THE TOP OF THIS RFQ, VIA FAX AT 304-558-4115, OR VIA E-MAIL AT SHELLY.L.MURRAY@WV.GOV. DEADLINE FOR ALL TECHNICAL QUESTIONS IS 04/27/2010 AT THE CLOSE OF BUSINESS. ALL TECHNICAL QUESTIONS RECEIVED, IF ANY, WILL BE ADDRESSED BY ADDENDUM AFTER THE DEADLINE.</p> <p>INTERNET FILTERING AND REPORTING SOLUTION</p> <p>EXHIBIT 3</p> <p>LIFE OF CONTRACT: THIS CONTRACT BECOMES EFFECTIVE UPON AWARD AND EXTENDS FOR A PERIOD OF ONE (1) YEAR OR UNTIL SUCH "REASONABLE TIME" THEREAFTER AS IS NECESSARY TO OBTAIN A NEW CONTRACT OR RENEW THE ORIGINAL CONTRACT. THE "REASONABLE TIME" PERIOD SHALL NOT EXCEED TWELVE (12) MONTHS. DURING THIS "REASONABLE TIME" THE VENDOR MAY TERMINATE THIS CONTRACT FOR ANY REASON UPON GIVING THE DIRECTOR OF PURCHASING 30 DAYS WRITTEN NOTICE.</p>						

SEE REVERSE SIDE FOR TERMS AND CONDITIONS

SIGNATURE  TELEPHONE **678.589.7100** DATE **5/12/2010**

TITLE **President** FEIN **26 3330752** ADDRESS CHANGES TO BE NOTED ABOVE

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'

GENERAL TERMS & CONDITIONS REQUEST FOR QUOTATION (RFQ) AND REQUEST FOR PROPOSAL (RFP)

1. Awards will be made in the best interest of the State of West Virginia.
2. The State may accept or reject in part, or in whole, any bid.
3. Prior to any award, the apparent successful vendor must be properly registered with the Purchasing Division and have paid the required \$125 fee.
4. All services performed or goods delivered under State Purchase Order/Contracts are to be continued for the term of the Purchase Order/Contracts, contingent upon funds being appropriated by the Legislature or otherwise being made available. In the event funds are not appropriated or otherwise available for these services or goods this Purchase Order/Contract becomes void and of no effect after June 30.
5. Payment may only be made after the delivery and acceptance of goods or services.
6. Interest may be paid for late payment in accordance with the *West Virginia Code*.
7. Vendor preference will be granted upon written request in accordance with the *West Virginia Code*.
8. The State of West Virginia is exempt from federal and state taxes and will not pay or reimburse such taxes.
9. The Director of Purchasing may cancel any Purchase Order/Contract upon 30 days written notice to the seller.
10. The laws of the State of West Virginia and the *Legislative Rules* of the Purchasing Division shall govern the purchasing process.
11. Any reference to automatic renewal is hereby deleted. The Contract may be renewed only upon mutual written agreement of the parties.
12. **BANKRUPTCY:** In the event the vendor/contractor files for bankruptcy protection, the State may deem this contract null and void, and terminate such contract without further order.
13. **HIPAA BUSINESS ASSOCIATE ADDENDUM:** The West Virginia State Government HIPAA Business Associate Addendum (BAA), approved by the Attorney General, is available online at www.state.wv.us/admin/purchase/vrc/hipaa.htm and is hereby made part of the agreement. Provided that the Agency meets the definition of a Cover Entity (45 CFR §160.103) and will be disclosing Protected Health Information (45 CFR §160.103) to the vendor.
14. **CONFIDENTIALITY:** The vendor agrees that he or she will not disclose to anyone, directly or indirectly, any such personally identifiable information or other confidential information gained from the agency, unless the individual who is the subject of the information consents to the disclosure in writing or the disclosure is made pursuant to the agency's policies, procedures, and rules. Vendor further agrees to comply with the Confidentiality Policies and Information Security Accountability Requirements, set forth in <http://www.state.wv.us/admin/purchase/privacy/noticeConfidentiality.pdf>.
15. **LICENSING:** Vendors must be licensed and in good standing in accordance with any and all state and local laws and requirements by any state or local agency of West Virginia, including, but not limited to, the West Virginia Secretary of State's Office, the West Virginia Tax Department, and the West Virginia Insurance Commission. The vendor must provide all necessary releases to obtain information to enable the director or spending unit to verify that the vendor is licensed and in good standing with the above entities.
16. **ANTITRUST:** In submitting a bid to any agency for the State of West Virginia, the bidder offers and agrees that if the bid is accepted the bidder will convey, sell, assign or transfer to the State of West Virginia all rights, title and interest in and to all causes of action it may now or hereafter acquire under the antitrust laws of the United States and the State of West Virginia for price fixing and/or unreasonable restraints of trade relating to the particular commodities or services purchased or acquired by the State of West Virginia. Such assignment shall be made and become effective at the time the purchasing agency tenders the initial payment to the bidder.

I certify that this bid is made without prior understanding, agreement, or connection with any corporation, firm, limited liability company, partnership, or person or entity submitting a bid for the same material, supplies, equipment or services and is in all respects fair and without collusion or fraud. I further certify that I am authorized to sign the certification on behalf of the bidder or this bid.

INSTRUCTIONS TO BIDDERS

1. Use the quotation forms provided by the Purchasing Division. Complete all sections of the quotation form.
2. Items offered must be in compliance with the specifications. Any deviation from the specifications must be clearly indicated by the bidder. Alternates offered by the bidder as **EQUAL** to the specifications must be clearly defined. A bidder offering an alternate should attach complete specifications and literature to the bid. The Purchasing Division may waive minor deviations to specifications.
3. Unit prices shall prevail in case of discrepancy. All quotations are considered F.O.B. destination unless alternate shipping terms are clearly identified in the quotation.
4. All quotations must be delivered by the bidder to the office listed below prior to the date and time of the bid opening. Failure of the bidder to deliver the quotations on time will result in bid disqualifications: Department of Administration, Purchasing Division, 2019 Washington Street East, P.O. Box 50130, Charleston, WV 25305-0130
5. Communication during the solicitation, bid, evaluation or award periods, except through the Purchasing Division, is strictly prohibited (W.Va. C.S.R. §148-1-6.6).



State of West Virginia
 Department of Administration
 Purchasing Division
 2019 Washington Street East
 Post Office Box 50130
 Charleston, WV 25305-0130

Request for Quotation

RFQ NUMBER
EDD327891

PAGE
2

ADDRESS CORRESPONDENCE TO ATTENTION OF
**SHELLY MURRAY
 304-558-8801**

POSTER

RFQ COPY
 TYPE NAME/ADDRESS HERE

**TeleMate.Net Software, LLC
 5555 Triangle Parkway, Suite 150
 Norcross, GA 30092**

SHIP TO

**DEPARTMENT OF EDUCATION
 BUILDING 6
 1900 KANAWHA BOULEVARD, EAST
 CHARLESTON, WV
 25305-0330**

DATE PRINTED 04/05/2010	TERMS OF SALE	SHIP VIA	F.O.B.	FREIGHT TERMS
BID OPENING DATE: 05/13/2010		BID OPENING TIME 01:30PM		

LINE	QUANTITY	UOP	CAT NO.	ITEM NUMBER	UNIT PRICE	AMOUNT
<p>UNLESS SPECIFIC PROVISIONS ARE STIPULATED ELSEWHERE IN THIS CONTRACT DOCUMENT, THE TERMS, CONDITIONS AND PRICING SET HEREIN ARE FIRM FOR THE LIFE OF THE CONTRACT.</p> <p>RENEWAL: THIS CONTRACT MAY BE RENEWED UPON THE MUTUAL WRITTEN CONSENT OF THE SPENDING UNIT AND VENDOR, SUBMITTED TO THE DIRECTOR OF PURCHASING THIRTY (30) DAYS PRIOR TO THE EXPIRATION DATE. SUCH RENEWAL SHALL BE IN ACCORDANCE WITH THE TERMS AND CONDITIONS OF THE ORIGINAL CONTRACT AND SHALL BE LIMITED TO TWO (2) ONE (1) YEAR PERIODS.</p> <p>CANCELLATION: THE DIRECTOR OF PURCHASING RESERVES THE RIGHT TO CANCEL THIS CONTRACT IMMEDIATELY UPON WRITTEN NOTICE TO THE VENDOR IF THE COMMODITIES AND/OR SERVICES SUPPLIED ARE OF AN INFERIOR QUALITY OR DO NOT CONFORM TO THE SPECIFICATIONS OF THE BID AND CONTRACT HEREIN.</p> <p>OPEN MARKET CLAUSE: THE DIRECTOR OF PURCHASING MAY AUTHORIZE A SPENDING UNIT TO PURCHASE ON THE OPEN MARKET, WITHOUT THE FILING OF A REQUISITION OR COST ESTIMATE, ITEMS SPECIFIED ON THIS CONTRACT FOR IMMEDIATE DELIVERY IN EMERGENCIES DUE TO UNFORESEEN CAUSES (INCLUDING BUT NOT LIMITED TO DELAYS IN TRANSPORTATION OR AN UNANTICIPATED INCREASE IN THE VOLUME OF WORK.)</p> <p>BANKRUPTCY: IN THE EVENT THE VENDOR/CONTRACTOR FILES FOR BANKRUPTCY PROTECTION, THE STATE MAY DEEM THE CONTRACT NULL AND VOID, AND TERMINATE SUCH CONTRACT WITHOUT FURTHER ORDER.</p> <p>THE TERMS AND CONDITIONS CONTAINED IN THIS CONTRACT SHALL SUPERSEDE ANY AND ALL SUBSEQUENT TERMS AND CONDITIONS WHICH MAY APPEAR ON ANY ATTACHED PRINTED</p>						

SEE REVERSE SIDE FOR TERMS AND CONDITIONS			
SIGNATURE 	TELEPHONE 678.589.7100	DATE 5/12/2010	
TITLE President	FERN 26 3330752	ADDRESS CHANGES TO BE NOTED ABOVE	

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'



State of West Virginia
 Department of Administration
 Purchasing Division
 2019 Washington Street East
 Post Office Box 50130
 Charleston, WV 25305-0130

Request for Quotation

RFQ NUMBER
EDD327891

PAGE
3

ADDRESS CORRESPONDENCE TO ATTENTION OF
**SHELLY MURRAY
 304-558-8801**

VENDOR

RFQ COPY
 TYPE NAME/ADDRESS HERE

**TeleMate.Net Software, LLC
 5555 Triangle Parkway, Suite 150
 Norcross, GA 30092**

SHIP TO

**DEPARTMENT OF EDUCATION
 BUILDING 6
 1900 KANAWHA BOULEVARD, EAST
 CHARLESTON, WV
 25305-0330**

DATE PRINTED	TERMS OF SALE	SHIP VIA	F.O.B.	FREIGHT TERMS
04/05/2010				
BID OPENING DATE: 05/13/2010		BID OPENING TIME 01:30PM		

LINE	QUANTITY	UOP	CAT NO	ITEM NUMBER	UNIT PRICE	AMOUNT
<p>DOCUMENTS SUCH AS PRICE LISTS, ORDER FORMS, SALES AGREEMENTS OR MAINTENANCE AGREEMENTS, INCLUDING ANY ELECTRONIC MEDIUM SUCH AS CD-ROM.</p> <p>NOTICE</p> <p>A SIGNED BID MUST BE SUBMITTED TO:</p> <p>DEPARTMENT OF ADMINISTRATION PURCHASING DIVISION BUILDING 15 2019 WASHINGTON STREET, EAST CHARLESTON, WV 25305-0130</p> <p>THE BID SHOULD CONTAIN THIS INFORMATION ON THE FACE OF THE ENVELOPE OR THE BID MAY NOT BE CONSIDERED:</p> <p>SEALED BID</p> <p>BUYER: SHELLY MURRAY</p> <p>RFQ. NO.: EDD327891</p> <p>BID OPENING DATE: 05/13/2010</p> <p>BID OPENING TIME: 1:30 PM</p> <p>PLEASE PROVIDE A FAX NUMBER IN CASE IT IS NECESSARY TO CONTACT YOU REGARDING YOUR BID:</p>						

SEE REVERSE SIDE FOR TERMS AND CONDITIONS			
SIGNATURE 	TELEPHONE 678.589.7100	DATE 5/12/2010	
TITLE President	FEIN 26 3330752	ADDRESS CHANGES TO BE NOTED ABOVE	

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'



State of West Virginia
 Department of Administration
 Purchasing Division
 2019 Washington Street East
 Post Office Box 50130
 Charleston, WV 25305-0130

Request for Quotation

RFQ NUMBER
EDD327891

PAGE
4

ADDRESS CORRESPONDENCE TO ATTENTION OF:
**SHELLY MURRAY
 304-558-8801**

VENDOR

RFQ COPY
 TYPE NAME/ADDRESS HERE
**TeleMate.Net Software, LLC
 5555 Triangle Parkway, Suite 150
 Norcross, GA 30092**

SHIP TO

DEPARTMENT OF EDUCATION
 BUILDING 6
 1900 KANAWHA BOULEVARD, EAST
 CHARLESTON, WV
 25305-0330

DATE PRINTED 04/05/2010	TERMS OF SALE	SHIP VIA	F.O.B.	FREIGHT TERMS
-----------------------------------	---------------	----------	--------	---------------

BID OPENING DATE: **05/13/2010** BID OPENING TIME **01:30PM**

LINE	QUANTITY	UOP	CAT. NO.	ITEM NUMBER	UNIT PRICE	AMOUNT
CONTACT PERSON (PLEASE PRINT CLEARLY): ----- Michael Hartley Office: 678.589.3630 Fax: 678.589.7110 Michael.hartley@telemate.net ***** THIS IS THE END OF RFQ EDD327891 ***** TOTAL: _____						

SEE REVERSE SIDE FOR TERMS AND CONDITIONS

SIGNATURE 	TELEPHONE 678.589.7100	DATE 5/12/2010
TITLE President	FEIN 26 3330752	ADDRESS CHANGES TO BE NOTED ABOVE

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'

West Virginia Department of Education REQUEST FOR QUOTATION EDD327891

Introduction

The West Virginia Department of Education (WVDE) is soliciting quotations for an **Internet filtering and reporting solution** that consists of software, licensing, software upgrades/updates, database updates and technical support. The vendor has the option to include servers or appliances and associated costs in the quotation if the vendor's software will not meet the requirements of this RFQ when installed on WVDE owned servers which are described in Section I-Current Environment.

Throughout this Request for Quotation (RFQ) the term "filtering solution" is used to refer to all vendor provided software and hardware used to perform Internet filtering and reporting functions, including but not limited to application software, operating system and database software.

The terms "server" and "servers" are used to refer to the hardware or appliances on which any component of the filtering solution is installed.

Every statement of this RFQ that includes the word "must" or "shall" is a mandatory requirement. A vendor should not submit a bid if the filtering solution cannot meet every mandatory requirement.

The products and services that are bid **must** be capable of providing a level of service appropriate for Internet Service Provider (ISP) facilities with 3 gigabits of Internet bandwidth. School based or district based filtering solutions are not an acceptable response to this RFQ.

Comply ✓

The WVDE currently has two independent Internet connections for the K-12 public schools. Internet filtering solutions **must** be installed at both Points of Presence (POP). Because of the diverse needs of schools, the WVDE **must** have selective filtering levels and capabilities for delegated administration of tailored filtering policies or profiles for different subnets. Updates to the filtering solution **must** be provided at least once each day to ensure that the filtering database is up-to-date using multiple methods and resources for the review of content on Internet sites. The Internet filtering **must** meet the requirements of the E-rate program (refer to <http://www.sl.universalservice.org/>) and the West Virginia Board of Education Policy 2460 that is available online at <http://wvde.state.wv.us/policies/p2460.html>. Information relevant to the Children's Internet Protection Act (CIPA) and the Federal requirement to implement Internet filtering is detailed at the URL <http://www.fcc.gov/cgb/consumerfacts/cipa.html>.

The Children's' Online Privacy Protection Act (COPPA) **must** not be violated by any requirements of the filtering solution to collect personal information about students. Refer to <http://www.ftc.gov/coppa/> for information about COPPA.

Section I – Current Environment

Comply ✓

Approximately 700 public schools in 57 school districts of West Virginia are connected with a privately addressed TCP/IP statewide network. The network uses the private Class A range of 10.0.0.0 IP addresses. The POPs are equipped with Cisco 6513 switches that contain Cisco router and Cisco PIX firewall modules that route and translate the private IP addresses to our Class B 168.216.0.0 public network IP addresses. A Packeteer appliance is used to manage bandwidth. The Internet filtering **shall** be done at the two POPs where the K-12 network is routed to the ISP. The POPs are located in the WVNET facilities in Morgantown, WV and in the IS&C facilities at Building 6 of the State Capitol Complex at Charleston, WV. Each one of the two POPs connects approximately 70,000 unique computers to the Internet with 3 gigabits/second of bandwidth.

POP Site #1 Charleston, WV, is equipped with the following WVDE owned servers on which the filtering solution may be installed.

8 (eight) Dell 2850 servers with following specifications:
3 GHz XEON Processor with 2 MB cache, 2 GB DDR2 dimm, dual 73GB scsi drives in mirrored RAID, dual onboard gigabit copper ethernet NICs.

1 (one) Dell 2850 servers with following specifications:
3 GHz XEON Processor with 2 MB cache, 2 GB DDR2 dimm, dual 73GB scsi drives in mirrored RAID, dual onboard gigabit copper ethernet NICs, and one 1 TB storage for reports and log files.

POP Site #2 Morgantown, WV, is equipped with the following WVDE owned servers on which the filtering solution may be installed:

8 (eight) Dell 2850 servers with following specifications:
3 GHz XEON Processor with 2 MB cache, 2 GB DDR2 dimm, dual 73GB scsi drives in mirrored RAID, dual onboard gigabit copper ethernet NICs.

1 (one) Dell 2850 servers with following specifications:
3 GHz XEON Processor with 2 MB cache, 2 GB DDR2 dimm, dual 73GB scsi drives in mirrored RAID, dual onboard gigabit copper ethernet NICs, and one 1 TB storage for reports and log files.

Comply ✓

If the servers described above are not adequate to support the vendor's filtering solution, the vendor **must** include appropriate servers or appliances and associated costs in the response to this RFQ.

Comply ✓

The total number of computers to be filtered is approximately 140,000 computers. The Internet filtering **must** occur at the point in the network after which the K-12 core routers consolidate Internet traffic but before the firewall dynamically changes the private IP addresses to public IP addresses as shown in the diagram on attachment A. The filtering servers and reporting servers **must** operate within the scope of the K-12 private network so that filtering control and reporting will reflect the private IP addresses of the client computers. In the event that portable computers are connected to residential, public, or other

networks, an option **must** be available to provide continued filtering of Internet web sites. No caching appliances are currently in use; however the Internet filtering solution **must** support the option for the WVDE to install caching appliances.

Section II - Technical Requirements

General

- Comply ✓ The vendor bid **must** provide an Internet filtering solution capable of filtering 140,000 total computers in a network consisting of two POPs. The solution **must** be configured to support 70,000 client computers using 3 gigabits/sec of bandwidth at each POP.
- Comply ✓ The vendor **must** provide evidence of at least one current, successful installation of the Internet filtering solution in a network configuration servicing 70,000 computers with 3 gigabits/second of Internet bandwidth.
- Comply ✓ The filtering solution **must** be a POP based installation; a filtering solution which involves the installation of filtering software or hardware school districts or individual schools is not acceptable.
- Comply ✓ The vendor **must** provide Internet filtering and reporting application software and all necessary supporting software including, but not limited to, operating system and database software.
- Comply ✓ The Internet filtering solution **must** meet the requirements of this RFQ using servers/appliances provided by the vendor or when installed on the WVDE owned equipment identified in Section I – Current Environment.
- Comply ✓ The WVDE will provide server hardware, equipment racks, networking components and cabling as specified in Section I – Current Environment.
- Comply ✓ The filtering solution **must** support gigabit speed, copper based, Ethernet network interfaces.
- Comply ✓ The filtering solution **must** not exceed a total of 12 servers or appliances at each POP.
- Comply ✓ The total of all hardware components of the filtering solution for each POP **must** be rack mountable and not occupy more than 24 units of rack space (about 48”) at each POP site. The equipment **must** operate on 110-120 Volts AC power.
- Comply ✓ In the event the winning bid does not meet the requirements of this RFQ when installed on vendor provided server/appliances or on the existing equipment identified in Section I- Current Environment, the vendor **must** provide additional servers and any other associated installation, shipping, labor and configuration expenses at no cost to the WVDE or the contract will be immediately terminated.
- Comply ✓ There **must** be no requirement for any configuration changes of any networking equipment or computers that are connected to the private WV K-12 network at the school districts or individual schools

- Comply** ✓ The filtering solution **must** provide client software which can be installed on mobile computers that will enforce the same filtering parameters whether a mobile computer is connected to the WV K-12 network or connected by wired or wireless networking to the Internet via any other Internet service provider. The client software **must** not be a VPN (virtual private networking) or similar type of client and **must** not rely on a web browser setting such as a proxy server configuration.
- Comply** ✓ The filtering solution **must** have the capability to filter based on the IP address of the client computer and not require user authentication.
- Comply** ✓ The filtering solution **must** have the capability to be integrated with unified authentication systems such as LDAP and Active Directory service.
- Comply** ✓ The Internet filtering solution **must** be engineered and operate with redundancy such that the failure of one server or appliance at a POP will not reduce the capability to provide filtering for 70,000 computers at 3 gigabits/sec of throughput.
- Comply** ✓ The vendor **must** begin installation no later than 30 days after receipt of the purchase order and must be completed within 60 days of receipt of the purchase order.

Internet Filtering

- Comply** ✓ The filtering solution **must** provide a web based interface for all management and configuration tasks which can be performed by WVDE.
- Comply** ✓ The filtering solution **must** have the capability to be configured to block Internet access in the event of the failure of the filtering solution at a POP so that unfiltered Internet access is prevented.
- Comply** ✓ The Internet filtering provided as a result of this RFQ **must** be verified by the vendor to meet the requirements of the Children's Internet Protection Act (CIPA) (refer to <http://www.fcc.gov/cgb/consumerfacts/cipa.html>) and the West Virginia Board of Education Policy 2460 that is available online at <http://wvde.state.wv.us/policies/p2460.html>.
- Comply** ✓ The filtering solution **must** be verified by the vendor to comply with the Children's Online Privacy Protection Act (COPPA). The filtering process **must** not require the collection of any personal information from any users under the age of 13.
- Comply** ✓ The filtering solution **must** provide the capability for the WVDE to selectively enable filtering of content based on categories of web sites or individual web sites using the http and https protocols.
- Comply** ✓ The vendor **must** include all categories that the vendor offers on the product. The vendor **must** not offer a reduced number of categories in an attempt to reduce costs by providing only the categories that are identified in this RFQ.
- Comply** ✓ The vendor **must** provide, but is not limited to, the pre-populated categories of the following classifications or equivalent classifications of content on web sites:

- Pornography
- Obscenity
- Dating (including sites for the purpose of establishing personal relationships)
- Gambling
- Criminal Activities (sites that condone or provide instructions for criminal activity)
- Illegal Drugs (sites that condone or provide instructions for illegal drug use, manufacturing and distribution)
- Anonymous Proxies (anonymizers to bypass filtering or hide the true source of Internet activity)
- Computer crimes, cracking and hacking (sites that condone or provide instructions for these activities)
- Malicious code (sites that contain, distribute, or execute malicious code such as malware, viruses, root kits, bots, etc or retrieve information from computers that are infected with malicious code)
- Instant messaging sites
- Peer to Peer (P2P sites)
- Phishing (fraudulent sites that imitate authentic sites, often to lure people into submitting personal or financial information.)
- Hate, racism, discrimination (sites that condone or encourage violence against or suppression of any minorities or grouping based on race, religion, sexual orientation, ethnicity or any other social grouping characteristic)

- Comply** ✓ The filtering solution **must** have the capability to allow or deny access to any individual web site, URL, or IP address whether or not it is included in any vendor provided category.
- Comply** ✓ The filtering solution **must** have the capability to permit the WVDE to create unlimited additional custom categories.
- Comply** ✓ The filtering solution **must** have the capability to permit the use of “regular expressions” (includes wild-card characters and other variables to specify complex text strings) when creating custom allow or deny lists of URL web addresses or search terms.
- Comply** ✓ The filtering solution **must** have the capability to block traffic related to peer-to-peer file sharing protocols.

- Comply ✓ The filtering solution **must** have the capability to enforce the “safe searching” mode of Google, Bing and Yahoo search engines, regardless of the settings chosen by an end user that is using those search engines.
- Comply ✓ The filtering solution **must** provide capabilities to create manageable client groups based on IP address ranges and assign names to those groups.
- Comply ✓ The capability **must** exist to delegate management of groups by creating additional administrators with restricted rights who can be assigned to manage filtering parameters for specific groups.
- Comply ✓ The filtering solution **must** provide for customizable, granular permissions so that additional administrator/user accounts can be tailored on a user by user basis to match the rights of a user to the tasks that a user needs to perform.
- Comply ✓ The filtering solution **must** have the capability to selectively display WVDE customized “site blocked” pages based on the client group and/or the categorization of the blocked web site.
- Comply ✓ The filtering solution **must** have the capability to selectively display WVDE customized “informational” pages based on the client group and/or the categorization of web sites to which access is allowed.
- Comply ✓ The filtering solution **must** have the capability to be configured to only perform filtering of outgoing requests and to perform no filtering of incoming traffic.
- Comply ✓ The product offered by the vendor **must** perform Internet filtering primarily by comparing outgoing requests to a database of categorized URLs and IP addresses to determine whether an attempt to access a site on the Internet is to be blocked or permitted.
- Comply ✓ Any other Internet filtering methods of the filtering solution, such as “on the fly” evaluation of incoming content, **must** be able to be selectively disabled at the option of the WVDE.
- Comply ✓ The filtering solution **must** provide a web based display of status and performance graphs for all components of the filtering solution.
- Comply ✓ The filtering solution **must** have the capability for the WVDE to set customized filtering policies based on the time of day and the day of the week for individual IP addresses and/or groups of client IP addresses.
- Comply ✓ The Internet filtering solution **must** not masquerade, spoof or change the source IP address of the computers on the K-12 network. The source IP address of the client computer **must** be passed to the PIX firewall.
- Comply ✓ The Internet filtering and reporting servers **must** operate on and report on the 10.0.0.0 private network IP addresses of the WVDE K-12 network.

- Comply** ✓ The filtering solution **must** have a synchronization capability. Synchronization means that when the WVDE makes a filtering configuration change using the web management tool, that change will be distributed to all of the filtering servers at both POPs. That change distribution **must** take effect automatically within 5 minutes after the act of saving of the configuration change, or be accomplished manually with no more than 5 mouse clicks after the configuration change is saved.

Internet Use Reporting

- Comply** ✓ The filtering solution **must** provide a web-based reporting application and a minimum of one terabyte of log file storage at each POP.
- Comply** ✓ The filtering solution **must** provide a method for the WVDE to download log files in a generic text format for analysis and archival storage.
- Comply** ✓ Complete details of web browsing activity **must** be stored in log files and **must** include, at a minimum, the complete URL, date and time and IP address of the client computer.
- Comply** ✓ All end user functions of the reporting application **must** be accessible via a web interface.
- Comply** ✓ The reporting solution **must** provide the capability to create reports based on specific IP address, web site address, date and time of day.
- Comply** ✓ The reporting capabilities **must** include the ability to schedule aggregate reports of web site accesses by categories, ranges of IP addresses and time periods.
- Comply** ✓ The reporting capabilities **must** include the ability to create "on demand" custom reports on selected client IP addresses, specific URLs and time periods.

Section III - Contract Terms

The contract that results from this RFQ will remain in effect for one (1) year from the date of award, with an option to renew for two (2) additional one (1) year periods.

- Comply** ✓ The costs for software and the annual licensing for Internet filtering can be invoiced upon delivery and acceptance by the WVDE. The technical support costs are payable in arrears and **shall** be invoiced not more often than on a monthly basis.
- Comply** ✓ Any terms and conditions **must** be submitted with the bid. After award, no changes will be allowed which modify and terms and conditions. Award will not be made until all terms and conditions are agreed to by the State.

The vendor is solely responsible for all work performed under the contract and for all services offered and products to be delivered under the terms of this contract.

- Comply** ✓ If the successful vendor is not the direct source, the vendor **must** provide documentation of being an authorized reseller to provide the equipment, filtering updates, maintenance and technical support.

Section IV - Service Requirements

Comply ✓

The vendor **must** provide modification or replacement of software that fails to perform according to the specifications. The vendor also **must** provide any software upgrades, at no cost to the State, that are necessary during the term of the contract in order to continue to meet the Internet filtering capabilities specified. This requirement includes replacement, at no cost to the State, which may be necessary due to possible end-of-life designation by the manufacturer.

The WVDE network staff will provide and maintain WVDE provided servers, associated networking hardware and wiring. The WVDE network engineers will be responsible for load balancing network traffic to the servers of the filtering solution. The WVDE will be responsible for purchasing additional servers and network hardware when necessary to accommodate increases in bandwidth the number of clients to be filtered.

Comply ✓

The filtering solution installation, configuration and testing at both the Charleston and Morgantown sites **must** be completed by the vendor within 30 days after the award of the contract. The vendor is responsible for any transportation and lodging costs of the installer.

Comply ✓

The Internet filtering **must** support the bandwidth requirements of 3 gigabits/sec and 70,000 client computers at each one of the two POPs as identified in the specifications in Section II- Technical Requirements.

The vendor understands that technical support includes verifying that all hardware and/or software remains operational in the event of WVDE modification, replacement or upgrade of any servers or network configurations that impact the functioning of the filtering solution. These costs are to be included in the line item for technical support on the cost page.

Comply ✓

Toll-free telephone and e-mail technical support **must** be available 7:00 AM to 5:00 PM Monday through Friday, Eastern Time (GMT -0500) for designated WVDE networking staff. Any costs associated with this requirement are to be included in the line item for technical support on the cost page.

Comply ✓

The vendor **must** provide a function that permits any user of the WV K-12 network to submit a web site to be reviewed and appropriately categorized by the vendor. This function allows the vendor to receive feedback with the intent of improving delivery of services or product functionality.

Section V - Vendor Response

The vendor is to complete the Cost Worksheet.

Comply ✓

The vendor **must** provide evidence of at least one current, successful installation of the Internet filtering solution in a network configuration servicing 70,000 or more computers

with 3 gigabits/second or more of Internet bandwidth. Use the following table.

Project Name	# of computers filtered	Internet bandwidth
CapRock	100,000+	> 1 Gig
Oklahoma One Net	200,000+	> 1 Gig
Mead West Vaco	80,000+	> 1 Gig

Comply ✓ If the vendor fails to identify any costs that are required to meet the terms, requirements and conditions of this Quotation, it **shall** be the responsibility of the successful vendor to pay those costs and such costs will not be passed on to the WVDE or the State of West Virginia.

Comply ✓ Pricing **must** be stated on the basis of one-year contracts.

The actual number of licenses purchased may vary from year to year. The quantities of computers listed on the Cost Worksheets are estimates only. The actual quantity to be purchased will be specified in a purchase order.

Comply ✓ Filtering licensing prices **must** be quoted based on the number of computers filtered annually so that the WVDE can determine the basis of the pricing submitted in the quote.

Comply ✓ Software updates/upgrades and technical support **must** be priced on an annual basis and this item is reflected as such on the cost page.

The vendor is responsible for any costs due to product end of life that will require replacement or upgrading of the vendor provided software or hardware during the term of the contract.

Section VI – Cost Evaluation

Comply ✓ All quotes **shall** be all inclusive. No separate reimbursements will be made for travel or any other expense.

The State intends to award the bid to the vendor with the lowest grand total costs to provide a complete Internet filtering solution, including software, filtering updates, licensing, technical support and maintenance according to the specifications. As previously explained, the vendor may also include servers in the bid if the filtering solution cannot meet the requirements of this RFQ when installed on the WVDE equipment identified in Section I – Current Environment.

The WVDE reserves the right to purchase in part or in whole any products and services offered by the vendor in the response to this RFQ. The actual number of licenses purchased each year will be based on a count of computers, provided by the WVDE, on the date of the annual contract renewals.

Cost Worksheet

Item	Vendor Description	Quantity	Unit Cost	Total Cost
Annual software cost for Filtering Servers.*	Annual cost for year 2 and 3.	1	\$78,500	\$78,500/yr
Annual software cost for Reporting Servers.*		N/A	No Cost	
Annual License for filtering of client computers on K-12 network.	Unlimited user license. Cost will never increase.	130,000	\$78,500	\$78,500
Annual License for mobile computers. (see note 1 below.)		10,000	No Cost	No Cost
Technical support and upgrades/updates for filtering solution		1 year	No Cost	No Cost
One Day onsite training, 6 hours. Charleston WV (see note 2 below)		1 day	\$2,400	\$2,400
Onsite installation, Charleston and Morgantown, WV (see note 2 below)		4 days	\$9,600	\$9,600
Filtering Servers (if required)*	Quad I7 Servers	4	\$5,500	\$22,000
Reporting Servers (if required)*		N/A		
Other Hardware (if required)*		N/A		
Hourly rate for custom system modifications		20 hours	\$200/hr	\$4,000
Total Costs	Total cost for first year subscription			\$116,500

Note 1: A mobile computer requires special client software that will force the computer to be filtered even when it is disconnected from the K-12 network and connected to any other network which provides Internet access. If there is no price difference for mobile computers, enter the same unit cost as for computers on the K-12 network.

Comply ✓

Note 2: Costs for training and installation, configuration and testing **must** inclusive of all incidental costs. Travel expenses, training materials and other reimbursable expenses will not be paid separately. The distance between Charleston and Morgantown WV is approximately 180 miles.

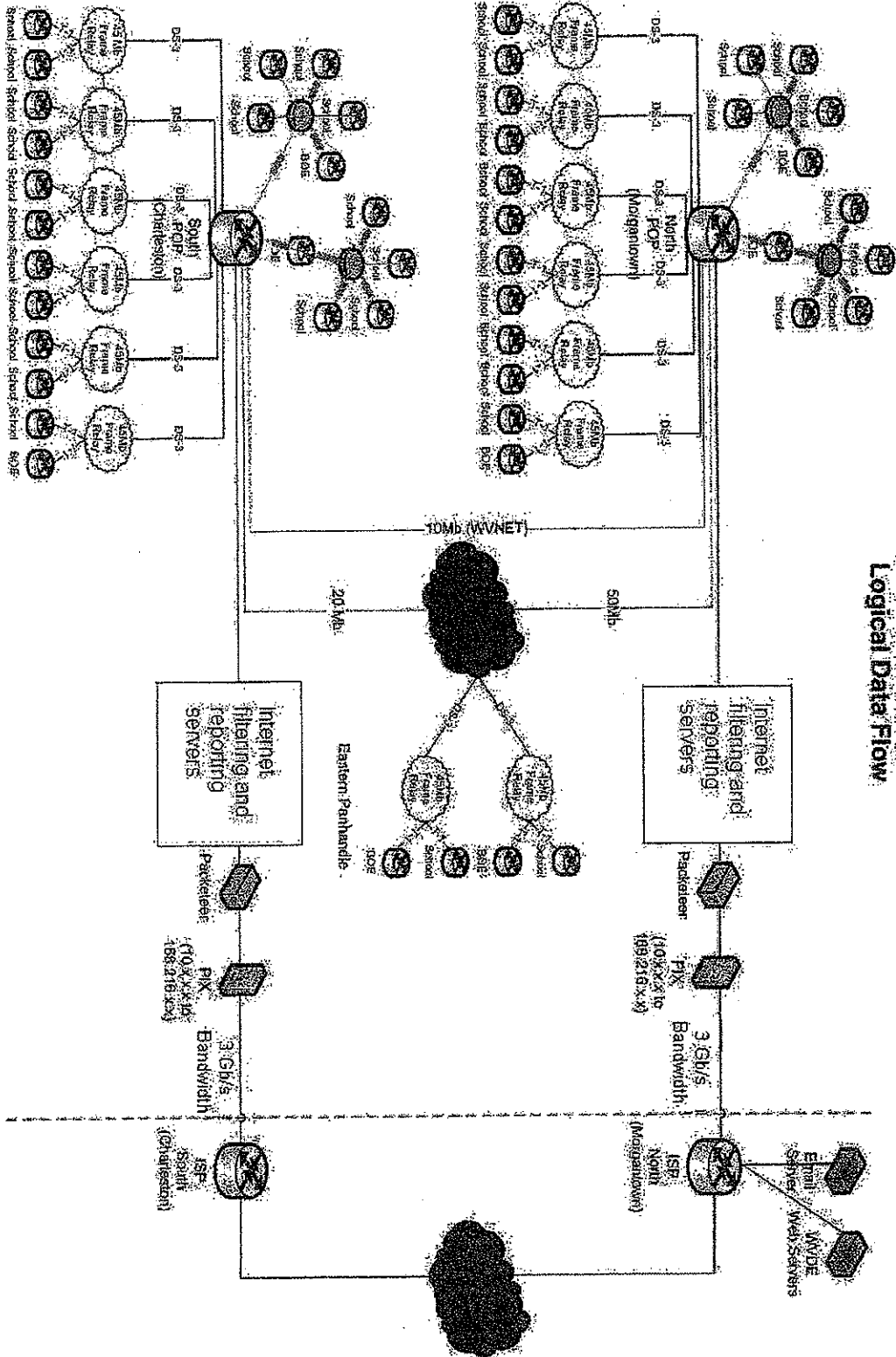
Item Pricing:

This worksheet is for vendors to identify items, quantities and provide prices. The vendor should indicate "No Cost" or "N/A" in the appropriate cells or blanks of the cost worksheet for which there are no separate or applicable costs. Any cost area that is left blank will be assumed to be "No Cost." The vendor may add notes to explain or clarify the bid.

* Vendor is encouraged to provide unit pricing for each of these items. However, it shall be the responsibility of the vendor to determine sufficient quantities needed for the scope of work outlined in the RFQ. For example, the quantity of servers needed to provide coverage for the WVDE's network may be set at one for vendor A, but be determined to be 5 by vendor B, due to design efficiencies.

Attachment A

West Virginia Department of Education K-12 State Network Logical Data Flow



Version: 07-23-09

RFQ No. EDD327891

STATE OF WEST VIRGINIA
Purchasing Division

PURCHASING AFFIDAVIT

West Virginia Code §5A-3-10a states: No contract or renewal of any contract may be awarded by the state or any of its political subdivisions to any vendor or prospective vendor when the vendor or prospective vendor or a related party to the vendor or prospective vendor is a debtor and the debt owed is an amount greater than one thousand dollars in the aggregate.

DEFINITIONS:

"Debt" means any assessment, premium, penalty, fine, tax or other amount of money owed to the state or any of its political subdivisions because of a judgment, fine, permit violation, license assessment, defaulted workers' compensation premium, penalty or other assessment presently delinquent or due and required to be paid to the state or any of its political subdivisions, including any interest or additional penalties accrued thereon.


"Debtor" means any individual, corporation, partnership, association, limited liability company or any other form or business association owing a debt to the state or any of its political subdivisions. "Political subdivision" means any county commission; municipality; county board of education; any instrumentality established by a county or municipality; any separate corporation or instrumentality established by one or more counties or municipalities, as permitted by law; or any public body charged by law with the performance of a government function or whose jurisdiction is coextensive with one or more counties or municipalities. "Related party" means a party, whether an individual, corporation, partnership, association, limited liability company or any other form or business association or other entity whatsoever, related to any vendor by blood, marriage, ownership or contract through which the party has a relationship of ownership or other interest with the vendor so that the party will actually or by effect receive or control a portion of the benefit, profit or other consideration from performance of a vendor contract with the party receiving an amount that meets or exceeds five percent of the total contract amount.

EXCEPTION: The prohibition of this section does not apply where a vendor has contested any tax administered pursuant to chapter eleven of this code, workers' compensation premium, permit fee or environmental fee or assessment and the matter has not become final or where the vendor has entered into a payment plan or agreement and the vendor is not in default of any of the provisions of such plan or agreement.

Under penalty of law for false swearing (*West Virginia Code* §61-5-3), it is hereby certified that the vendor affirms and acknowledges the information in this affidavit and is in compliance with the requirements as stated.

WITNESS THE FOLLOWING SIGNATURE

Vendor's Name: TeleMate.Net Software, LLC

Authorized Signature:  Date: May 13th, 2010

State of Georgia

County of Gwinnett, to-wit:

Taken, subscribed, and sworn to before me this 12 day of May, 2010.

My Commission expires _____, 20____.

AFFIX SEAL HERE

**MY COMMISSION EXPIRES
SEPT 22, 2012 NOTARY PUBLIC
GWINNETT COUNTY**



Important Confidentiality Notice

The information (data) contained on all sheets of this document/quotation constitutes confidential information of TeleMate.Net Software or its affiliates (collectively hereinafter TeleMate) and is provided for evaluation purposes only. In consideration of receipt of this document, the recipient agrees to maintain such information in confidence and to not reproduce or otherwise disclose this information to any person outside the group directly responsible for evaluation of its contents, unless otherwise authorized in writing. There is no obligation to maintain the confidentiality of any such information which was known to recipient without restriction prior to receipt of this document as evidenced by written business records; which becomes publicly known through no fault of recipient; or which is rightfully received by recipient from a third party without restriction.

This document includes information about current TELEMATE products, sales, and service programs that may be enhanced or discontinued at TELEMATE's sole discretion. TELEMATE has endeavored to include in this document the materials that are believed to be reliable and relevant for the purpose of recipient's evaluation. Neither TELEMATE nor its representatives make any warranties as to the accuracy or completeness of the information. Accordingly, this document is provided for information purposes only in the hope that TELEMATE may be considered to receive your business. Neither TELEMATE nor its representatives shall have any liability to recipient or any of its representatives as a result of the use of the information provided. Only a mutually agreed-upon written definitive agreement, signed by the authorized representatives of the parties, shall be binding on TELEMATE or its affiliates.

The term "solution" in the context of this proposal is defined as the products and services proposed herein. Since additional information may be required from State of Vermont in order to develop the appropriate configuration for State of Vermont project, the term "solution" does not imply that those products or services as proposed are guaranteed to, or will, meet State of Vermont requirements.

The use of the terms "partner" or "partnership" in this proposal does not imply a formal, legal, or contractual partnership, but rather a mutually beneficial relationship arising from the teamwork between the parties.

Unless otherwise agreed in writing, pricing estimates are valid for 30 days from date of submission of this proposal.

TeleMate's proposal is submitted via electronic format and hard copy for your convenience. If the content differs between the hard copy and soft copy, ONLY the content of the hard copy will be binding on TeleMate's proposal.

If there are any concerns, questions, or issues regarding this Confidentiality Notice, please contact your sales representative.

Table of Contents

<i>What makes TELEMATE.NET UNIQUE?</i>	2
Solution Overview	3
3.1. General Description of Solution.....	4
3.2. Compatibility Requirements	5
3.4. Design / Installation / Integration / Testing:.....	7
3.5. Maintenance, Patching and Upgrades:	8
3.6. User Interface Requirements:	9
3.7. User Access / Security Requirements:	10
3.8. Business Continuity and Recovery Requirements:.....	11
3.9. Web Filtering Requirements:.....	12
3.10. Administrative Requirements:	15
3.11. Reporting Requirements:	16
3.14. Warranty and Support Requirements:	18
3.15. Value Added Features:	19
4. Miscellaneous Requirements:	20
4.3. Organizational Listing of Involved Parties.....	21
4.5. References	22
Maintenance and Support.....	23
TeleMate.Net Software Compliance / Regulatory Data	24

What makes TELEMATE.NET UNIQUE?

TeleMate.Net Software is a global leader in providing scalable network monitoring and security solutions. Our product families including, TeleMate™ Unified Call Accounting, NetSpective™ Content Filter, and NetAuditor™ Firewall Reporting are considered products of choice for many Federal, State, Local, Educational, and Fortune 1000 institutions.

As a premier leader in network monitoring solutions TeleMate.Net Software's vision is to bridge the awareness gap created by the accelerated convergence of voice and IP services being deployed in complex networks. Visibility is vital in critical business and TeleMate is uniquely positioned to fill the void.

TeleMate.Net Software offers an effective Voice & Data Network Monitoring solution that enables your organization to:

- Allocate network services and related expenses back to the cost center or department, creating accountability
- Reduce Internet Security Threats
- Improve Quality-of-Service through Bandwidth Optimization
- Provide visibility into enterprise-wide Voice & Data status through pre-configured reports
- Help management measure the effectiveness of your Voice & Data Networks
- Meet legal and regulatory compliance requirements

Solution Overview

The TeleMate.Net Software (TELEMATE) is pleased to provide this response:

NetSpective's Key Features:

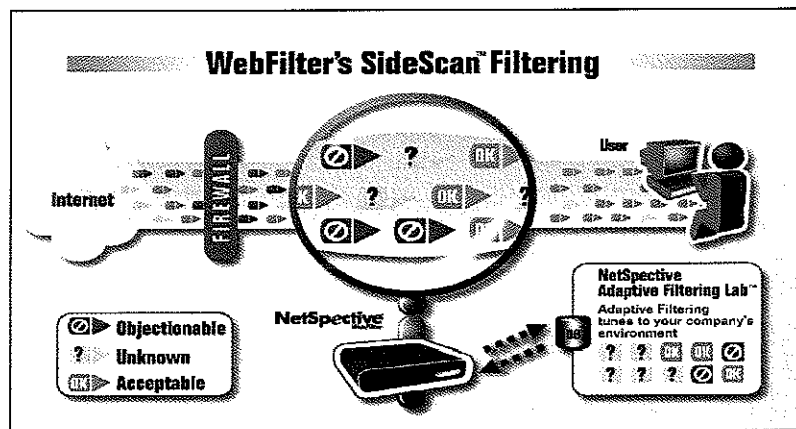
- SideScan™ Filtering Technology - NOT a point of network failure
- Monitor or block HTTP, HTTPS, NNTP, FTP, chat, Peer-To-Peer (P2P), Skype, VoIP (SIP, H.323), and streaming media protocols
- Load Balancing, Fail-Over Hot-Spare Configuration
- Signature-based blocking subscription with live updates
- Support for Citrix and Terminal Server
- Support for mobile users and home offices regardless of location
- Customized modes of operation by network IP address range(s) by time of day enabling pass through, monitor / report, or block / report traffic management
- **Location based filtering**
- Network Abuse Detection with session lockout
- Centralized policy management for distributed network environments
- **Automated Replication for multi-appliance management.**
- Alternate Policy Management – Control by Day of the Week
- Custom policies for special user group designations, supports “unlimited” groups
- Support for usernames in DHCP environments via NetSpective Logon Agent
- Support Microsoft Active Directory and Novell eDirectory via LDAP
- Flexible policy exemption by IP Address, username or URL using wildcard overrides
- Search Engine “safe search” enforcement
- 100+ categories provided
- User defined categories
- **Separate Block Pages can be assigned per group.**
- Application and protocol level control of Peer-to-Peer traffic
- Comprehensive web-based reporting tool, NetAuditor
- **Capacity and speed of reporting is unaffected by the current usage on the appliance.**
- NetAuditor documents all monitored and blocked activity
- Automated signature updates and product enhancements
- Automatic synchronization of URL overrides to TeleMate.Net's On-Line Service
- **Policy management and security access profiles available for administrative delegation.**
- Available monitoring interfaces: 1000 MB and Quad GigE
- **Seamless Upgrades**

3.1. General Description of Solution

NetSpective is a network appliance that monitors a LAN for HTTP, FTP, and NNTP resource requests using the SideScan™ filtering technology. It can be configured to enforce the management of established Internet usage policies or to simply log requests made on these services, appending category flags to them. For additional flexibility, NetSpective can also be configured to take no action with regard to any of the above-listed resource requests. At the user interface level, these three discrete actions or policies are referred to as blocking, monitoring, and ignoring, respectively.

With one interface configured as a conventional network activity analyzer, the SideScan™ filtering technology reviews every raw network packet on the wire. As such, SideScan™ is highly redundant, and does not pose the risk of interrupting Internet access in the event of a shutdown or failure. The efficiency of the SideScan™ packet analysis process relies on highly accurate methods for detecting the target TCP protocols without the need for tracking individual TCP sessions. The Category Management process returns codes to the network analyzer indicating whether a specific request is either approved (monitored or ignored) or disapproved (blocked), based on the policies configured via the Web interface. If a request is disapproved, a TCP-terminate message is sent to both the client and the server, and the client is subsequently redirected to a dynamically generated "block" page hosted on NetSpective.

The diagram below depicts the Packet-by-packet traffic inspection (SideScan™)



SideScan™ Filtering Technology is...

- **Firewall Independent / Not a Point of Failure / Never a reason for Network Slowdowns**
- **Transparent to the Network applications - 1000 MB and Quad GigE and OC48 certified***

NetSpective includes functionality to block based on traffic signatures, keywords, file extensions, and sites known to contain malware/spyware. NetSpective also leverages the Online Service to provide real time analysis of new/uncategorized sites.

3.2. Compatibility Requirements

3.2.1. LDAP Sources

There are two options for associating NetSpective groups with **Active Directory** groups containing users with mixed domain membership. Both methods involve the use of a Global Catalog Server (GCS).

Option 1: Using Universal Groups

This method only needs one configured LDAP Source. This source must be a Global Catalog Server that listens on port 3268. Configure this source with an empty search base or a search base that is above all domains in the forest, for example, "dc=com". You may associate a NetSpective group to any Universal Group in this source.

Option 2: Using Non-Universal Groups

This method requires one LDAP source which is a Global Catalog Server, as described above in Option 1. In addition, you must configure a regular Active Directory source (port 389) for each domain in the forest. A source for each individual domain is required because a Global Catalog server does not contain enough membership information for non-universal groups. You may associate a NetSpective group to any group returned by the GCS source, universal or not.

3.2.2. User Name Resolution

NetSpective can provide **user name resolution**. There are several methods that can be used to provide the user name resolution. First NetSpective can use a logon agent. The Logon agent does not need to install on the client workstations, the logon agent just needs to be placed in a network location that is accessible to the client machines and it is then run via a logon script or group policy.

The logon agent will pull the current user information from the local workstation and sends this information to The NetSpective appliance before exiting. For Citrix and Microsoft Terminal Servers a terminal server logon agent is provided. The Terminal Server Agent will need to install on all the Citrix and MS Terminal Servers to provide the user name resolution and it also allows the appliance to differentiate the multiple users on the same IP address from each other.

Alternately NetSpective includes a built in web based authentication portal in the appliance itself. The web portal can verify user credentials against a LDAP source or in an Active Directory environment the web portal can leverage NTLM single sign on with Internet Explorer and Firefox/Mozilla browsers.

3.2.3. Browser Compatibility

NetSpective has been tested with Internet Explorer, Firefox/Mozilla, Safari, and Chrome for both clients accessing the internet and for accessing the appliance's administrative interface. We are not aware of any untested browser being incompatible with our solution.

3.2.4. Citrix Environment

NetSpective sees and filters traffic from Citrix servers the same as any other server or workstation. To be able differentiate the different users and apply different filtering policies to users on the Citrix server the Terminal Server Logon Agent will need to be installed on each Citrix server.

3.2.5. Windows Clients

NetSpective can filter traffic from local Windows clients based on the IP address of the client or the logged on user. To filter based on the logged on user use of the logon agent or the authentication portal will be required.

3.2.6. MAC Clients and Compatibility

NetSpective is compatible with filtering MAC desktops. MAC desktops can be filtered by the IP address of the desktop or the network authentication portal described in the name resolution section can be used to filter the traffic based on the currently logged on user.

3.2.8. Linux Desktops

NetSpective is compatible with filter Linux desktops. Linux desktops can be filtered by the IP address of the desktop or the network authentication portal described in the name resolution section can be used to filter the traffic based on the currently logged on user.

3.4. Design / Installation / Integration / Testing:

3.4.1. It is a requirement that the proposed system be sized to support at least 6,000 users.

NetSpective's hardware is sized based on network bandwidth. The standard NetSpective appliance will handle up to 1 gigabit of saturated traffic. This is an Enterprise Application – Unlimited Users – See Proposed Pricing Schedule

3.4.2. If it is a requirement that the vendor must be prepared to provide its own personnel (or subcontract personnel if the Vendor proposes to use subcontractors on the engagement) to install the system.

Telemate considers this acceptable. Included in Proposed Pricing Table

3.4.3. It is a requirement that the vendor describe any design, installation, integration and testing recommendations that have not been addressed elsewhere in the RFP which in their experience will make this project a success.

Telemate will work with the Fulton County and provide the needed additional information once the project begins – as needed or recommended by the County with proposed solution.

3.5. Maintenance, Patching and Upgrades:

3.5.1. Software Enhancement

Software updates/enhancements are released approximately 4 times a year. Patches are release as needed. Administrators will receive notification of the update or patch being available and will have the option to install or ignore the update. Signatures and Categories are update nightly but with the Micro Update feature enabled, the **Signatures and categories can be updated as frequently as every 10 minutes**. As long as the NetSpective subscription is up to date all patches and software upgrades are provided at no charge.

3.5.2. Maintenance of System

Remote support is available via phone and email. If remote access is needed to troubleshoot a problem our support staff will use a WebEx session to provide access to the administrative interface. If access is needed to the console of the appliance, the appliance has a feature that Fulton County can activate to create a SSH tunnel on port 10000 back to TeleMate to allow an engineer to access the console.

3.5.3. Maintenance Plan

The yearly subscription covers all maintenance and support of the appliances hardware and software.

3.6. User Interface Requirements:

3.6.1. Block Pages

When a user attempts to access a HTTP site that is blocked they will be redirected to NetSpective's block page which will inform the user that the site is blocked. NetSpective's block page is fully customizable, including the message and graphics. Separate block pages can be applied to separate groups.

3.6.2. No Requirement of Desktop Client or Software

Users can be authenticated via several methods. The Logon Agent, which the executable is hosted on a network share and then is run via a logon script or group policy when a user logs in to a workstation. The Network Authentication Portal is a web based user authentication portal which can authenticate users against Active Directory or can use NTLM SSO. Citrix servers and remote filtering on laptops will require local installation of software. Citrix servers will need to have the Terminal Server Logon Agent installed on them to properly differentiate the different users on the same IP address. Remote filtering of Windows and MAC laptops will require the installation of the Remote Agent on all laptops requiring remote filtering.

3.7. User Access / Security Requirements:

3.7.1. Transparent User Access

Transparent user authentication can be provided by the Logon Agent, Terminal Server Logon Agent, Remote Agent, and the Network Authentication Portal (NAP). The three agents provide transparent authentication by reading the user information from the local system. The NAP can provide transparent authentication for windows clients by using NTLM SSO.

3.7.2. Security Updates and Temporary Lapses of Maintenance

Critical security updates will be automatically provided to the appliance free of charge for the duration of the subscription. If at the end of a subscription period, Fulton County is in contact with TeleMate during a renewal period, TeleMate will extend the subscription in good faith to cover you while the renewal is being processed. In addition if Fulton County is not in contact with us and the subscription was to expire, the appliance will continue to function and provide filtering. The ability to receive software and category/signature updates will be the only functionality lost if the subscription expired.

3.8. Business Continuity and Recovery Requirements:

High availability is provided via a Hot Spare appliance which can easily replicate all of its configuration from the primary appliance. The primary and hot spare appliance will both be actively monitor traffic on the network and the quickest appliance to react to the objectionable traffic will be the one to handle the blocking of that traffic. Then if one appliance was to go down the other would take over all the blocking of objectionable traffic.

3.8.2. Failure Scenario

NetSpective is a passive solution that does not sit inline in the network, thus if there was a failure it will not impede any network traffic.

3.9. Web Filtering Requirements:

3.9.1. Predefined Categories

NetSpective provides 10 user defined Categories as well as over 100 plus pre-defined categories. Each category can be set to either, block, log/monitor, or ignore traffic.

3.9.2. Ports, Protocols, and URL

NetSpective can block and/or monitor web traffic using the HTTP and HTTPS protocols, regardless of the port being used. Web traffic can be monitored and/or blocked based on the following categories:

Advertising	Alcohol	Anonymous Proxy and Hacking	Art
Automotive	Chat	Chat Extended	Consumer Information
Criminal Skills	Cult and occult	Drugs	Dynamic Hosting
Education	Entertainment	Finance/Investing	Gambling
Games	General Business	Glamour	Government
Hate speech	Health	Hobbies	Hosting Sites
HTTPS Trusted	HTTPS Unrated	HTTPS Untrusted	Internet Tools
Job search	Law	Lingerie	Mature content
Military	News	Nudism and Naturism	Peer-to-peer
Personals/Dating	Politics and Religion	Pornography	Portal
Reference	Science	Sex Education	Sexual Advice
Sexual Orientation	Shopping	Shopping Auction	Society
Sports	Streaming Internet Radio	Streaming Media	Technology
Tobacco	Travel	Uncategorized	Violence
Weapons	Web Email	Web Log	Web Search
	Web Search Filtered		

3.9.3. Filter Avoidance and Anonymous Proxies

NetSpective leverages its Micro Update feature and our Online Service to maintain blocking proxy sites. As new sites are seen by NetSpective, they will be sent to our Online Service for review. The Micro Update feature allows these new sites to be transmitted as frequently as every 10 minutes and at the same time the appliance will be receiving updates to the category lists. The new site should then be categorized and returned to your appliance on the next Micro Update.

3.9.4. File Sharing Sites and Protocols

File Share web sites are covered by the Peer-to-Peer category and following file sharing application protocols are supported:

BitTorrent	Direct Connect	EDonkey/EMule
Nutella	Kazaa	Napster
Piolet	The Onion Router	WinMX

3.9.5. Social Media Sites

“Social media” sites are in NetSpective’s Society category.

3.9.6. White lists, Black lists, and Overrides

The overrides functionality of NetSpective’s administrative interface provides for white listing and blacklisting of sites. Site categorization can be overridden at both the system level or at a group level. Lists of sites may also be imported into the system. Steps required to override a single site;

1. Log into the NetSpective administrative interface.
2. Under the Management section, click on the Overrides link.
3. From the Group drop down, select the Group of Users you wish to override the sit for, or select the System group to override the site system wide for all user groups.
4. Click on the Add button
5. Enter the Domain Name, IP Address, or URL that you wish to override.
6. Enter a comment (Optional).
7. Select the category to put the site in. This can be Admin Block, Admin Allow, any one of 10 user defined categories, or any one of the **100+ provided** categories.
8. Click OK

The site will now be blocked, monitored or ignored based on the policy assigned to the category the site was overridden. Also functionality is provided to import lists of sites.

3.9.7. Regular System Updates

Nightly, NetSpective will connect to the NetSpective Online Service (OLS) to download category update information. The updated category information will be downloaded and applied automatically and will not require user interaction. Additionally NetSpective includes a Micro Update feature that will allow NetSpective to connect to the OLS on an every 10 minute, hour, or 3 hour basis to download and apply category updates.

3.9.8. Streaming Audio and Video

NetSpective can block streaming audio and video based on URL and/or streaming protocol. **Administrators can also selectivity block specific streaming content by source or protocol.** Streaming audio and video URLs are covered by the Streaming Internet Radio and Streaming Media categories. The following streaming media protocols are supported:

Flash
Slingbox

QuickTime
Winamp Shoutcast

Real
Windows Media

3.9.9. Access to Blocked Sites

NetSpective allows for temporary access to be granted to a blocked web site right from the block page itself. This feature can be enabled on a per user group basis, and can provide temporary access to the site to just the user that was initially blocked from accessing the site or the temporary access can be granted to the entire group of users. The block page override will require knowledge of the override password for the user group or will require use of a user name & password that has been authorized to override block pages for that group of users

3.10. Administrative Requirements:

3.10.1. Ease of Use

NetSpective is managed through an easy to use browser based administrative console. The administrative console can be accessed via HTTP or HTTPS. NetSpective includes centralized management so all appliances in a deployment can be managed from one central point.

3.10.2. Delegated Administration by LDAP Group

NetSpective allows for additional Administrator and Manager Logins to be brought in from Active Directory. NetSpective allows administrative and manager access to be granted to entire groups or individual users. Three security levels are provided, Administrator, Group Manager, and Block Page Override Manager.

3.10.3. Exclusions of Users or Groups

The users that need to be excluded from all monitoring and reporting can be placed in a Group that can be synced from AD. Then the policy for this group will have all of the categories set to an ignore action.

3.10.4. Enabling Access to Specific Sites

The Overrides feature can be used to enable or limit access to specific sites. Steps to perform and override are outlined in 3.9.6.

3.11. Reporting Requirements:

3.11.1. Web-Based and Windows-Based Reporting

NetSpective provides on appliance summary and detail reporting that will cover the current day's activity. NetAuditor is also included with the NetSpective appliance. NetAuditor is a Windows based reporting software used for detail and historical reporting for NetSpective. NetAuditor includes a built in web portal for access to reporting capabilities.

3.11.2. Departmental Reporting

NetAuditor provides the functionality to restrict the data available to a user based on the User Groups in the NetSpective appliance. As these User Groups can be tied to groups or OUs in AD, this allows this segregation of data to be accomplished by AD grouping.

NetAuditor can restrict user's access to reporting data based on user groups and/or the device(s) being reported on.

3.11.3. Web Browsing Time

NetAuditor includes a Browser Session Summary report that will report the amount of time spent browsing the web.

Browser Session Settings

These settings affect how browser sessions are detected in the "Browser Session Summary" report. It is impossible to accurately detect how long a user spent surfing the web, scanning news groups, or chatting with friends just by looking at firewall logs, but a reasonable estimate can be determined by checking the timing of a user's accesses. This is still difficult to do because various programs (i.e. RSS readers, news readers, chat programs, peer-to-peer programs) may generate "noise" traffic that must be filtered out to get a better picture of browsing activity.

Browser Session Timeout: This setting tells NetAuditor how much inactivity to allow before closing a browsing session to start a new one. For instance, if a user generates a steady stream of HTTP traffic for 10 minutes, stops for 7 minutes, and then starts again for another 10 minutes, should that be seen as one browser session for 27 minutes, or two separate 10-minute browsing sessions that are 7 minutes apart? The user may have stopped browsing for 7 minutes, or he may have spent that time reading a web page or composing a web email. It is up to you to choose a timeout value that you feel gives the best results.

Smallest Browser Session: This setting tells NetAuditor to ignore sessions that are too short to be worth mentioning. This helps eliminate some of the "noise" mentioned above. If you have an RSS reader that generates a spike of traffic once every 30 minutes, but that spike only lasts for a minute or two, then setting this to 3 should eliminate that traffic. By itself, this setting does not remove very much of the unwanted noise. However, it works quite well when combined with the noise reduction setting below.

Noise Reduction: (You configure this each time you run the report.) Many programs generate a small amount of traffic every few minutes or possibly even every minute. To help eliminate this "noise", NetAuditor attempts to automatically calculate a noise floor for each user. Think of this noise floor as a water level, and any minute that is under water is ignored as noise. When this setting is set to 0%, the noise floor will be set to 0 and all traffic will be treated as part of a session. When it is set to 100%, all traffic will be filtered out as noise. When it is set to 25%, the water level will be set to the lowest level that covers at least 25% of the minutes being counted as part of a session. The water level should be different for each user because each user may leave different applications running in the background.

3.11.4. Reporting Detail

NetAuditor provides numerous summary and detail reports, which will allow a user to view totals usage and then be able to drill down all the way to the individual accesses that made up the users total usage.

3.11.5. Additional Reporting capability

NetAuditor can also report on firewall and proxy server log files in addition to NetSpective's log files. NetAuditor provides both a GUI interface as well as a web based portal for reporting.

3.14. Warranty and Support Requirements:

3.14.1. Hardware Warranty

The Appliance will be fully warranted for the first year. The warranty will be extended for an additional year at a time with each subscription renewal.

3.14.2. Technical Support

Remote support is available via phone and email. If remote access is needed to troubleshoot a problem our support staff will use a WebEx session to provide access to the administrative interface. If access is need to the console of the appliance, the appliance has a feature that the State of Vermont can activate to create a SSH tunnel on port 10000 back to TeleMate to allow an engineer to access the console.

3.14.3. Level of Support

Standard support hours are Monday through Friday 7:30 AM to 6:00 PM. Extended support of 24 x 7 x 365 is available on request.

3.14.4. Access to Support

Support of the NetSpective appliance is included in the subscription renewal. All support options are available for all active deployments.

Technical Support

Phone	+1.678.589.1626
Phone	+1.678.589.7120
Email	TeleMateSupport@TeleMate.Net
Email	NetSpectiveSupport@TeleMate.Net
Email	NetAuditorSupport@TeleMate.Net

3.15. Value Added Features:

3.15.1. Additional Value

NetSpective also supports filtering of Chat, Remote Login, and VOIP protocols, provides for Safe Search Enforcement, and supports SNMP monitoring and NTP time synchronization. NetSpective also supports blocking of UltraSurf, an anonymous proxy application. Chat protocols supported include AOL, ICQ, IRC, MSN/Live, MySpace, and Yahoo. Remote Login protocols supported include OpenVPN, SSH, VNC, Citrix, Remote Desktop, and PCAnywhere. VOIP protocols supported include SIP, NetMeeting/H.323, and Skype.

4. Miscellaneous Requirements:

4.1. Quality of Performance

TeleMate.Net Software has been an industry leader in providing voice and data network monitoring solutions since 1986. The our 22 year history TeleMate has deployed and monitored in excess of 18,000 distinct deployments including many of the country's leading companies, Federal institutions, State Agencies, County municipalities, and largest school districts. Below is a brief listing of current customers using our network monitoring and filtering technology.

Enterprise

- *Verizon*
- *IBM*
- *Mead Westvaco Corporation*
- *URS*
- *Humana*
- *Continental Airlines*
- *Commerce Banks*
- *Flagstar Banks*
- *Blue Cross Blue Shield*
- *Computer Science Corporation*
- *TRX Corporation*

Education

- *One Net ISP*
- *East Baton Rouge Parish*
- *Texas ESC 5, 13, and 16*
- *Putman County*
- *Ohio State Medical*
- *Gwinnett County*

Government

- *Missouri Department of Transportation*
- *Federal Reserve Banks*
- *IRS*
- *State Department*
- *US Navy*
- *Army National Guard*
- *Air National Guard*
- *FDIC*
- *US Treasury*
- *US Space Alliance*
- *US AID*
- *California State Assembly*

- *Cobb County*
- *Alabama Public Library*
- *Gardner Webb University*
- *McDuffie County Schools*
- *Chesterfield ISD*
- *Erie School District*

4.3. Organizational Listing of Involved Parties

TeleMate.Net Software Corporate Headquarters	5555 Triangle Parkway Suite 150 Norcross, Georgia 30092
U.S and Canada	+1.678.589.7100
Fax	+1.678.589.7110
Remittance FEIN Address	26-3330752 TeleMate.Net Software LLC. 5555 Triangle Parkway Suite 150 Norcross, Georgia 30092
U.S and Canada	+1.678.589.7100
Fax	+1.678.589.7110
Email	<u>AccountsPayable@TeleMate.Net</u>
Worldwide Sales Phone Phone Fax Email	+1.678.589.7100 +1.678.589.7150 +1.678.589.7110 <u>Worldwide.Sales@TeleMate.Net</u>
Michael Hartley (PM) Phone Email	+1.678.589-3630 <u>michael.hartley@telemate.net</u>
Technical Support Phone Phone Email Email Email	+1.678.589.1626 +1.678.589.7120 <u>TeleMateSupport@TeleMate.Net</u> <u>NetSpectiveSupport@TeleMate.Net</u> <u>NetAuditorSupport@TeleMate.Net</u>
Registration Services Phone Email	+1.678.589.7140 <u>Registration@TeleMate.Net</u>
President U.S and Canada Email	John O'Reilly +1.678.589.3524 <u>John.OReilly@TeleMate.Net</u>
Director of Operations Phone Email	Cathy Adams +1.678.589.3515 <u>Cathy.Adams@TeleMate.Net</u>

4.5. References

Cobb County

Contact: Bill Knapp
Phone Number: (770)528-8761
Email: bill.knapp@cobbcounty.org
Address: 100 Cherokee Street, Suite 520
Marietta, GA 30090-7000

Gwinnett County

Contact: Anthony Winter
Phone Number: (770)822-7527
Email: anthony.winter@gwinnettcountry.com
Address: 75 Langley Drive
Lawrenceville, GA 30045

Missouri Department of Transportation

Contact: Todd Walters
Phone Number: (573)526-3164
Email: todd.walters@modot.mo.gov
Address: 105 West Capital Ave.
Jefferson City, MO 65101-6811

East Baton Rouge Parish

Contact: Jesse Noble
Phone Number: (225)922-5522
Email: noble@ebrpss.k12.la.us
Address: 1050 South Foster Drive
Baton Rouge, LA 70815

Maintenance and Support

TELEMATE's Software Services portfolio provides a comprehensive suite of personalized, proactive services, dedicated electronic services and business advocacy, creating a valuable long-term partnership between you and your TELEMATE team.

Support Contact

Technical Support

Phone +1.678.589.1626

Phone +1.678.589.7120

Email TeleMateSupport@TeleMate.Net

Email NetSpectiveSupport@TeleMate.Net

Email NetAuditorSupport@TeleMate.Net

Registration Services

Phone +1.678.589.7140

Email Registration@TeleMate.Net

Director of Operations Cathy Adams

Phone +1.678.589.3515

Email Cathy.Adams@TeleMate.Net

TeleMate.Net Software Compliance / Regulatory Data

Enterprises are stretching to prove compliance to mandatory regulation while balancing compressing budgets and increased risk due to security threats

Government and industries across the globe force regulatory mandates to ensure that both business sensitive and personal information is secure and individual are protected from unwanted threats. In North America alone mandates affect network requirements and best networking practices for all Healthcare Providers, Financial Services Companies, Educational Institutions and Government Agencies.

Regulations including HIPAA, CIPA, Sarbanes-Oxley Act, the Graham Leach Bliley Act and SEC rule 17A-4, NIST & FISMA. Each regulatory compliance does not only require monitoring ingress and egress internet activity, but voice communications as well.

Each hole in your security blanket jeopardizes information leaks and increases risk and liability from failure to comply or risk for lawsuits. Examples include installation and use of unauthorized chat application including Skype™, file sharing clients like Kazaa or Bittorrent, or even employees accessing pornography or terroristic material. Each places your organization in a legally vulnerable position. In fact, the average cost of one potential legal liability case is \$500,000! Employees spend from 30 minutes to three hours a day surfing non-work related sites. And prime time surfing hours for the worst of the web is 9 to 5 - when most employees are hard at work!

NetSpective™ Content Filter and NetAuditor™

- Provides selective blocking of chat clients and extended file sharing features
- Signature based blocking inspects all packets regardless of port
- Deep packet inspection identifies even undocumented and encrypted protocols like Skype™
- Enables monitoring on all internet traffic regardless of protocol or pathway.
- Facilitates network audits with historical gas-gauge, detail and summary reports by user, group, protocol, domain, and category.
- Provided integration with internal directory services for centralized control and policy assignment.
- Provides Micro-Updates to ensure current and accurate signatures for policy enforcement.

Thank you for the consideration and
we look forward to working with you on the project!

