

Enterasys Networks

Response to

Joint Committee of the Higher Education  
and Entertainment Communities  
Technology Task Force

Request for Information

Technologies for Addressing Issues Associated with  
Unauthorized File Sharing on the University and  
College Campus



"There is nothing more important  
than our customers"

A handwritten signature in black ink, appearing to be 'M. Kauf'.



June 13, 2008

Bruce Block  
Block & Associates  
12512 Palatine Court  
Potomac, Maryland 20854

Dear Mr. Block,

Thank you for providing Enterasys Networks, Inc. (Enterasys) with the opportunity to submit a response to the Technology Task Force's Request for Information. Enterasys builds the world's most secure enterprise networks, providing intelligent and best-in-class Secure Networks to enterprise customers worldwide. Enterasys can do this because of the Enterasys Secure Networks™ architecture, which ensures the confidentiality, integrity and availability of IT services and the business users that rely on them – without sacrificing performance. Higher education customers will not have to choose whether to deploy security at the edge, around the middle or in the core of the data center – it's built-in everywhere with granular, policy-based visibility and control over individual users and applications. With one of the industry's broadest product portfolios – plus a full range of service and support offerings – Enterasys is uniquely qualified to meet the evolving needs of higher education.

Enterasys is a different kind of networking company – our goal is to become our customer's favorite vendor by delivering on our promises – on-time and on-budget. There is nothing more important than our customers as we measure our success based on your satisfaction. We are the perfect-sized company – big enough to meet our customer's needs now and in the future, yet small enough to have a personal relationship with each of our customers. We encourage direct access to our talented developers and experienced executives. With thousands of active customers in more than 70 countries, we will earn the right to your business every day through thought leadership without arrogance.

Enterasys' proposal contains an executive summary and point-to-point responses to the Technology Task Force's technology requirements. We welcome any questions and feedback on our submission and appreciate the opportunity to participate in the Joint Technology Committee's efforts.

Should any questions arise as a result of our submission, please feel free to contact me at 978-684-1623. Again, thank you for the opportunity to participate in this RFI evaluation process. We are fully committed to providing as much detail as necessary for a complete review of our capabilities and look forward to this opportunity.

Sincerely,

Mark Townsend

## Executive Summary

Enterasys Networks is pleased to respond to this Request for Information sponsored by the Joint Technology Committee of Higher Education and Entertainment Communities. Enterasys has been an innovator in providing solutions to the education market for more than 25 years. As the Joint Technology Committee and participants have discovered over the last two years, each educational institution is different in the technologies that they use, their philosophical approach and operational goals.

While these differences will prohibit industry from creating a “magic box” in the near future, Enterasys Networks would like to offer information on key technologies for managing the copyright infringement concern. The standards-based, open architecture approach from Enterasys allows for the centralized visibility and control to discover, deny, redirect, bandwidth restrict, and/or audit peer-to-peer file sharing. Enterasys offers a way to accomplish copyright compliance automation without requiring forklift upgrades. The Enterasys approach also offers financial advantages in that technology refresh budgets for connectivity upgrades can be leveraged to build-in, rather than bolt-on, the peer-to-peer traffic visibility and control solution.

We have reconciled in Technology Committee meetings that no two networks are the same. Each organization designs their information infrastructure to suit the specific goals of their institution. Within higher education, the exchange of information and promotion of learning is the critical organizational objective of the network. When there are freedoms, there will be those who misuse these freedoms. The problem created by the sharing of copyrighted materials without the permissions of its creators is a recognized problem in society and is exacerbated in environments where there is little control. As no two networks are the same, no two solutions offered in today's marketplace are the same either. An architectural approach is more suited to solving diverse business problems at a lower expense and lower capital cost than point solutions.

Looking around the market today, a number of point product solutions promise to solve a particular problem. These products target a particular space, such as content/protocol inspection or network access controls. Each of these products has a particular value and cost, but they are limited in the value that they may bring because they fail to address the entire network. Point products also represent a separate cost to IT organizations. Every problem should not require a new product to be deployed for resolution. In today's competitive and cost aware environment, organizations are faced with choices to spend their finite resources to address individual point problems or address larger organizational initiatives. With architecture based solutions such as Enterasys Secure Networks®, institutions do not need to choose between point problems and alignment with organizational objectives. With the Enterasys Secure Networks architecture, a customer can implement a [peer-to-peer visibility and control solution](#) to fit their current network, regardless of the incumbent vendor.

Enterasys will explain how elements of the Secure Networks architecture can be applied to an existing network to provide an easy to deploy solution to address illegal file sharing

concerns. Secure Networks architectural elements such as network policy enforcement, detection with location awareness, automated response and automated remediation found throughout the Enterasys product line will be used to address the requirements outlined in the Joint Technology Committee RFI.

The Enterasys response will provide answers to individual questions with combinations of products suited to meeting that particular requirement. The Enterasys switching, routing, intrusion detection/prevention and network management products are based on industry standards and all leverage the Secure Networks architecture to provide advanced functionality not available in competitive products.

As institutions find themselves investing in technology refresh cycles, Secure Networks enabled technologies will improve the ability to manage the concern of illegal file sharing, and improve the ability to support other organizational initiatives such as unified communications, server virtualization and compliance automation. The ability to further key organizational initiatives while at the same time gaining the ability to manage P2P file sharing presents a win-win opportunity for the organization.

#### Enterasys Submission Contents

**Enterasys® has responded in a point-by-point format to the structured outline provided in the RFI provided by the Joint Committee. Enterasys Secure Networks™ solutions discussed in this document are designed to secure any network from any vendor. Secure Networks, an architecture from Enterasys, provides key technologies that solve not only the peer-to-peer file swapping legal liability issues, but can also be leveraged to solve other security challenges at educational institutions. The Enterasys Secure Networks architecture is designed to ensure the integrity and performance of IT services and the higher education users that rely on them. Enterasys Secure Networks embeds security technologies directly into the network fabric itself to respond to threats proactively, increase operational efficiency, reduce deployment complexity, and scale as the network expands over time. Enterasys Secure Networks solutions discussed in this document include Enterasys® Network Access Control (NAC), Security Information and Event Management (SIEM), Distributed Intrusion Detection and Prevention (IDP) and Automated Response.**

#### Features of the Technology

This section of the response to the RFI should provide sufficient information about the vendor's technology so that the reader can acquire an adequate understanding of the tool, its method of operation, and its capabilities and effectiveness.

All technology submittals that are considered by the vendor to be applicable to the problem addressed by this RFI will be considered. However, the Joint Committee of the Higher Education and Entertainment Communities believes that most proposals will range over the following classes of tools. Some submissions may include features of several of these classes of tools. In those cases where the vendor possesses multiple tools, each should be separately discussed in its particular area of class of tool.

Audit Tools - This class of tool covers applications that could be used by systems administrators to configure and maintain computer assets owned by the university or college. Such tools may allow auditing of installed applications against a standard “build” for the machine or may allow profiling of file archives on university-owned storage devices, for instance on public ftp servers, etc.

**Enterasys response:** The Enterasys Dragon® Intrusion Defense solution includes Host Intrusion Detection Sensors (HIDS) for monitoring university systems and alerting if changes occur to the configuration from the established standard. The Enterasys Dragon HIDS protects at both the host and application level, monitoring the operating system and critical applications. Changes to the server are communicated on a secure channel.

A university deploying the Dragon Host Sensor on a protected host system would gain the benefit of Dragon’s variety of techniques used to detect attacks and misuse on the system. This includes analyzing the security event log (syslog), checking the integrity of critical configuration files, or checking for kernel level compromises.

For example; Dragon Host IDS monitoring a university FTP server would provide alert changes on new content added to the system, directory creation, systematic account failure (indicating brute password attack) as well as many other application and system level alerts.

Dragon Host Intrusion Detection monitoring offers assurance that changes to the host are logged via an encrypted alert channel to a centralized event processing system (Dragon Enterprise Management Server) to be processed for event notification and stored for historical reporting and potential forensic analysis.

Dragon Security Command Console provides an aggregation and intelligence engine for summarizing syslog and change control information from all the network devices, consolidates the events into alarms, prioritizes the alarm data and notifies appropriate personnel of configuration changes to key system devices. The Dragon Security Command Console provides key Security Information and Event Management (SIEM) summarization to improve the operation of a network operations or security operations center.

Bandwidth Shaping – This class of tools has the capability to adjust and/or alert other devices to adjust the amount of bandwidth and/or priority allocated in a network to a particular file type or application at any point in time. The technology may address uploading, downloading, or both, and may take origin or destination IP addresses into account.

**Enterasys response:** The Enterasys Secure Networks architecture provides for the classification of traffic and then applies permit/deny rules and setting class of service (CoS) and/or packet rate limiters on a per application, per user or per port basis. These classifiers can be leveraged as enforcement (above) or as detection mechanisms that automatically modify the established forwarding policies to contain users or systems deviating from established standards.

Enterasys also provides its patent-pending [Distributed Intrusion Prevention solution](#) to extend the scope of bandwidth shaping from perimeter devices to the network edge. The solution integrates with switches and intrusion detection/prevention appliances from multiple vendors to leverage existing infrastructure investments while automating responses to security incidents. This provides a solution framework that works with the existing infrastructure investment and provides a solution for mitigating illegal file sharing and other security concerns facing the university.

In the example of a unauthorized P2P connection, the Enterasys Distributed IPS solution locates the source of the attack's access to the network and reconfigures network devices from Cisco, Enterasys, Foundry, HP ProCurve, Juniper, Nortel, and other vendors to rate limit or prevent future access. Depending on the capabilities of existing switches, automatic responses can range from throttling inappropriate traffic and/or blocking individual user/device access (for Enterasys policy-enabled switches), assigning packets to a quarantine VLAN (for all RFC 3580 compliant switches) or turning off the port (for any SNMP MIB II compliant switches)

Data/File Sharing Blocking – This class of tool takes an active role in blocking and preventing access to file-sharing and/or streaming applications on a network or machine basis. The technology may block access based on external information such as DMCA notices.

**Enterasys response:** As mentioned in the Bandwidth Shaping response, the Enterasys Secure Networks enabled infrastructure components are capable of not only rate-shaping P2P traffic, but can also block that traffic. The traffic can be isolated per machine or user and different forwarding policies can be enforced on a per machine or per user basis. For example, a student using their laptop would be prohibited from using a P2P protocol, but would be able to use that protocol on a campus provided system.

Alternately, or in cooperation with the Enterasys Secure Networks enabled infrastructure, the Enterasys Distributed Intrusion Prevention System can accept messages such as SNMP, syslog and email alerts as notifications (such as an electronic DMCA notice) and provide location and remediation configuration to the network. This includes the aforementioned capabilities of rate-limiting an application or port, blocking specific protocols or shutting down the network connection (port).

During the remediation period, end user notification is attempted via protocol redirection, email messaging, instant messaging etc., to notify the user of the violation and subsequent network service changes. The Enterasys Distributed Intrusion Prevention System leverages an open architecture so different remediation and notification solutions may leverage the data for end-user and operations center notification.

Matching, Screening and Filtering – This class of tool can match transmitted data with, for example, data in a predetermined database and provide administrative reporting and/or

selective filtering. This includes technologies that can provide activity reporting without blocking.

**Enterasys response:** The Enterasys Dragon Intrusion Defense solution leverages three different approaches that can be combined to provide a view into peer-to-peer protocols and their use on the network. These approaches; packet pattern, protocol and behavioral analysis each provide data used to generate administrative reports on the use of the network environment.

Packet pattern analysis provides connection attempt information for many P2P networks, and the XML-based signature libraries are perpetually updated and customizable by the customer. Protocol analysis suites allow for the verification of protocols as they are transmitted and monitors for multiple types of evasion techniques, techniques that misuse common network protocols to evade monitoring. The Dragon behavioral monitoring suite analyzes network connections and looks for anomalies, such as rogue servers and P2P hot spots.

The Dragon Intrusion Defense solution leverages this information, as well as information from external sources to provide visualization for current network and historical network operations. Pre-formatted administrative reports are available as well as customizable reports, such as analysis of peer-to-peer application usage.

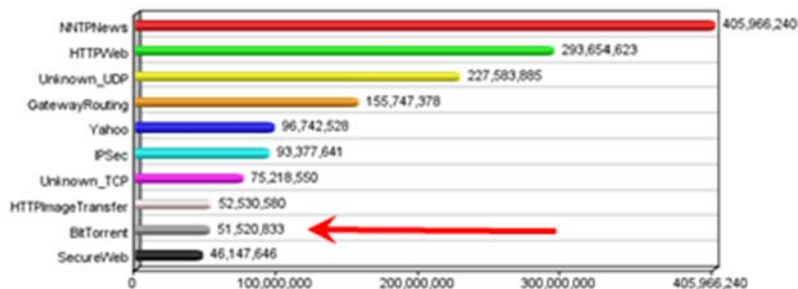


Figure 1 - Dragon Protocol Summary

The Distributed Intrusion Defense solution can be paired with the Dragon Intrusion Defense solution to perform screening actions based on traffic match criteria. The screening actions can be broad or granular and can be enforced at network consolidation points (ex: distribution layer) or at the individual port level.

User Management and Communication – This class of tool can match the inappropriate action with the infringer and then communicate with the user. This includes technology to configure graduated levels of response and actions.

**Enterasys response:** Enterasys provides, as part of the Distributed Intrusion Prevention System, an end-user Remediation System. Available to work with existing network hardware, the user can be redirected, based on the policy settings, to a centralized remediation system. The centralized remediation server correlates data from the Enterasys Distributed Intrusion Prevention System for the individual, and the resulting web

page notifies the user of their violation. A sample message would read “you have been found to be using P2P protocols against university policy”.

The Enterasys Distributed Intrusion Prevention System will first provide a warning of policy violation and if the policy violation continues then escalate the response and action based on university policies. This is the “Three Strikes You’re Out” scenario used at many of Enterasys customers not only with peer-to-peer problems but with other network misuse problems as well. Using an architectural approach, a customer can gain the benefit of managing P2P without assignment of dedicated equipment.

With the Enterasys solution, end-user (student) personally identifiable information does not need to be stored or presented. This addresses a concern voiced by several universities during the Technology Committee meetings. The amount and type of data retrieved and presented is customizable to meet each organization’s specific requirements.

Network Performance – This class of tool is directed at overall network operation, performance and traffic analysis. Such tools may simply provide information such as traffic data/session, source address, application type, destination address, ports, etc.

**Enterasys response:** Performance visualization tools also can be leveraged (depending on information they can provide) to analyze network traffic to identify potential abuse of established policies, including those centered on use of particular applications and protocols.

One of the issues identified at previous Technology Committee meetings was having enough visibility – especially at the network edge closest to the user. NetFlow is one of the more popular methods for collecting flow data for analysis by management and security tools. Not all flow collectors are created equal. Some products implement flow sampling which limits the data collected – misstating the actual network metrics.

Enterasys implements full NetFlow support with no data sampling in its Matrix® line of switching and routing platforms. With the Enterasys Matrix, performance and security systems get all the traffic and a clear picture of what the network state is. Accurately reporting the network traffic with statistics of which machines (IP addresses) are communicating with other nodes, the protocols they use and the amount of traffic exchanged allows performance management and security management tools to provide accurate reports of the network operation and usage.

Enterasys Dragon Security Command Console provides clear reports on data/session and includes data such as source and destination address, protocols and ports used and amount of data exchanged per session. Top 10 reports can be automatically produced and behavioral signatures can be applied to look for “Top 10 P2P” systems (subscribers and hosting systems).

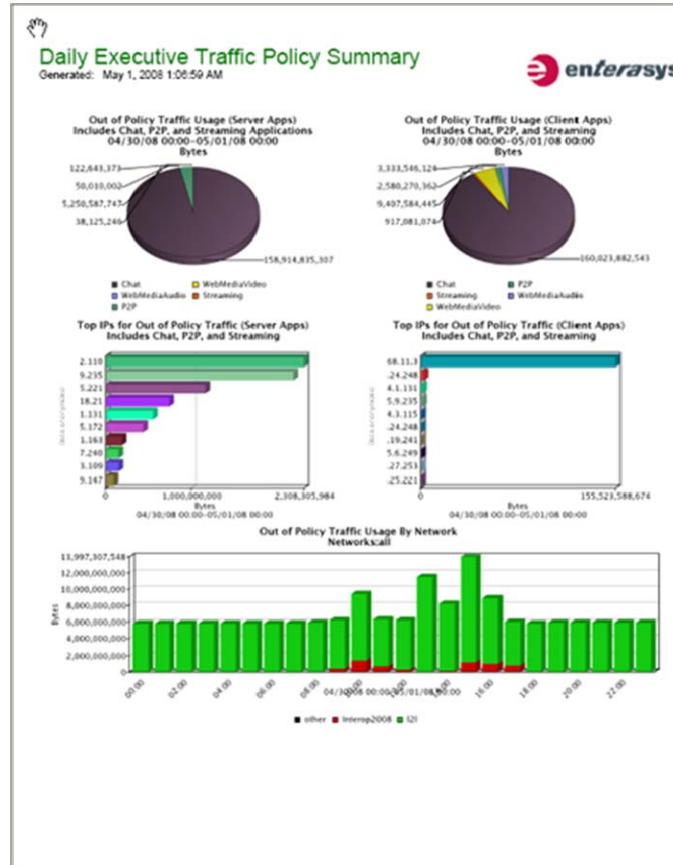


Figure 2 – Top 10 Policy Violations

The Network Surveillance and Flow Viewer components of Dragon Security Command Console provide a wealth of information in particular, the Network Surveillance component allows engineers to graphically view network traffic and data mine on spikes of interest. Network Surveillance graphs display the time interval on the x-axis and the volume of traffic on the y-axis. The Flow Viewer displays data such as source and destination IPs and ports, byte count information, protocol, application, QoS, flow source, source or destination ASN, and much more. In addition, the display types (aggregates) allow for the quick generation of top-talker and other network-centric reports.

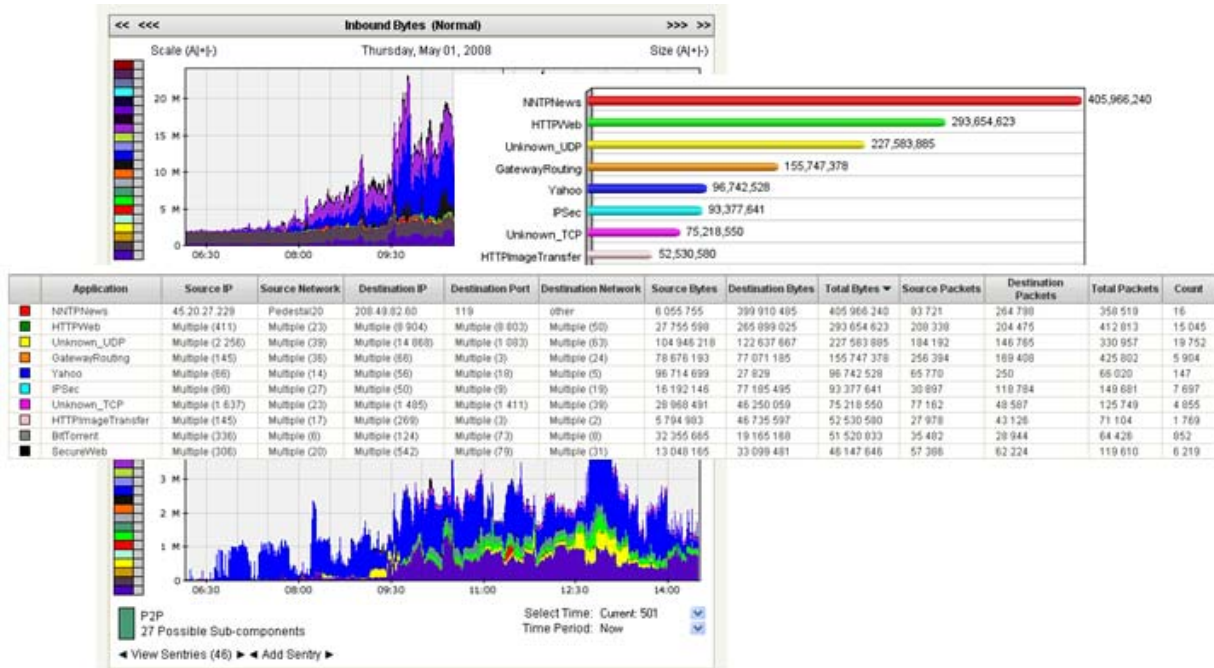


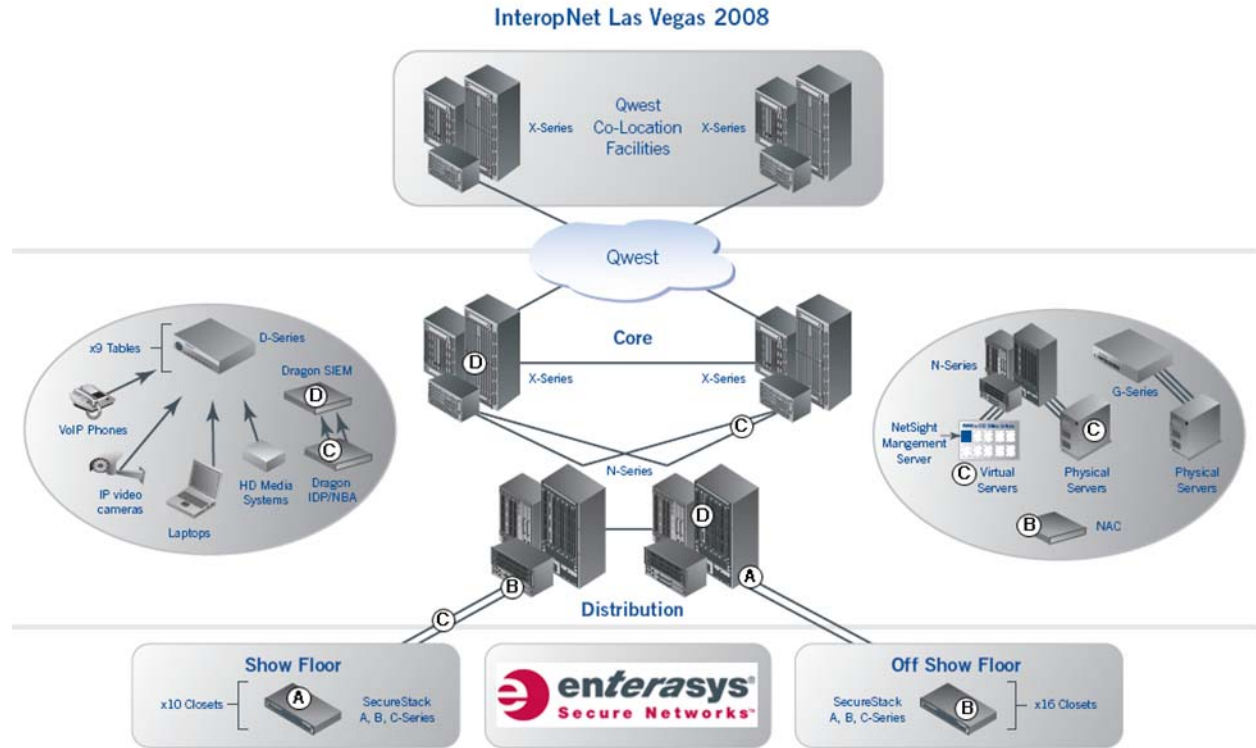
Figure 3 - DSCC Flow Views

Enterasys Dragon Security Command Console can collect intensive flow information via dedicated Enterasys Dragon Flow Collectors, but can also use NetFlow data provided by existing switches and routers in the campus environment. This addresses the “number of canaries” problem presented by a campus at the Technology Committee meetings.

### Network architecture

The vendor should provide descriptions of how its technology could be installed in typical networks including architecture diagrams.

Enterasys response: Using the [2008 Interop network](#) as a sample network, the following solutions are an example of network areas that can be improved using Secure Networks solutions. The whitepaper describes how Enterasys delivered a world-class policy enabled network for 40,000 users in less than 40 days. The network challenges with Interop were very similar to most higher-education solutions, always available without intruding on which applications could or could not run on the network. The network below was implemented without any firewalls, similar to some university networks.



**Figure 4 - InteropNet 2008 Sponsored by Enterasys**

Legend:

- A: Policy Control
- B: Enterasys Network Access Control
- C: Enterasys Intrusion Defense
- D: Enterasys Behavioural Flow Sensors and NetFlow compatible products

**Enterasys Response:** Universities may opt to leverage combinations of technologies that best match their business objectives. For example, in new construction – upgrading to Enterasys policy-enabled switches (A) would allow for granular control over applications (forward/deny, rate limiting, etc) and this can be assigned by user group. For legacy network edge, upgrades to key network aggregation switches (A) can provide similar controls.

Combining Enterasys Network Access Control (NAC) (B) with either Enterasys or legacy switches can provide context to whether network systems are running applications not in compliance with established organizational standards. For example, network-based assessment of end-points might find a group printer that has been compromised and hosting copyrighted content.

Enterasys Dragon Network and Host Intrusion Detection/Prevention (C) technologies can be deployed to monitor network packet data for connections to unauthorized peer-to-peer networks or detection of changes to key servers such as the installation of unauthorized peer-to-peer hosting services.

If intrusion detection or security information event management projects are funded, the Enterasys Dragon Security Command Console can aggregate data from a variety of sources, including Dragon Behavioral Flow Sensors and switch/router NetFlow data (D) to provide context into network utilization. This can include (or not) any depth of personal data (optional integration with NAC data for resolution to a person). Standard event resolution is event to location.

Enterasys has provided webpage addresses below to whitepapers for each solution discussed within our response. These documents include typical architecture diagrams for how the technology could be installed within a given Network environment.

- [Enterasys Secure Networks Peer-to-Peer Security Solution](#)
- [Enterasys Secure Networks Network Access Control Whitepaper](#)
- [Enterasys Secure Networks Distributed Intrusion Prevention System](#)
- [Enterasys Supporting Compliance: A Network Approach](#)

#### *Scalability*

Due to the high capacity of many university networks, particular reference should be made to the scalability of the tool. Each vendor should discuss the throughput of its technology (using aggregate bandwidth handled as the standard of measure), and the potential effects of its technology on network latency.

Enterasys response: Enterasys Secure Networks has been proven in user environments from 10,000 to 60,000+ users. Some case studies for your consideration are:

- [Bethel University](#)
- [University of North Carolina – Chapel Hill](#)
- [University of Bern](#)
- [European Investment Bank](#)

The throughputs of the various technologies that have been presented are on par with industry established standards. Secure Networks components are designed to have minimal, if any, performance impact on the transmission of packet data. As each network is unique, and the products selected variable – it is recommended that a customer contact Enterasys Networks or one of its authorized sales agents to discuss the implementation of a potential solution.

### Protocol identification

The vendors should discuss whether and how network protocols are identified (e.g. by port number, by layer 7 analysis, etc.) and the methods that the vendor uses to update its software to detect new and mutated protocols. The vendor should address how the technology is able to adapt to changes in protocols as they evolve.

Enterasys response: The Enterasys Secure Networks enabled infrastructure can [identify, classify, prioritize](#) and secure traffic based on criteria specified in Layers 2,3 and 4 of the standard OSI model (Figure 5). As networking products advance, future switching products will provide same functions and include Layer 7 (Application Layer) with deep packet inspection.

The Secure Networks enabled infrastructure products provide the ability to remove unwanted protocols that could be used to establish 'darknets', enforce IP addressing rules and verify which protocols may be forwarded by particular end-points.

Enterasys Dragon advanced security applications (Dragon Network IDP and Dragon Behavioral Flow Sensors) perform Layer 7 deep packet inspection. This provides critical vision into the traffic traversing the network. Both Dragon applications provide a full suite of protocol analysis – examining for protocol misuse and mutations occurring in current protocol use.

Dragon Security Command Consoles (DSCC) can detect unauthorized peer-to-peer activity through its Network Behavioral Analysis (NBA) threat detection, application-level policy setting and broad threat analysis. DSCC determines the true source of an attack or behavior by initially profiling all aspects of normal network behavior, per host, application by network etc. The algorithm that enables this is the Holt Winters Triple Exponential Smoothing Algorithm. When abnormal behavior occurs, such as a new P2P server the behavior analysis within DSCC enables the identification of 'out of characteristic conditions' down to the specific.

Examples of problems detected by DSCC network behavioral analysis in customer environments:

- Peer to Peer networks
- Darknet discovery
- Worm propagation
- Illegal file transfer, data theft
- Denial of Service attacks
- Botnets
- Spyware
- Rogue servers/services
- Reconnaissance
- Applications on non-standard ports (SSH over port 80)

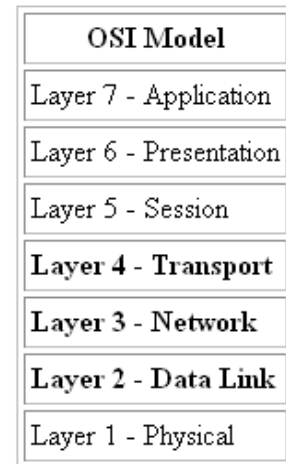


Figure 5 - Standard OSI Model

- Communications to undesirable geographies or remote networks
- Trojans

#### *Granularity of protocols*

Each vendor should discuss its technology (where applicable) in terms of addressing those file sharing applications that employ multiple protocols (e.g. control, searching, file transfer, etc). Descriptions should be provided as to: which protocols does the vendor's technology detect; whether the technology can address each of these protocols independently; and whether different rate limits can be set for "search" vs. "file download."

**Enterasys response:** Enterasys Dragon advanced security applications (Dragon Network IDP and Dragon Behavioral Flow Sensors) perform Layer 7 deep packet inspection. Leveraging the deep packet inspection, Dragon applications can examine packet data to determine network joins to peer-to-peer networks. Dragon can identify instant messengers and P2P applications such as:

- Gnutella
- Kazaa
- eDonkey
- BitTorrent
- SoulSeek
- LimeWire
- DirectConnect
- AOL Instant Messenger,
- MSN Messenger
- Yahoo! Messenger
- ICQ

Dragon also provides XML based open tunable signatures which allow implementation, modification, and custom creation of a set of signatures designed to detect protocols that apply to each unique environment.

#### *Product Configuration and Installation*

The vendor should describe how much downtime is required for installation and maintenance and what elements of the network are involved. The degree of network integration and integration with other products should be presented. The vendor should discuss if the technology requires initial setup by individual users or requires installation of any components on individual user PCs. Specify if there are other setup or maintenance actions at the user level.

**Enterasys response:** Enterasys solutions outlined in this response require no end-user configuration, registration or effort. There are no requirements to load any agents or perform any configuration changes on student systems for the Enterasys peer-to-peer solutions to provide immediate benefit to the university.

Downtime required for the successful installation and maintenance of our solutions will vary. Some solutions are more intrusive to the network while others can be configured and tested with minimal network interference.

End user requirements and user configurations are driven by which solution is deployed within a given infrastructure. If user configuration is required, this would be based on the type of authentication and/or the type of assessment along with any remediation requirements. Conversely, some of our offerings are completely transparent to the end user.

Each customer network is different and Enterasys will approach configuration and installation engagements based on defined prerequisites as a guideline. To that end, Enterasys Professional Services will identify individual customer needs using our plan/design/implement/operate methodology. Using this methodology provides Enterasys Professional Services with the required information needed to properly set customer expectations and to deliver a quality implementation within budget and on time.

#### *Content identification*

If the technology operates at the individual file level and is intended to selectively identify communications that represent potential infringements of copyright law, explain in detail how the technology will identify such content. The vendor should specify what categories of content can be identified (i.e. compressed audio files, video, images, etc). The vendor should list any external content databases that are required, and whether or not they are proprietary. The vendor should indicate what information, if any, is captured and reported for further analysis and actions.

**Enterasys response:** Enterasys has partnered with many companies, including Audible Magic, to provide solutions for customers that require content identification. Audible Magic's CopySense appliance has integrated capabilities to send event data regarding a local network machine (IP address) that is transmitting protected materials.

Enterasys Distributed Intrusion Prevention System can accept CopySense event traffic, resolve the offending machine to the network ingress (wall-plate or WiFi access point) and apply network traffic policies to disable the transmission and provide traffic redirection to a network remediation point to inform the end-user of the violation and any subsequent actions.

#### *Examination of network packets or file content*

Each vendor should indicate any aspects of the use of its technology that requires the examination or "opening" of network packets or files of information in order to carry out the technology's work. The vendor should indicate which fields of the Internet packets and which components of corresponding files are used by the technology and in what way. The vendor should include not only the degree of content inspection that is required in order to make the technology work, but also the degree of inspection and logging that the



identify connection attempts for a range of known P2P applications. Enterasys Dragon IDP signatures are customizable to support organization specific requirements.

### *Distribution systems*

Each vendor's response should specifically list all file sharing protocols or networks for which the technology is effective. In addition, the vendor should list other distribution systems, such as FTP, IRC, Usenet, for which the technology is applicable.

**Enterasys response:** Enterasys Dragon IDP and Security Command Console support and analyze a number of protocols such as: DNS, FTP, H225, H245, HTTP, IIS Unicode, NTP, RIP, RPC, SIP, SMB, SMTP, SNMP, Telnet, Unicode, Unicode v2, TCP, UDP, ICMP, etc. A sample of current file sharing protocols supported includes:

- Gnutella
- Kazaa
- eDonkey
- BitTorrent
- SoulSeek
- LimeWire
- DirectConnect

In addition to this list, Dragon provides an open signature architecture and custom signatures can be written for any protocol or application.

### *Resilience of the technology to countermeasures*

Each response should indicate the technology's ability to resist:

- (i) Countermeasures by file sharing software, for example, file compression, data encryption, etc.
- (ii) Circumvention efforts by users ( i.e. port tunneling, proxy servers, fragmented packets, etc).
- (iii) Denial-of-service or other attacks against components of the technology.

**Enterasys response:** Solutions to this problem will be affected by many factors, including campus policies on protocol usage, presence of alternative file sharing systems, etc. Enterasys will outline the current state of the industry and recommends that interested parties make inquiries as technologies and methods are in constant flux.

Illegal file sharing has evolved as measures to control it have not. As identified at the Joint Technology Committee meetings, this is a virtual arms race between IT departments and the violators. As the committee has learned, there is a trend to defeat popular methods by encrypting the data streams – so the content itself cannot be learned (point one above).

While encryption technology can disable content monitoring, behavioral monitoring can identify network attached end-systems that are creating and maintaining more connections with higher traffic volumes than their peer group. While there is no indication

of a violation of campus policy with behavioral monitoring alone, it is a valid tool not only for investigating potential violations of illegal file sharing and other network problems such as a worm-infested host.

Many universities are offering a hosted file sharing alternative, and this makes the above problem much easier – especially for file sharing protocols that are known to be [primarily used for illegal file sharing](#).

Users will still seek to circumvent controls established in the network to achieve their goals. Implementation of audit and control systems such as Enterasys' Distributed Intrusion Prevention System identifies protocol anomalies e.g., excessive fragmentation, port tunneling and unauthorized proxies, and can then identify the actual offending source station and enforce network remediation techniques to contain the threat. The Enterasys Dragon Security Command Console also includes a notation library that is searchable, so when repeat actions or similar actions occur – the network operator can search and review past cases to compare the current event to what was seen before.

Other implementations such as integrating with Entertainment Community projects such as [Automated Copyright Notice System](#) (ACNS) are currently feasible within the Enterasys Distributed Intrusion Prevention System today. If a university were to implement an ACNS system, event data from the ACNS system could activate the Enterasys Distributed Intrusion Prevention System to locate the offending system and then provide optional logging and administrative notification or implement remediation actions to isolate the offending system(s) and start remediation notices to those system operators. This is achieved by leveraging the Secure Networks architecture and Enterasys' adoption of standards and implementation of standard interfaces.

#### *Testing and installed base*

Each vendor should provide descriptions of the extent of testing of its technology, particularly the testing procedures employed prior to releasing an updated version (e.g. an updated detector) and specific examples (where available) of how technology applies in real-life situations. The vendor should describe the features, maturity, status, availability, and installed base of its technology for each version that is currently supported.

**Enterasys response:** Enterasys is committed to exceeding the networking and security expectations of enterprise customers worldwide by providing complete, reliable products, and service and support based on industry standards. All products go through a thorough quality assurance testing process before being released. As part of this process, products are tested in a lab environment to ensure functionality and stability before released for Beta Testing. Beta Testing is performed by Enterasys approved sites and additional development and testing is performed as needed.

The monitoring and analysis components of the Enterasys solution are tested and certified using several complimentary methods which make use of a variety of tools. For testing with Dragon, these tools include machines to generate a variety of exploits as well as traffic generation equipment such as Spirent Avalanche, Spirent Reflector, Spirent Smartbits and IXIA. We also incorporate a customized automated test harness to generate signature based traffic to verify the proper response is received from Dragon in the form of



a database update, page, email or SNMP Trap. The traffic generated simulates network traffic that may be sent by computer criminals, hackers, network anomalies, and employee misuse.

We verify that Dragon is capable of detecting and logging a wide range of common exploits accurately. We use an automated test harness to generate traffic for each of the signatures loaded into Dragon and to automatically verify that the proper database update occurs or that the proper email, page or SNMP Trap is sent for each individual signature. This test harness allows us to automatically deploy a specific set of signatures to the sensor and verify that only those signatures that are deployed cause an event to be triggered.

We maintain a library of exploit and attack scripts or pcaps designed to generate traffic in the following areas: HTTP, HTTPS, DNS, FTP POP3, SMTP, SIP, Telnet, and ICMP. In addition, we run a variety of tests to ensure that our solutions are resistant to false positives.

All discussed Enterasys solutions are generally available and have been deployed in numerous College and Universities worldwide.

#### *Competitive approaches*

Each vendor should provide clear descriptions of how its technology compares to other known competitive approaches and the benefits of its technology over competitive approaches.

**Enterasys response:** Most network security appliances can identify an attack by source IP address, MAC address or other such packet header information – but very few can find the physical location of the attacker. This is a major impediment to rapid response because it limits IT / Security Operations to blocking the attack, rather than isolating and remediating the attacker. Enterasys Distributed Intrusion Prevention has been developed specifically to address this challenge.

Enterasys Distributed Intrusion Prevention is a multi-vendor application uniquely designed to accept security events from any vendor's security hardware or software, locate the switch where the attacks are entering the network, and take immediate action to stop the threat. When deployed in combination with a Secure Networks enabled infrastructure, Enterasys Distributed Intrusion Prevention delivers the additional granular control of dynamically denying, bandwidth rate limiting or changing the priority of the threat source's access to the network.

Enterasys Distributed Intrusion Prevention intelligently interacts with Enterasys Dragon and other third-party advanced security applications e.g., Audible Magic CopySense, to automate responses to security incidents. A simple example is automatically disabling or isolating the source of illegal or inappropriate traffic that was identified. Enterasys Distributed Intrusion Prevention can search and locate attacker IP addresses located within the network and provide response action through the network infrastructure. Actions that can be taken by utilizing the network infrastructure include disable the

attacker switch port, quarantine VLAN, or switch port policy to prevent the specific attack traffic. Attacks that are mediated at the switch port provide greater protection for other internal IP assets compared to techniques that only update edge router ACLs or firewall rules.

#### *Third-party components*

Each response should describe any third-party components required by the technology that are not provided by the vendor, but necessary for implementation (i.e. content databases, etc).

**Enterasys response:** The Enterasys solutions are not dependant on third-party components. The solutions are designed to work with third-party hardware and security applications.

#### *Comparison with Hypothetical Scenario*

Technology and its capabilities to respond to the hypothetical scenario should be discussed.

**Enterasys response:** Enterasys has provided webpage addresses below to whitepapers for each solution discussed within our response.

- [Enterasys Secure Networks Peer-to-Peer Security Solution](#)
- [Enterasys Secure Networks Network Access Control Whitepaper](#)
- [Enterasys Secure Networks Distributed Intrusion Prevention System](#)
- [Enterasys Supporting Compliance: A Network Approach](#)

#### *Performance with respect to the Requirements Described in the 2007 Workshop Report*

Provided in this section is a brief summary of the requirements that were documented at the April 2007 Workshop. Each vendor should refer to the report itself (<http://www.educause.edu/ir/library/pdf/CSD5170.pdf>) for a more detailed presentation. The vendor should provide a description on how their technology responds to the requirements presented in each of the areas in the Workshop Report.

#### *Identifying Infringing Traffic at the Campus Border*

The level of false positives (i.e., transmissions that are identified as infringing but are not) should be controllable by each individual campus. The settings that determine how many, or how few, false positives are generated should be selectable, rather than hard-wired into the solution. The solution should be time synchronized with the campus network to support accurate identification of the current assignment of IP addresses. The system should have a method for dealing with false positives (such as some sort of adjudicatory process that could be initiated by the student in response to an infringement notification). Further, it must be able to guarantee that critical traffic (e.g., network control signals) will always pass through the system unhindered.

The solution must be network friendly to the existing campus network architecture and “fail open.” That is, it must have no effect on network traffic in the case of system failure. The solution must be transparent to unrecognized traffic and induce no additional latency and jitter. The solution should operate in a way that leaves decisions to notify users and the Network Operations Center (NOC) of flagged infringements up to the individual campus. It should have the capability and flexibility to identify and/or block at either the application level or at the individual media file content level.

The solution must be able to evolve technologically as new protocols, signatures, modalities, and other changes occur in the file sharing technologies. Updates and upgrades should be supplied automatically by the vendor and must be easy to install and operate. The solution should work not only at the current speed, but also have the ability to be upgraded through a range of speeds (E.g. 1-10-100 Gigabits/sec) in tandem with the campus network.

Logging should be capable of being turned on or off, as well as be able to set the retention and deletion dates of logs, determine what is captured in the logs, and how those logs are used. The ability to move logs to other devices should also be a capability, and such logs should be protected.

**Enterasys response: The solutions discussed from Enterasys are scalable and offer configuration flexibility to meet the desired goals above.**

The Enterasys Distributed Intrusion Prevention suite can be deployed without any impact to the existing network infrastructure, with no added latency or jitter. Where applicable, the solutions can fail-open so there will be no impact of network traffic flow if a system failure were to occur. The Enterasys solution is customizable to allow the decision of what to do if there is a violation up to the university. Enterasys solutions may be configured to log and report on as much or as little of the data, person or location of the event as the university requires as part of its compliance auditing efforts.

Enterasys maintains a staff of highly trained security research personnel who update our products, including signature database, by monitoring a variety of online open-source security resources, conducting internal research and through working with other security experts in various fields to keep Enterasys products detecting the latest security threats. As a threat becomes apparent, a new signature is written to recognize it and then deployed. Signature upgrades can be done automatically.

Enterasys Distributed Intrusion Prevention solution allows for scalability to work in networks of varying speeds and can be upgraded or expanded as needed in the campus network.

#### *Responding to Infringing Traffic at the Campus Border*

The technology should be selectively configurable to perform a range of responses, and the response policy at the campus level should be capable of being modified according to such considerations as source, destination, etc. The solution should be capable of integration with existing judicial systems so that the campus could elect to have an automated response to those users committing infringement violations. A flexible white

list of addresses that will never be blocked should accompany a solution that blocks at the border.

**Enterasys response:** Enterasys solutions monitoring and detection options deliver a flexible solution allowing you to configure what action should be taken to adhere to defined campus acceptable use policies.

#### *Identifying Infringing Traffic Local to the Campus Network*

Technology solutions should be capable of identifying infringing traffic within subnets at the lowest possible level. Technology implemented on the internal network must meet all the network-friendly requirements discussed in the border case in 6.2.1.

#### *Responding to Infringing Traffic Local to the Campus Network*

Technology implemented must support the usual topologies of internal campus network architecture. The technology cannot require routing all traffic through single points of failure. The overall solution must not interfere with the legal access to and transport of, \ non-infringing or authorized content within the campus network. The technology should provide the ability to select different levels of responses to flagged infringements. A technology designed to identify infringing traffic local to the net should support multiple CIDR blocks, or IP address blocks.

**Enterasys response:** Each of the Enterasys solutions discussed can provide system-wide visibility throughout the Local Campus Network.

#### *Supporting the Campus Judicial System*

Technology should provide appropriate, integrated, automated support for the campus judicial system and an interface for reporting flagged infringements. Communication between the identifying technology and the network operators (judicial system) should be secure. The technology should be flexible enough to provide campuses with a broad range of metadata and allow each campus to select what information is required. Communication of evidence to and from campus systems should be tamper-proof.

**Enterasys response:** The discussed Enterasys solutions can provide the level of data required to support each institution's unique Campus Judicial System requirements. Enterasys solutions can be implemented to provide the depth of information and restrict access to pre-defined systems or users. A sample of data available includes:

- Offense
- Source IP
- Destination IP(s)
- System MAC address
- User Name (if authentication available)
- Location (network location)
- Start / End
- Duration

- Event(s)

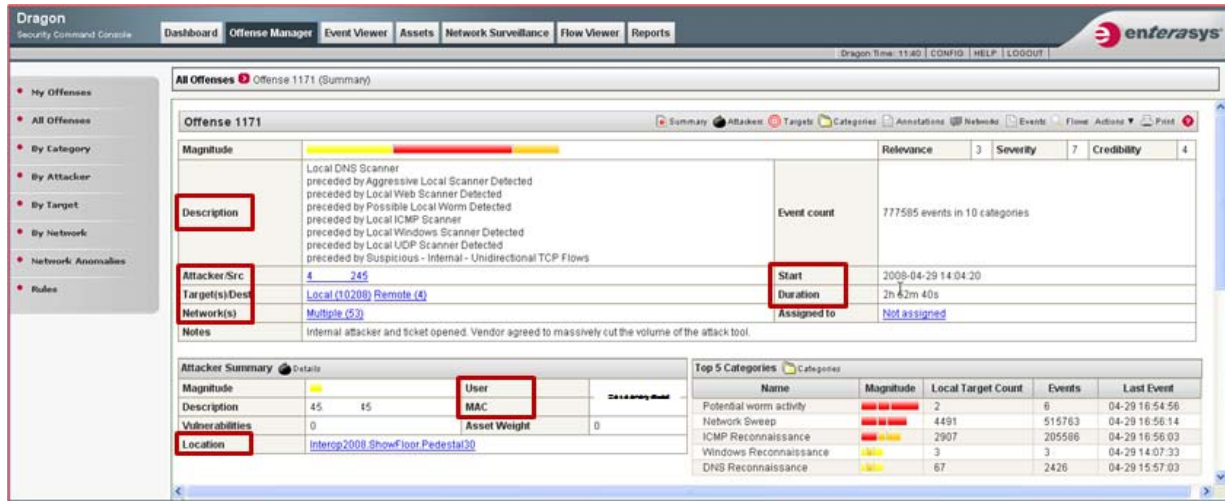


Figure 8 - Sample Judicial Data

### *Avoiding Disruption of All Non-infringing Traffic*

Technology should not affect the transmission of any and all non-infringing traffic. It should have the ability to support access to and distribution of content that has been flagged as potentially infringing, but could be permissible under fair use.

**Enterasys response:** Enterasys solutions monitoring and detection options deliver a flexible solution allowing you to configure what action should be taken to adhere to defined campus acceptable use policies. This includes event/alert actions and event/block actions. This is customizable per event or system.

### *Considerations for Purchase and Operations*

The technology should possess the characteristics of predictability, transparency, auditability, and scalability. Pricing must be predictable and include cost to purchase (or license), install, operate, maintain and upgrade.

**Enterasys response:** The proposed Enterasys solutions can be priced based on the specific customer environment. Scalability of the solutions will allow universities to implement the various solutions in phases. Enterasys' support & maintenance services have been built and are managed with a customer's uptime and reduced TCO in mind. Our standard warranties ensure products are protected against manufacturing defects, while our maintenance agreements typically enhance these services with additional features or extend the duration of coverage. We can be a partner that manages basic elements of support such as parts stocking and distribution or be your valued partner in a collaborative, continuous improvement support agreement with dedicated resources focused on improving network and support experience. Ultimately, our objective is to



provide customers with the level of coverage that most appropriately meets the demands of their specific environment.

### *Intellectual Property*

This section of the vendor's response to the RFI should provide information concerning intellectual property associated with the technology. The information should provide insight as to whether any patents have been applied for, when and in what territories, and what (if any) claims have been granted. Where a patent has been granted, the vendor should provide the patent number and attach an abstract of the patent.

The vendor should remember that submissions to this RFI are governed by Section 7. The vendor should not have the expectation that information held to be confidential will necessarily remain within the Joint Committee. **(Confidential information should not be included in the response.)**

**Enterasys response:** Enterasys has a strong history of [technology leadership](#) and product innovation. Our patent portfolio exemplifies our innovations in secure, intelligent, automated and integrated networking hardware and software solutions. We have assembled an experienced team of developers and engineers and have established a corporate culture that facilitates continuous product innovation. We intend to continue investing in research and development initiatives to strengthen and increase the functionality of our Secure Networks™ solutions.

### *Corporate Characteristics and Resources*

This section of the vendor's response to the RFI should provide information about the vendor's corporate capabilities. Include information about the vendor in terms of general and specific corporate characteristics: size, personnel, facilities, year of organization, corporate history, clients, revenues, capitalization, investors, etc. Information about corporate products or technologies other than that directly applicable to this RFI should not be included.

**Enterasys response:** Enterasys Networks, Inc. (Enterasys) delivers Secure Networks™ that ensure the integrity and performance of IT services and the business users who rely on them. Enterasys designs, deploys, supports and services integrated hardware and software solutions that intelligently sense and automatically respond to security threats on customers' networks, proactively preventing threats from entering the network.

Enterasys has more than 3,500 customers in 70 countries, including 109 of the FORTUNE Global 500. The company holds more than 500 global patents resulting from an R&D investment in excess of US \$1 billion.

### *Background & History*

Enterasys has been in the networking industry for over 25 years, having originated as part of the highly successful company known as Cabletron Systems, which was founded in



1983. Built upon strong engineering principles, Cabletron Systems helped develop the networking industry with the continual introduction of new technologies. Cabletron Systems became an innovative developer, manufacturer, installer and supporter of standards-based Ethernet, Fast Ethernet, Gigabit Ethernet, Token Ring, Fiber Distributed Data Interface (FDDI), Asynchronous Transfer Mode (ATM) and Wide Area Networks (WAN) networking solutions. As the enterprise market matured, Cabletron System's product family matured as well.

Enterasys was formed in March 2000 specifically to seize enterprise market opportunities and to better serve its customers. On August 6th, 2001 Enterasys officially began trading under the symbol of ETS on the New York Stock Exchange.

On March 1, 2006, Enterasys became a private company owned by an investor group led by The Gores Group, LLC and Tennenbaum Capital Partners, LLC. This is a significant milestone in the history of the Company and one that positions Enterasys for success. Our industry-leading Secure Networks capabilities are what made Enterasys a highly attractive investment for Gores and Tennenbaum. With the new partnership, Enterasys is continuing to develop innovative new products, solutions and services, and bring the unique business benefits of Secure Networks to more enterprise customers worldwide in order to fulfill our potential. Some of the many benefits of our new, private ownership include:

- Strong financial backing
- The ability to pursue opportunities not available to us as a public company
- The ability to take a leadership role in potential industry consolidation

Today, Enterasys is the perfect-sized company in that we are big enough to meet our customers' needs now and in the future, yet small enough to have a personal relationship with them. We encourage direct access to our talented developers and experienced executives.

How we measure our success is through our customers' satisfaction. By delivering on our promises on-time and on-budget, we earn the right to your business by putting the words *"There is nothing more important than our customers"* into action every day.

### *Financial Status*

Enterasys has built a solid financial foundation through profitable revenue growth, new customer additions, and new hardware, software and services delivery. We expect those trends to continue. In February 2008, Enterasys announced financial results for the fourth quarter and fiscal year ended December 29, 2007. Revenues grew for the second consecutive year while net income increased more than 100% over fiscal year 2006 and EBITDA was greater than 10% of revenue for the second year in a row. The company has now reported ten consecutive quarters of pro-forma profitability.

"2007 was a good year as we continued to increase customer satisfaction, grow revenues profitably, deliver new products and add significant new customers," said Mike Fabiaschi, President and CEO of Enterasys Networks. "As we begin 2008, I am optimistic that we can

continue to deliver profitable growth by leveraging the significant operating improvements we have implemented over the past two years.”

**New customers in APAC included:**

- Computing – IBM Philippines
- Government – Investigation and Legal Affairs Bureau Thailand
- Government – Korea Army 65th Div
- Professional Services – SK C&C
- Retail – Family Mart (Bogwang)

**New customers in the CALA region included:**

- Education – Universidade Estadual de Feira de Santana – UEFS
- Government – Banco de Prevision Social
- Government – Prefeitura Municipal de Cuiabá
- Government – Tribunal de Contas da União (TCU)
- Hospitality – Grande Hotel Araxá

**New customers in the EMEA region included:**

- Electronics – Philips
- Finance – Banca D’Italia
- Government – Slovak Army
- Government – Moscow North-West Underpass
- Healthcare – St. Bonifatius Hospital

**New customers in North America included:**

- Education – Murphy School District
- Education – University of Cincinnati
- Energy – Emerald Coast Utilities Authority
- Government – Instituto Nacional de Ciencias Médicas y Nutrición Salvador Zubirán
- Manufacturing – Mercedes-Benz

**Highlights for the fourth quarter of 2007 include:**

- Fixed Layer 2 switching port shipments, led by the SecureStack™ A-Series and SecureStack B-Series edge switches were up 6% on a year-over-year basis.
- Fixed Layer 3 switching revenues and port shipments for the SecureStack C3 triple speed Power over Ethernet (PoE) stackable switch increased more than five-fold from the year ago period.
- Revenues and port shipments for the new Enterasys® I-Series industrial Ethernet offering were up more than 250% sequentially for the quarter.
- Enterasys’ Diamond Distributed Forwarding Engines (DFEs) for the Matrix® N-Series flow-based switches continued to gain traction, with revenue and ports more than doubling sequentially.
- 10 GbE port shipments for the Matrix X-Series and Matrix N-Series more than doubled on a year-over-year basis.
- Triple-speed PoE shipments increased more than 90% from the year ago period as Enterasys continues to be deployed in conjunction with IP telephony (VoIP) solutions from Avaya, Cisco, Mitel, NEC, Nortel, Panasonic, ShoreTel, and Siemens.

- RoamAbout® wireless product revenue increased nearly 20% on a year-over-year basis.
- Revenues of the Enterasys Dragon® Security Command Console (DSCC) security information and event management (SIEM) solution increased nearly 90% sequentially, and posted gains of more than 400% compared to the year ago period.
- Enterasys Dragon Network IPS solution also posted strong growth, with revenues more than doubling on a year-over-year basis.
- License shipments of the Enterasys Network Access Control (NAC) solution once again doubled compared to the year ago period.
- Enterasys announced new solutions for Data Center Virtualization, Enterprise Notification and 10GbE IDS/IPS, while announcing customer success stories from Aldine ISD, Bethel University, Douglas County PUD, European Investment Bank, Grant JUHSD, and Sinclair Community College.
- Increased demand generation through face-to-face interaction with prospects at events where Enterasys demonstrates the practical, achievable, rapid time to value of Secure Networks solutions for convergence, connectivity and compliance.
- The addition of more than 150 new customers, bringing the total for the past seven quarters to more than 1,150.

### *Pilot Testing*

It is possible that certain colleges or universities may elect to test some of the technologies. The selection of those technologies will be done by the individual campuses based in part upon the results of the knowledge base created as a result of this RFI. Many factors will enter into the decision as to which technologies will be tested. One significant factor will be the level of interest and potential involvement of the vendor in the actual testing. Therefore, the vendor should present the vendor's concept for testing its technology in a real-life situation on campus. The vendor should also provide its concept for an evaluation license and any conditions that are associated with it.

The vendor's schedule for implementing its particular technology should be provided, allowing a period of sufficient duration to test and evaluate the results of that implementation.

The vendor should also provide information regarding the costs that might be incurred by a campus during pilot testing as well as information on whether or not they might consider conducting testing on a pro bono basis.

**Enterasys response:** One of the most useful tools we offer customers is the opportunity to evaluate our solutions in their test environment. More than just an "evaluation", a proof-of-concept [POC] provides customers the ability to have hands-on experience with our products, guided and supported by an Enterasys Solution Engineer, which enables them to fully experience the Secure Networks capability. Proving that Enterasys can deliver on our promises is a competitive differentiator as we stand behind our products. Performing a Proof-of-Concept (POC) is one of the best ways to have a potential new customer experience the value that Enterasys Networks can bring to their university.

### *Commercial Terms*

This section of the vendor's response to the RFI should discuss, in general, information about the commercial terms for its product (e.g. requirements for an annual license, requirements for annual maintenance, ability for one-time purchase). In those cases where the vendor has published prices for the subject technology, the vendor should provide those prices. If standard licenses exist, they should be provided as well. **In no instance should the vendor provide cost information that would not be considered public information.**

**Enterasys response:** General terms and conditions included with the purchase of Enterasys products and services are available upon request.

Pricing information can be provided by contacting Enterasys Networks at 1-877-801-7082, or +1-978-684-1000. Additional company, product or services information is also available at <http://www.enterasys.com/>

### *Additional Information*

This section of the vendor's response should present other information or raise issues that the vendor considers important in terms of documenting its product.

**Enterasys response:** Enterasys Networks would like to thank the Joint Technology Committee of Higher Education and Entertainment Communities for the invitation to respond to this Request for Information. We believe that Enterasys' 25 years of innovation and dedication to architectures based on open standards provides a better suite of options to the higher education community.

**We recognize that it will be many years before industry can create a "magic box" to provide a technical means to control illegal file sharing, but solutions do exist today that will reduce the problem space and make it more manageable.**

Enterasys also believes that customers should not have to make budgetary compromises to manage emerging network, security and regulatory concerns. Customers should consider a change in focus from product-centric solutions to architectural solutions to better manage their resources across all business projects. The Enterasys approach also offers financial advantages in that technology refresh budgets for connectivity upgrades can be leveraged to build-in, rather than bolt-on, the peer-to-peer traffic visibility and control solution.

Every problem should not require a new product to be deployed for resolution. With the Enterasys Secure Networks architecture, a customer can implement a [peer-to-peer visibility and control solution](#) to fit their current network, regardless of the incumbent vendor and be able to leverage that investment for other business projects.

Enterasys has explained how elements of the Secure Networks architecture can be



applied to an existing network during regular technology refresh cycles to provide an easy to deploy solution to address the problem of managing peer-to-peer networking and illegal file sharing. More information about Enterasys products and solutions can be found on our homepage at: [www.enterasys.com](http://www.enterasys.com).