ADDENDUM 1

SPRING BRANCH INDEPENDENT SCHOOL DISTRICT
Duncan F. Klussmann, Ed. D., Superintendent of Schools

PURCHASING DEPARTMENT
1031 Witte Road, Building E, Houston, Texas 77055-6016
Phone 713/251-1100 Fax 713/365-5216

Date: February 19, 2009

BARBARA A. ROBILLARD
Director of Purchasing

NOTICE TO OFFERORS

ADDENDUM TO REQUEST FOR PROPOSAL

DATE: February 19, 2009

This Addendum forms a part of and modifies the original Proposal Document, issued by the Spring Branch Independent School District.

Invitation to Proposal entitled: CONTRACT FOR WEB CONTENT FILTERING AND DATA LEAK PREVENTION

Original Proposal Opening Date & Time: March 05, 2009 @ 11:00 AM
Revised Proposal Opening Date & Time: March 12, 2009 @ 11:00 AM

ADDENDUM NO. 1

PROPOSAL NO. 8805P

Please make the following additions, revisions, and/or deletions to the Proposal Document:

- **See Revised Proposal Opening Date**
- **See Scope of Proposal**
- **See Questions and Answers**
- **See Overview**
- **See Revised Date for Questions**
- **See Revised Date for Addendum Issued**

The offeror shall acknowledge receipt of this addendum in the Proposal Form.

ADDENDUM 1

S C O P E O F P R O P O S A L

SBISD prefers the content filter solution to be configured in active/active or active/passive mode for failover. Therefore, please include the following:

It is the intention of SBISD to establish an Annual Contract for the Purchase of Web Content Filtering. Award of contract, should not be construed to be a guarantee as implementation is dependent upon continued availability of funding.

SBISD intends to award Internet Services for a period of one (1) to three (3) years, whichever is most advantageous to the District. Therefore, SBISD is interested in receiving proposals for one (1) and three (3) years as follows:

- July 1, 2009 through June 30, 2010
- July 1, 2009 through June 30, 2012

The term of the contract will commence July 1, 2009 and renew each year. Each renewal shall be subject to the same terms, conditions, requirements and specifications as listed herein unless noted and agreed to by both parties in writing.

All deliveries and or installations shall be made to designated campus. For shipments designated on the purchase order to the SBISD Central Warehouse, delivery hours are 7:00 a.m. to 3:00 p.m. NO DELIVERIES WILL BE ACCEPTED AFTER 3:00 P.M.

PRE-PROPOSAL CONFERENCE
A pre-proposal conference will be held on February 11, 2009 @ 2:00 P.M. at the SBISD Telecommunications Theater at 10670 Hammerly Houston, TX 77043. Non-attendance may be grounds for disqualification at the option of SBISD.

ADDENDA TO RFP. SBISD reserves the right to revise and amend the specifications prior to the date set for the opening. Respondents are requested to clarify any ambiguity, conflict, discrepancy, omission or other error(s) in the RFP in writing and request modification or clarification desired. Revisions or amendments, if any, will be made by issuing an addendum. Every effort will be made to send addenda issued to the parties known to have been furnished a complete copy of the RFP. **All questions must be received in writing by the Director of Purchasing via fax (713/365-5216) no later than 12:00 P.M. on February 26, 2009. No addenda will be issued later than March 06, 2009,** except an addendum withdrawing the proposal or postponing the opening of the proposal. It is the responsibility of each Proposer, prior to submitting the proposal, to contact the Purchasing Department to determine if addenda were issued and, if so, to obtain such addenda for attachment to the Proposal.

Note:

MARCH 16-20 2009 FOR SPRING BREAK

ADDENDUM 1

QUESTIONS AND ANSWERS

Question #1: Is SBISD required to Purchase the Web Content Filtering and Data Leak Prevention solution from an authorized DIR or TCPN Vendor?

Answer#1: The competitive bid process allows SBISD to purchase from the selected vendor.

Question #2: Many manufacturers require their resellers to use third party financing since they will not finance internally the solution proposed on monthly, quarterly or yearly basis. The SBISD funding out clause prohibits a bank or finance company such as a GE Credit, from funding this transaction. Can SBISD propose an alternative to the funding out clause for three year pricing billed annually which would be acceptable to a Finance company? Most resellers will not send a PO to their vendor for three years without a contractual relationship with the end user.

Answer #2: SBISD can not propose alternative to "Funding Out Clause" for three year pricing. Refer to RFP, General Terms and Conditions 1.15.0.

Question #3: Please explain 9.3.15 in more detail.

Answer #3: Does solution dynamically throttle bandwidth for a user once a pre-defined configurable threshold has been reached?

Question #4: No mention was made of SBISD issued laptops needing to be filtered when off the SBISD campus network? Is Laptop filtering a requirement when off the network? If so, please explain in more detail how SBISD policy would work with SBISD issued laptops outside the SBISD network using a public Internet access point such as Comcast, Wifi etc?

Answer #4: Filtering laptops outside of the SBISD network is not a requirement at this time. If the solution can provide this functionality it would be a point to consider for future policy.

Question #5: Please explain the formula for all qualified proposals in more detail 9.7.0. Will points be earned? As an example, out of 1,000 points available, the vendor with the best references may end up with 15% (150 points) out of the 20% weighting?

Answer #5: Vendors will be ranked based on responses in each category. Higher ranked vendors will receive proportionally higher points.

ADDENDUM 1

QUESTIONS AND ANSWERS CONT.

Question #6: Do your school systems have their own separate IP address zones all the way to the desk?
Answer #6: SBISD uses an internal IP scheme.

Question #7: Are the schools using Network Address translation on their local networks?
Answer #7: No

Question #8: Are there any terminal servers?
Answer #8: Not at this time, however, deployment is an option being considered by SBISD.

Question #9: Is there a network diagram available?
Answer #9: A current network diagram is not available. Vendors are welcome to schedule a time with to review current configurations.

Question #10: Is the connection between the firewall and core router fiber?
Answer #10: The firewall connection to our core router is copper.

Question #11: When you deploy the second circuit, how will you aggregate the traffic? (I.e. which load balancers? Will this be active/passive or active/active or just aggregated)?
Answer 11: Both connections will be aggregated.

Question #12: Are there redundant firewalls right now? Are they load balanced or running in active/passive mode?
Answer #12: We currently use Cisco firewalls in an active/passive configuration.

Overview

Corporate	
Provide a brief history of your company.	
What is your annual revenue for this DLP product?	
What is the location of your DLP head office and work sites?	
Please provide a list of your company's major shareholders.	
What is the current market share of the DLP product?	
How many employees does your company have?	
How many employees are developers?	
How many employees are consultants?	
How many employees are dedicated for customer support staff? Local support?	
How many employees work directly on the product?	
How much revenue is based on maintenance and on consultancy?	
What percent of total revenues are spent on R&D?	
Who are your company's strategic partners?	

Product and Versions	
1. What is the current generally available version of your product?	
2. Please provide a brief overview of your product line and where the products reside within the IT infrastructure.	
3. Please detail the release history of the product.	
4. Please detail the forecast for future releases and what improvements they will add to the product.	

Customer Deployments	
1. How many of your customers are similar in size and complexity? Please describe your experience working with similar customer environments.	
2. Please provide a sample list of customers similar in size and complexity.	
3. What percentage of your customers continue to use your product year over year? How many customers have you lost in the last 24 months?	
4. What percentage of your deployments are enterprise/company-wide?	
5. How many customers do you currently have using your DLP solution?	

DLP System Management

Policy Definition	
1. Does your system have the ability to use a single policy to scan data where ever it is stored, transmitted or used, both on the network and on the endpoint? Will the system automatically apply the relevant response to the threat detected? Please explain.	
2. Do you provide a centralized interface for policy editing and policy management, across all products (across monitoring and prevention and across network and endpoint)? Please explain any aspects of policy editing or management that are not covered by the centralized interface.	
3. Does your product provide command line interface, API, and/or scripting language interface?	
4. Can policies be defined based on any of the following: content, sender/recipient, file characteristics, and communications protocol? Please provide a screenshot of the interface where the user creates custom detection policies.	
5. Does your system allow for configurable scoring of incident severity based on the amount of data exposed?	
6. Where applicable does the system use standardized scoring metrics?	
7. Can your system support inclusion and exclusion detection rules based on corporate directory data to enforce policy based on the senders and recipient/destination.	
8. Does your system have predefined detection policies to cover regulations and detection best practices, including pre-defined lexicons for commonly required regulations? Please provide a complete list of supported policies.	

Detection - General	
1. Does your product provide identical detection capabilities across all threats covered (e.g., for both network and endpoint-based products, and for both data monitoring and prevention and data discovery and protection)? Please explain any differences across products (e.g. fingerprinting on the endpoints).	
2. Does your product have enterprise search capability?	
3. Can your system extract and inspect the text content of files and attachments? Please provide a complete list of supported file types for which your system can extract and inspect text content.	

4. Can your system inspect slack space on files when inspecting stored content?	
5. Can your system inspect metadata on files when inspecting stored content? Please explain.	
6. What hashing algorithm or mechanism is used to fingerprint files in storage and being transmitted?	
7. How many nested levels of folders can be inspected?	
8. How are hidden folders detected and scanned?	
9. How are ACL'd folders detected and scanned?	
10. Please provide general guidance around how much time should be allotted for scanning of files in storage.	
11. Do the detection capabilities of your system apply for Western European and Asian (Japanese, Chinese simplified, Chinese traditional, Cyrillic and Korean) language content? Please explain any limitations or behavioral differences for detection of European language content, such as limited capabilities for certain detection technologies. Please list all supported languages. For unsupported languages, please describe expected behavior of the detection process.	
12. Can your system recursively inspect the contents of compressed (e.g. ZIP, TAR, RAR) archives and detect against fingerprinted content? How many levels of embedded archives does it handle?	
13. Can your system deal with very large files or attachments (20MB and larger) during the detection process of fingerprinted content? What is the maximum file size the system can reliably process for confidential content detection?	
14. Do you have information about the false positive and false negatives percentages produced by your solution? Please describe.	

Detection – Structured Data Fingerprinting	
1. Does your system provide a method for fingerprinting data such as customer records?	
1. Does your system provide ODBC connection to databases for fingerprinting? Please explain and provide screenshots.	
2. Does your solution copy and/or store confidential data (when fingerprinting) to a central repository? Please explain.	
3. Please describe what access privileges are required in order to fingerprint structured data.	
4. Does your system provide control measures to validate accuracy of a fingerprint at the time of its creation? Please explain and provide screenshots.	

5. Can your solution combine elements (e.g., Name + SSN) and thresholds of data that is fingerprinted?	
2. Can your system protect at least 10 million rows of specific content from a database of sensitive information (such as a customer or employee data) without relying on keywords or patterns? If so, what is the maximum size of database (expressed in rows or cells) you have deployed without experiencing a drop in detection speed or accuracy?	
3. Can your method of detection of fingerprinted data allow you to specify which columns of data constitute a match on a per-policy basis?	
4. Does your method of detection of fingerprinted data distinguish between data fields that belong to the same record or row of a database versus different rows?	
5. Can your method of detection of fingerprinted data match on only First Name and Last Name from a customer database, without needing a pattern based number (e.g., Social Security number, credit card number, etc.) present?	
6. Can your system distinguish between different types of PII or PHI numbers? For example, can the system distinguish a customer's nine-digit social security number from a nine-digit phone number without the presence of a keyword (e.g. "SSN")?	

Detection – Unstructured Data Fingerprinting	
1. Does your system provide a method for fingerprinting documents such as CAD drawings or merger and acquisitions documents?	
2. Does your solution copy and/or store confidential data (when fingerprinting) to a central repository? Please explain.	
3. Please describe what access privileges are required in order to fingerprint structured data.	
4. Does your system provide control measures to validate accuracy of a fingerprint at the time of its creation? Please explain and provide screenshots.	
5. Can your system protect at least 100,000 specific documents containing sensitive content (such as intellectual property, source code, and/or financial documents) without relying on keywords or patterns? If so, what is the maximum number of documents you have deployed without experiencing a drop in detection speed or accuracy?	
6. Is heuristics done on files such that relationships can be established between data in files, emails, and between the two?	
7. Does your method of detecting fingerprinted documents support detection of the same text or	

portions of text in different file formats? For example, if a fingerprinted document is in Microsoft Word format, will your system detect that same text that has been cut and pasted into an email directly?	
8. Does your system support content matching of specific documents such as source code, specific paragraphs, design documents, marketing documents or financials?	
9. Does your system support detection of derivative or cut-and-paste versions of content matching specific documents such as source code, specific paragraphs, design documents, marketing documents or financials?	
10. How much protected document content can the system support before experiencing a drop in detection speed or accuracy?	
11. Can your system "whitelist" boilerplate content, safely removing this textual content from detection?	

Detection – Pattern Data Identification	
1. Does your system support described content detection using fully customizable rules with keywords and key phrases? If so, does your system provide the option to detect keywords either as stand-alone words only or within other words?	
2. Does your system support keyword lists for detection of at least 10,000 entries? If so, what is the maximum length of a keyword list used for detection that you have tested without performance degradation?	
3. Does your system support detection based on fully customizable regular expressions? Customizable keywords?	
4. Does your system support detection for pattern matching combined with validations specific to the content being detected? For example, can it detect common credit card number patterns as well as doing the checksum validation to ensure a valid credit card number (the "Luhn" check)? If so, please list all out-of-the-box data types that are detected.	
5. How do you reduce false positives for types of data that incorrectly match a pattern? Example: A coupon code matches a credit card pattern ID and checksum, but is not. Please explain.	
6. Does your system check for substitutions as seen in malicious concealment?	
7. Can your system detect the presence of encrypted transmissions or files? What different types can it distinguish?	
8. Can your described content detection be customized to include match data within certain custom defined ranges without having to write a	

regular expression? For example, can it detect credit card numbers only with a specific Bank Identification numbers?	
9. Does your system support detection based on a particular document type, even if the sender has changed the file extension? Please provide a complete list of file types the system can recognize.	
10. Does your system detect and inspect video or audio files? Please describe.	
11. Does your system detect and inspect image files? Please describe.	

Automated Response & Enforcement	
1. Can alerts be sent via email? Please describe the available formatting and message detail that may be included. Please include a sample notification screenshot.	
2. Does your system support the ability to automatically notify senders or their managers when a policy has been violated? Please describe the notification capabilities	
3. Does your system support the ability to provide on-screen notifications to users for endpoint based violations?	
4. Can automated response actions be defined by different parameters, such as the policy violated, the severity of the incident, the number of matches found, the communications protocol used, the connected status of the endpoint, and the product being used? Please explain.	
5. Does your system provide automatic workflow functionality for tracking the remediation of an incident (e.g. status codes, attributes, assignment queues, severity etc.)? Please explain.	

Incident Response Workflow	
1. Are confidential data loss events viewable via the web in a format usable by non-IT business level users? Please provide screenshots.	
2. Does the incident include a clear indication of how the transmission or file violated policy (not just which policy was violated), including clear identification of which content motivated the match? Please provide screenshots and describe.	
3. Is it possible to view identity information on the sender (such as full name, manager name, business unit) and destination of the transmission (e.g., data sent to a blog, chat board, spyware site)? How is this accomplished, especially in the case of non-email network events, storage events, and endpoint events?	
4. Is it possible to open the original attachments of an event directly from the UI?	
5. Can each user in the workflow be assigned to remediation of a certain set of incidents? Please describe the process, including how incidents are passed between users.	
6. Can incident managers receive automated notifications that they have new incidents to review?	
7. Can your system define and track a "case" or set of incidents found to be related after an investigation? If so, how is a case defined and managed?	
8. Can an incident be locked to prevent deletion/edit? Please explain.	
9. Can a group of incidents be exported easily from the system in a format easily readable by a person without system access (e.g., to satisfy a discovery request)?	
10. Is it possible to manually launch response workflow functionality for remediation of an incident (e.g. status codes, attributes, assignment queues, notifications, etc.)? Can the UI be customized to allow multiple responses be combined into a single action by a user? Please explain.	
11. Is it possible to add custom attributes to incidents to correlate with custom remediation business process?	
12. Does your system support industry best practices for incident response? Please explain how this is built into the product and which best practices are followed.	

Role Based Access and Privacy Control	
1. Can your system control incident access based on role and policy violated? Please explain.	
2. Can a role be defined to not have viewing rights to identity-based information to protect employee privacy?	
3. Can a role be defined to not have viewing rights to content of the message that violated policy to reduce dissemination of sensitive intellectual property of the company?	
4. Can your system create separate roles for technical administration of servers, user administration, policy creation and editing, incident remediation, and incident viewing for data at rest, in motion, or at the endpoint? Please provide screen shots and describe.	

User Authentication and Identity Resolution	
1. Can multiple users be created within the system and assigned to various roles? If yes, please define the default roles and what permissions are allowed to be assigned. Please include screen shots where possible. Also are the following supported:	
a. Can a role be configured to contain any combination of permissions?	
b. Can a role be created to have access to system administration functions but not to policy, incident, or employee information?	
c. Can a role be created that allows users to view incidents but not to modify or remediate them?	
d. Can a role be created that has the ability to see summary reports, trend reports and high-level metrics without the ability to see individual incidents?	
2. Does the system allow user authentication to be controlled in an external directory, e.g. Active Directory.	
3. Does your system support integration with directories for sender/file owner identity resolution? Please explain specific uses.	
4. Can these external lookup integrations be easily updated as the directory information and sources change? Describe how this is accomplished.	

Distributed Architecture	
1. Does your architecture support remote sites and network users distributed across many different locations? Describe any limitations around number of components. Please describe a typical deployment and where each component resides. If there are variations that can be deployed please describe.	
2. Can all network components be configured and managed through a centralized UI? Please describe conditions where UI is not centralized.	
3. Please describe the high availability/failover capabilities of your solution.	

System Management	
1. Do you offer standard reports on system traffic and performance and throughput metrics? Please describe the capabilities and provide a screenshot.	
2. Does your solution store captured data and logs in a centralized database? What Database and is it included?	
3. Does the server support a choice of operating systems?	
4. Does your system run on commodity hardware? What are the hardware requirements for your system?	

System Security	
1. Can customers determine the security of the underlying technology platform?	
2. Are security patches managed for your system? How does your system “know” that a security patch is needed?	
3. Are the communication links into and out-of the hosts that run your application secured? List the specific protocols, ciphers, and key lengths used to secure this traffic.	
4. Are there any special measures taken to secure confidential data in your system? If so, list these measures including (as appropriate) ciphers, key-lengths, and key-management schemes.	
5. Are users of your system authenticated and authorized securely? Specifically list the measures used to securely store and process passwords or other authentication tokens.	
6. Is logging configurable? Please describe and provide screen shots.	
7. How long can logs be retained? Can they be saved off the system? If yes, please provide	

detailed information on how logs can be saved off the system.	
8. Is every login into the system and modification to system policies or incidents logged into an audit trail?	
9. Does the application have the capability to disallow logins? How are logins re-enabled? Explain.	

Integration & APIs	
1. Does your system support integration with Web proxies? Support ICAP?	
2. Does your system have predefined integration with any case or problem management systems? Please explain.	
3. Does your system have predefined integration with forensic tools? Please explain. Is your system certified to integrate with Guidance, Encase?	
4. Does your system support integration with an email archiving solution? Please explain.	
5. Does your system support integration with an email encryption gateway? Please explain.	
6. Does your system support integration with MTA's (Message Transfer Agents?)	
7. Does your system support CITRIX?	
8. Does you system support integration with a Security Incident Event Management (SIEM) tool? Please explain.	
9. Please provide details of other supported integrations.	

Reporting & Analytics	
1. Can your system provide custom report filtering across different variables and attributes? Please explain.	
2. Does you solution include web-based favorite reports by administrator?	
3. Can your system provide custom report summarization and grouping across different variables and attributes? Please explain, including how many levels of summarization are possible.	
4. Can your system generate trend reports, including summarization for different time segments and trend graphs? Please explain.	
5. Can report data be exported to formats such as a PDF or HTML? Please list specific export capabilities.	

6. Can reports be saved for reuse?	
7. Can reports be shared based on role? How are these reports administered and maintained?	
8. Can users or sets of users “subscribe” to sets of incident reports that match specific criteria and receive a scheduled email delivery daily, weekly, or monthly?	
9. Can reports be graphically displayed and printed?	
10. Can reports be emailed directly from the UI without manual re-formatting? Can these email reports be edited if customization is required for company-specific formatting? Please provide screenshots for how these emailed reports appear in email clients..	
11. Is there a ”dashboard” view designed for use by executives that can combine information from data in motion (network), data at rest (storage), and data at the endpoint (endpoint) in a single view? Please provide a screenshot.	
12. Can reports be run for all historical events? If so, with what limitations? What is longest period of time for which a current customer has been storing incidents that are still available in their production system for full reporting?	
13. Are reports query times reasonably short? What is the expected wait time to generate a report containing 500 incidents captured at different network exit point?	
14. Are reports interlinked, for example clicking from a summary report directly to a list report, directly to an incident detail view?	
15. Does your system come with a prepackaged set of reports? Please provide a complete list.	
16. Can reports be scheduled for automated distribution?	
17. Can reports be generated from multiple data sources across many DLP systems from a single console or system? Example system 1 and system 3 collect data if I am using system 2 and want to report on all data inspected across the enterprise will system 2 collect and report on the data collected from the other systems?	

Network Data Monitoring and Prevention

Network Monitoring/Prevention	
1. Can your solution monitor and enforce without adding latency or failure points to the network? Please explain.	
2. What protocols can you monitor/prevent inline vs. out of band? Please explain.	
3. Does your solution provide for inline deployment in transparent mode? What network changes are required to accomplish this?	
4. Does your system classify traffic into protocols without relying on specific port numbers (e.g. port 80 for HTTP)? Please explain how your system classifies protocols.	
5. Does your system provide notification of unprocessed traffic due to network bursts (e.g. dropped packets or sampling)? Please explain how yours system handles bursts of traffic.	
6. Does your system monitor gigabit speed lines without packet loss? Please describe the hardware requirements for monitoring a gigabit line.	
7. Does your system analyze traffic and report incidents in real-time, even at high scale? What is the average time, in milliseconds, between an incident being captured from the network and being available for reporting and alerts?	
8. Does your system monitor web traffic, including web mail, web postings, and other protocols using HTTP and HTTPS including uploaded files? Please enclose a screenshot of how an HTTP event appears in your system.	
9. Can your solution monitor/prevent network printing of confidential information? Please explain how this is accomplished.	
10. Does your system provide geographical and web site detail to resolve/classify the destination of HTTP/S transmission (not just an IP address). Please explain and provide screen shots.	
11. Does your solution provide native inspection of SSL communications? If so, please explain. If not, please explain how this can be accomplished (e.g., w/ integration) and provide a price estimate for integration tool.	
12. Does your system monitor both active and passive FTP traffic including fully correlating transferred file data with control information?	
13. Does your system monitor instant messaging traffic? Which IM networks can be monitored?	
14. Does your system monitor instant messaging traffic when they tunnel through HTTP, port-80 or through a java app?	
15. Are both sides of instant message conversations correlated into incident	

presentation? Can it record or terminate a session based on keyword or offensive content?	
16. Does your system allow for monitoring network traffic on arbitrary ports or port ranges to deal with unclassified or rogue threats? Please explain.	
17. Can your system monitor traffic up to 1Gbs without dropped packets?	
18. Can your system queue messages for review if it cannot review them in real time?	
19. Does your solution resolve the user [offending] in real time (not just IP address and not just LDAP lookup, post event)? If so, please explain how this is accomplished.	
20. Over a rolling eight-hour period, what is the mean time added to message delivery by your system? How is this number affected by hardware?	
21. Please provide a detailed list of all application based network traffic that is specifically inspected for and what is inspected for.	
22. Please provide a detailed list of all network traffic that is specifically inspected for and what is inspected for.	

Email Prevention	
1. Does your system block outbound emails that are in violation of company policy on confidential data? Please explain.	
2. Does your system monitor and enforce for internal email traffic, including attachments. Please explain how this is accomplished and provide screenshots of relevant incidents.	
3. Does your solution utilize either its own MTA or another means of email prevention? Please explain.	
4. Does your system quarantine emails that are in violation of company policy on confidential data? Please explain.	
5. Do you have any production customers using automated email prevention? What is your claimed accuracy rate? Please explain.	
6. Can your solution take prevention actions without introducing another "hop" in the outbound message chain?	
7. Are different deployment configuration available based on the current mail infrastructure? Please describe options available.	
8. Does your system ensure message delivery even in the event of a failure of your system? Please explain.	
9. Can senders and security administrators be notified of a blocked or quarantined email? Please explain.	
10. Does your solution scale to cover multiple millions of messages per day? How many messages can your solution monitor in a 24-	

hour period with a reasonable hardware configuration and what is that hardware requirement?	
11. Does your system monitor for emails that are generated by hand using the ESMTP and SMTP commands via Telnet?	

Web Prevention	
1. Does your solution support content aware blocking of network transmissions over HTTP natively, and provide notification? Please explain. If integration is required, please explain and provide pricing.	
2. Does your solution support content aware blocking of network transmissions over HTTPS natively, and provide notification? Please explain. If integration is required, please explain and provide pricing.	
3. Does your solution provide visibility into the type of site data is posted to and its geo location? Please explain and provide screenshots.	
4. Can sensitive content be removed or replaced to prevent confidential data loss? Please explain.	
5. Can your solution block network transmissions over FTP? Please explain.	
6. Can your system control the latency it introduces to normal network communications? Please explain.	
7. Does your system provide notification of a policy violation? Please provide screenshot.	
8. Does your web prevention solution account for Web 2.0 (AJAX based) sites that dynamically update content? Describe how.	
9. Does your system use ICAP as a means to communicate with web proxies for traffic inspection? Do you provide your own proxy? Please explain.	

Network Data Discovery and Protection

Target Coverage	
1. Please define the file systems, platforms, databases, applications, and other devices you cover?	
2. Please list each OS which you have an agent?	
3. Can your system scan Windows file servers, desktops and laptops? Please list file systems and explain how they are scanned.	
4. Can your system scan Unix file systems? Please list file systems and explain how they are scanned.	
5. Can your system scan DB2?	
6. Can your system scan ODBC or JDBC?	
7. Can your system scan NAS filers, such as NetApp? Please explain.	
8. Can you system scan NAS gateways? Please explain.	
9. Can your system scan Unix file servers without the use of file sharing technologies such as NFS and CIFS?	
10. Can your system scan data found in Lotus Notes databases?	
11. Can your system scan data found in relational (SQL) databases?	
12. Can your system scan data found in SharePoint servers?	
13. Can your system scan web servers and applications through native HTTP crawling?	
14. Can your system discover data found in Microsoft Exchange?	
15. Can your system discover source code? Please list	
16. Can your system scan other kinds of targets, including custom repositories and support full reporting on policy violations found in those repositories?	

Data Protection	
1. Can your system automatically copy files which violate policy? Can your system automatically encrypt files in violation of policies?	
2. Can your system automatically quarantine and delete files which violate policy	
3. If quarantined, is this data automatically encrypted at rest and in transmit?	
4. Does your system provide a way to inform file owners about quarantined files, including details of why the file was quarantined, such as which policy it violated, etc.	

Discovery Information	
1. Does your system display the original file location (and quarantine location if applicable) and policy match details for files found to violate policy?	
2. Can your system integrate with corporate directories to allow data-at-rest policy violations to be associated with a particular individual and business unit? Please explain.	
3. Can your system provide a single report covering data at rest (storage) throughout the global enterprise? Please explain.	

Scan Management	
1. Does your system provide a single management interface for all scan configuration and control, enterprise-wide?	
2. Does your system leave the "last accessed" attribute of scanned files unchanged so as not to disrupt enterprise backup processes?	
3. Does your system support automatically scheduled, repeat scanning?	
4. Can your system automatically limit scanning during certain configurable time windows, such as during daytime work hours?	
5. Does your system support throttling to control impact on network and scanned system?	
6. Does your system support incremental scanning to reduce the volume of data to be scanned?	
7. Can your system run multiple scans in parallel?	

Scale and Security	
1. Can your system scan remote locations with low network bandwidth? Please explain.	
2. Does your system restrict communications to known ports between the scanned system and the scanning server only? Please explain.	
3. Does your system offer both agentless and agent-based deployment options?	
4. Does your system impose any requirements (such as OS version or pre-requisite software/system libraries) on the scanned system?	
5. Are the communications between the system and the agent encrypted?	

Endpoint Data Monitoring and Prevention

Event Coverage	
1. Can your endpoint solution detect user attempts to copy confidential data to removable storage devices (e.g. USB drives, floppy, CD/DVD, etc.)? Can actions be taken to prevent this transfer regardless of whether the user is on/off network?	
2. Can your endpoint solution display complete details about the incident including the file name, user information, policy match details, and a copy of the original file that violated policy?	
3. Do endpoint incidents get populated into a centralized management/workflow interface with network incidents? Please provide screenshots.	
4. Does the endpoint have the ability to monitor/prevent the following (please explain and provide screenshots):	
a) Cut/Copy	
b) Paste	
c) Print Screen	
d) File Access	
e) Print (network and endpoint)	
5. Can the endpoint perform the actions in item 5 based on a specific application (e.g., Cut/Copy is not permitted from Excel)? Please explain and provide screenshots.	
6. Can the endpoint perform the actions in item 5 based on the content in use from a specific application (e.g., cut/copy is not permitted from Excel when displaying confidential data)? Please explain and provide screenshots.	
7. Can the endpoint perform the actions in item 6 and 7 based on an application category (e.g., all spreadsheet applications)? Please explain and provide screenshots.	
8. Can the endpoint automatically prompt external security controls (e.g., file encryption)? Please explain.	

Continuous Monitoring/Protection	
1. Does the endpoint solution provide continuous monitoring/protection of confidential data regardless of whether the user is on or off the network?	
2. Can the endpoint solution monitor/protect remote users who may be disconnected for a long time or only connected via a slow link?	

Multi-tier Detection Accuracy	
1. Can your endpoint solution protect confidential content regardless of file type or file location (e.g. distinguish between an Excel document with confidential data which must be protected vs. an Excel document without confidential data which is not protected)?	
2. Does your endpoint solution support detection based on fingerprinting of content? Can it support 100's of thousands of fingerprinted documents without crippling the endpoint devices?	
3. Does your endpoint solution support hierarchical user/group policies with configurable remediation/responses?	

Global Scale	
1. Can your endpoint solution scale to protect 10's of thousands of agents? Please explain how the solution supports this.	
2. Please provide distributed system architecture diagrams, design guide, and specifications.	
3. Does your endpoint solution support geographically dispersed machines for global deployments of endpoint agents while maintaining a central management/reporting interface? Please explain.	

Agent Deployment and Management	
1. Can your endpoint solution be deployed with existing desktop management tools (i.e. Microsoft SMS, IBM Tivoli, Altiris)?	
2. Does the endpoint solution operate without requiring much system resources, including CPU, disk, and memory footprint? Please explain resource requirements.	
3. Please describe the endpoint solutions network communication requirements.	
4. Is the endpoint configured via the centralized management interface (along with network management/configuration)?	
5. Can your endpoint solution support automatic agent updates and policy changes without requiring third party tools?	
6. Can the endpoint agent be customized before distribution? Please explain.	
7. Please list the OS platforms that the endpoint solution supports.	

Agent Security	
1. Does your endpoint solution secure the agent from end user tampering? Please explain.	
2. Does your endpoint solution secure the agent from administrative users tampering? Please explain.	
3. Does your endpoint agent solution log tampering with the agent?	
4. Can your endpoint solution detect end-user tampering and restart itself if it's stopped?	
5. Does the endpoint include a local/remote bypass?	
6. Can your endpoint solution ensure that communications between agents and server are authenticated and secure? Please describe.	
7. Does your endpoint agent support communicating with the server over a configurable port?	
8. Are agent communications susceptible to network traffic attacks like DNS spoofing, MITM, packet sniffing, etc.?	
9. Does your endpoint agent obfuscate its presence and network communications? If so, please describe.	

Endpoint Data Discovery and Protection

Discovery	
1. Does the system include agent-based data discovery on end-user machines?	
2. Does the agent perform detection locally, avoiding the need to transmit data over the network?	
3. Does agent-based scanning continue to operate when the machine is off the network?	
4. Can policies be defined once and used for both network (agentless) and agent-based discovery in a centralized management interface?	
5. Does the endpoint discovery process include local fingerprints? Is this configurable? Please explain.	
6. Does the endpoint discovery process include all built-in pattern policies? Please explain.	
7. Is scan progress reported centrally while scans are running?	
8. Is the endpoint discovery configurable? Please explain and provide screenshots.	
9. What is the CPU impact from endpoint discovery?	

Interface	
1. Does the application have a single, unified console for all configuration and reporting operations across all detection paths that is fully integrated with the network management?	
2. Does the application allow multiple concurrent accesses to the administration/reporting system? Please indicate the maximum number of concurrent users supported.	
3. What modes can the endpoint be configured to operatein? Can it be run without the users knowledge?	
4. What endpoint information is displayed to the local user? Please provide screenshots.	
5. Please provide screenshots of the user notifications.	
6. Can endpoints be configured with different profiles for different user groups? Is this configurable by directory services?	

Technical Specifications

This section shall provide a description of its technical operational requirements for the following:

Platform	
The proposing vendor shall provide a description of the platform(s) required (i.e. Linux, Unix, Windows) – If the proposed solution is appliance platform based, so state.	
1. CPU type and number of cores	
2. Operating system type and version	
3. Required Kernel if applicable	
4. RAM Type and quantity	
5. Onboard storage (hard drive(s)	
6. Processing speed	

Database	
If an external data base is required, it must reside on the districts SQL 2005 Enterprise cluster.	
Recommended D.B size, per number of monitored nodes	

Virtualization	
If an external platform is required, it must reside on the districts ESX virtual host or be appliance based.	

Communication	
The Proposing vendor shall indicate what communication protocols are supported	
1. Identify supported communication protocols	
2. Identify type and depth of encryption	
3. TBD	

Support

Implementation	
1. Do you have a professional services team to assist with the implementation on-site?	
2. Are implementation services available? Please describe these services.	
3. Do you have domain experts who can assist in the creation of policies, advise on industry best practices, and establish the right business processes?	
4. What has been the typical time for implementing your solution? Have there been any failures during implementation and what were the lessons learned?	

Training	
1. What has been the typical time for a typical end user to become proficient?	
2. What training is necessary for installing your product?	
3. What documentation is provided?	
4. What training is necessary for operating your software package?	
5. Is additional training available? If so, please describe.	
6. How is training delivered?	

Support	
1. Do you provide on-site support and consulting?	
2. Do you have defined support levels, response times, and escalation paths? Please explain.	
3. Do you provide a 24x7 support option?	
4. Do you have email-based, web-based, and phone-based support?	
5. Provide a detailed description of your company's support organization.	
6. Do you work with any partners? In what way?	
7. How is customer input handled for feature enhancements?	
8. How do you handle bug fixes and new version releases?	
9. Does your company have a process for bug remedy? If so, please describe.	
10. Do you measure and report client satisfaction? Please explain.	
11. Provide a list of the recommended tool set and best practices needed for support, including, but not limited to, Backups, Service Assurance and Monitoring, Application Performance Monitoring, Database backups and recovery.	

Upgrades	
1. Describe your process for testing system upgrades before releasing to the public.	
2. Describe your process for performing system upgrades.	
3. Can software updates and patches be deployed automatically to all network monitors through a centralized mechanism?	
4. Describe the support your company will provide during a software upgrade. Examples are on-site, on-call, remote dial-in, none, and other.	
5. Are previous versions supported after a new release? Please describe.	
6. In the event of a failed upgrade, how can the system be restored?	
7. Describe the type of test environment recommended for testing new fixes/upgrades.	
8. Describe the hardware lifecycle.	
9. Any upgrade hardware plans in the one to two years?	
10. Do hardware upgrades require “fork lift” upgrades?	
11. How is the system backed up?	

OPTION I – Following all guidelines and specifications mentioned in RFP 8805P. Please use and attach proposal form below as additional required submittal. This form should list additional cost for content filter failover in an active/active or active/passive configuration.

Option I (Additional cost for content filter failover) Proposal Form

COMPONENT		COST
10.0.01	Software – Web Content Filtering Service (including installation, management, maintenance, administration, support, etcetera).	
10.0.02	Hardware – Web Content Filtering System Service (including installation, management, maintenance, administration, support, etcetera).	
10.0.03	Hardware – Additional Hardware	
10.0.04	Backup	
10.0.05	Training	
10.0.06	Installation & Implementation	
10.0.07	Other Related Costs (please explain)	
10.0.08	Total Cost	

Please propose maintenance and support, including on-site service charges, for one and three years if purchased within 60 days of acceptance. All maintenance plans and warranties must be manufacturer guaranteed and will be verified by SBISD. The manufacturer, in case of default by the proposer, must provide any maintenance services or warranty provided by the proposer. The proposer must provide SBISD a letter from the manufacturer specifying that the manufacturer will provide the specified service and warranty plan at no cost to SBISD in the case of default by the proposer. The cost elements are contained in the following two tables.

Web Content Filtering Maintenance Plan		One Year Term	Three Year Term
10.0.09	Software Maintenance for failover system		
10.0.010	Software Support Service: 24 hr x 7 day x 4 hr response		
10.0.011	Hardware Maintenance for failover systems		
10.0.012	Hardware Support Service: 24 hr x 7 day x 4 hr		
10.0.013	Other Maintenance and/or Service Costs		

10.0.0 PROPOSAL FORM, continued

OPTION II – As a second option, SBISD would deploy an integrated DLP solution. The solution should be based on specifications in RFP 8805P as well as the following criteria.

A. Proposed solution

A description of the solution being proposed to meet the requirements listed is required. Also, any modifications or additions to the system necessary to meet SBISD's requirements should be specifically noted.
The vendor is also to submit an Implementation Plan of the proposed solution. The Implementation Plan shall be developed based on the phased approach detailed in the SOW within this Addendum. The plan should detail all commitments expected of SBISD staff and management, all major activities to be performed, and any conversion activities required.
As part of the Implementation Plan, the vendor will prepare and submit a timeline that incorporates the phased approach detailed within this Addendum.
In addition the plan will include (but not be limited to) the following:

1. Project milestones
2. Process for testing all aspects of the installation
3. All commitments expected of SBISD staff and/or management
4. Post implementation support
5. Training

B. Itemized Costs

This section should include a complete breakdown of all costs associated with the proposed solution including installation, implementation, and support costs.
Costs to be included in the proposal are (if applicable):

1. Licensing fees cost and structure (Based on SOW and Requirements) – 1 year option
2. Licensing fees cost and structure (Based on SOW and Requirements) – 3 year option
3. Maintenance and support cost for aforementioned licenses – 1 year option
4. Maintenance and support cost for aforementioned licenses – 3 year option
5. Estimate of technical training cost
6. User Training cost
7. Implementation services
8. Other costs not included above

C. Vendor support

The proposal should include a statement of the vendors support related activities, such as:

1. Training
2. Ongoing application software support
3. Means for providing support (web, phone, etc.)
4. Software modification/customization
5. Hours software support is available
6. Response time to an incident
7. Other

The quantity and cost, if any, of such support should be included. Pricing of the support services, in excess of that being proposed, should be noted.

Option II (DLP)
Proposal Form

COMPONENT		COST
10.0.09	Software – Data Leak Prevention (including installation, management, maintenance, administration, support, etcetera).	
10.0.010	Hardware – Data Leak Prevention System (including installation, management, maintenance, administration, support, etcetera).	
10.0.011	Hardware – Additional Hardware	
10.0.012	Backup	
10.0.013	Training	
10.0.014	Installation & Implementation	
10.0.015	Other Related Costs (please explain)	
10.0.016	Total Cost	

Please propose maintenance and support, including on-site service charges, for one and three years if purchased within 60 days of acceptance. All maintenance plans and warranties must be manufacturer guaranteed and will be verified by SBISD. The manufacturer, in case of default by the proposer, must provide any maintenance services or warranty provided by the proposer. The proposer must provide SBISD a letter from the manufacturer specifying that the manufacturer will provide the specified service and warranty plan at no cost to SBISD in the case of default by the proposer. The cost elements are contained in the following two tables.

Web Content Filtering Maintenance Plan		One Year Term	Three Year Term
10.0.014	Software Maintenance for primary system		
10.0.015	Software Support Service: 24 hr x 7 day x 4 hr response		
10.0.016	Hardware Maintenance for primary systems		
10.0.017	Hardware Support Service: 24 hr x 7 day x 4 hr		
10.0.018	Other Maintenance and/or Service Costs		

10.0.0 PROPOSAL FORM, continued

Having carefully examined the Proposal Notice, Terms, Conditions, Specifications and Proposal Form, the undersigned hereby proposes and agrees to furnish goods and/or services in strict compliance with the specifications and conditions at the prices quoted unless noted in writing.

The undersigned affirms that they are duly authorized to execute this proposal and that this company, corporation, firm, partnership or individual has not prepared this proposal in collusion with any other Proposer.

ADDENDA, if any: If issued in accordance with this document, the undersigned acknowledges receipt of:

Addenda No: _____ dated _____.

The undersigned agrees to abide by all delivery schedules and timelines provided as part of the proposal and to provide all services and products in accordance with those timelines unless the district provides a properly executed change order.

FIRM NAME_____

ADDRESS_____

CITY/STATE/ZIP_____

TELEPHONE NO._____

FACSIMILE NO_____

EMAIL ADDRESS_____

AUTHORIZED SIGNATURE_____

TYPED/PRINTED NAME_____

E-RATE SPIN NUMBER_____

POSITION WITH COMPANY_____

REPRESENTATIVE'S NAME_____