

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

**Request for Information Response**

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

- Introduction ..... 3**
- 6.1 Solution Background ..... 3
- 6.1 Features of the Technology ..... 4
  - 6.1.1 Network architecture ..... 8
  - 6.1.2 Scalability ..... 9
  - 6.1.3 Protocol identification ..... 10
  - 6.1.4 Granularity of protocols ..... 11
  - 6.1.5 Product Configuration and Installation ..... 11
  - 6.1.6 Content identification ..... 12
  - 6.1.7 Examination of network packets or file content ..... 12
  - 6.1.8 Distribution systems ..... 13
  - 6.1.9 Resilience of the technology to countermeasures ..... 14
  - 6.1.10 Testing and installed base ..... 15
  - 6.1.11 Competitive approaches ..... 15
  - 6.1.12 Third-party components ..... 16
  - 6.1.13 Comparison with Hypothetical Scenario ..... 17
- 6.2 Performance with respect to the Requirements
  - Described in the 2007 Workshop Report ..... 17
  - 6.2.1 Identifying Infringing Traffic at the Campus Border ..... 17
  - 6.2.2 Responding to Infringing Traffic at the Campus Border ..... 18
  - 6.2.3 Identifying Infringing Traffic Local to the Campus Network ..... 19
  - 6.2.4 Responding to Infringing Traffic Local to the Campus Network ..... 19
  - 6.2.5 Supporting the Campus Judicial System ..... 19
  - 6.2.6 Avoiding Disruption of All Non-infringing Traffic ..... 19
  - 6.2.7 Considerations for Purchase and Operations ..... 19
- 6.3 Intellectual Property ..... 20
- 6.4 Corporate Characteristics and Resources ..... 20
- 6.5 Pilot Testing ..... 20
- 6.6 Commercial Terms ..... 21
- 6.7 Additional Information ..... 25
- Conclusion ..... 25**

## Introduction

---

### 6.1 Solution Background

As identified and articulated by the attendees to the “Workshop on Requirements for Technological Control of Illegal File Sharing on College and University Networks” the successful implementation of intellectual property protection on higher education campuses will resemble the three legged stool – in which ethics education, easy to use alternatives to illegal use and enforcement - are used in combination. Alcatel-Lucent believes that this multi-pronged approach will prepare today’s student for their work in corporations as Intellectual Property rights education and training have become part of the business ethics classes which major corporations require their employees to master and adhere to.

Alcatel-Lucent has read and understood the scope and goals of the Joint Taskforce. In particular, we have crafted our response to be aligned with the participating CIO’s desire of a solution which:

1. can be adjusted to reflect individual campus policies
2. does not degrade network performance or security
3. can address concerns surrounding privacy of communication and users
4. does not interfere with non-infringing traffic
5. meets normal standards of effectiveness and vendor support
6. can implement an automated initial notification system that retains the information that
7. can be used as part of an escalated judicial response for repeat infringers

To meet the needs for the Joint Taskforce, Alcatel-Lucent believes the OmniAccess SafeGuard appliances provide the features which allow large and small campuses, with homogeneous, or heterogeneous networking equipment to easily deploy. OmniAccess SafeGuard appliances provide comprehensive network admission control (NAC), visibility and auditing, user segmentation and threat containment benefits. They differentiate users and applications while controlling LAN access without massive infrastructure disruption, capital investment or performance upheaval.

The OmniAccess SafeGuard’s strengths are in providing flexible authentication, sophisticated host integrity checks, layer 7 policy enforcement, security threat detection, superior visibility and performance together with OmniVista Guard Manager. Unlike traditional network management systems that report at the MAC or IP level, OmniVista maps events to the network users. A user is identified by an appliance during authentication. This user ID (i.e., user name) is then bound to the MAC and IP addresses of the user’s computer, so all communications from the machine is then linked to that user ID. This architecture allows an administrator to identify any user incidents or identify the location of a violating machine.

This best of breed technology recently won the “Network World Clear Choice” award in Network World’s NAC appliance test. The key features for this response include:

- Network Admission Control (NAC) – authentication and posture check to control who can enter the LAN (wired or wireless)
- Comprehensive LAN Visibility – Incident- and exception-based information at Layer 7, including attributes such as file name, tied back to the user
- Identity-based Control – role-based access control to restrict user activities on the LAN
- Threat Control – block propagation of worms and other malware on the network (Statistical anomaly detection and intrusion protection)
- Client-less host integrity check for wire-line and wireless users (Windows (Vista, XP, 2000, ME, 98), MacOS X, and Linux operating systems)
- Per user stateful inspection firewall

While there are synergies when installed in an Alcatel-Lucent switched network environment, this product family can accomplish the goals as set by the Joint Taskforce in any third party network.

## 6 Submission Requirements

---

This section outlines the structure within which technology vendors are invited to respond to this RFI.

This structure is intended as a guideline. If the vendor feels their submission can be better handled in another form, we still welcome their submission, although 1) it must respond directly to all the questions raised in the RFI, and 2) extensive variations in format may severely limit the effectiveness of the response for the reader.

### 6.1 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.

Alcatel-Lucent Response: the OA SafeGuard solution provides the University the ability to load a dissolvable agent to all users of the network which can determine if the presence of unwanted applications on an enduser’s computer. Application detection includes recognition of the following P2P applications: BitTorrent, eDonkey 2000, Gnutella, WinNY, eMule, Kazaa, and AppleJuice.

The following table describes some of the host posture agent capability:

Method	Dissolvable Agent
OS Patch Level	Yes
Antivirus Patch Date	Yes
Antispy-ware Patch Date	Yes
Windows Registry Values	Yes
File: Presence	Yes
File: Running	Yes
File: Modified Since	Yes
File: Checksum	Yes
Malware: Presence of Key Loggers	Yes
Malware: Presence of Browser Plugin	Yes
Malware: Presence of Dialers	Yes
Malware: Presence of Hacker Tools	Yes
Malware: Presence of Remote Admin Tools	Yes
Malware: Presence of Screen Loggers	Yes
Malware: Presence of tracking cookies	Yes

Other reports that can be generated include:

**Malware events** – if a user triggers the anomaly-based traffic monitor

- User and Role, Malware Type (Algorithm triggered), Criticality, Time, MAC, S/D IP address, Status,

**Posture events** – if the user fails a posture check, the failure will be noted and what caused the failure.

**Authenticated User Sessions** – an audit trail of successful and failed log in attempts.

- User Identity and Role, IP/MAC of user, Authentication status, Authentication method (e.g. 802.1x, Kerberos, Captive Portal, MAC), Computer Name, Login Type, VLAN, Domain, Packets In/Packets Out

**Summarized Applications** – Reports applications for up to 300 different apps.

- Application name, total bytes/packets in/out, total number of users, total number of flows

**Applications by user** – same information as Applications, but now filtered by user

**Individual Application Flows with Layer 7 info** – all user flows are captured, if flows are from a protocol that SafeGuard decodes, application data is provided.

- Username and Role, Application Name, S/D IP, S/D Port, Start-time, End-time, Packets/Bytes In/Out, Application

**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.

Alcatel-Lucent response: the SafeGuard solution does not perform bandwidth shaping. However, we can allow/deny access to file types – i.e. allow FTP traffic, but deny file put/get of MP3.

**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.

Alcatel-Lucent response: the SafeGuard solution can implement 'flow' based restrictions and apply these policies to specific users or groups.

**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.

Alcatel-Lucent response: the SafeGuard solution does not perform signature matching. Instead, it can accomplish deep-packet inspection, glean the application (Layer 7) information and apply policies against specific applications and their flow (source/destination). For example, BitTorrent may be used by faculty. A policy could be created which allows internal BitTorrent traffic, but to deny the use of BitTorrent to access content outside the local campus.

**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.

Alcatel-Lucent response: the SafeGuard solution can redirect a user to a customizable web page that the university creates and maintains. This page could contain all relevant information that the user needs to understand what policy they violated and why it is important to adhere to the policy.

**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.

Alcatel-Lucent response: the SafeGuard solution can provide a vast array of reports and graphs which depict the traffic on the network. Network administrators can view Username, Role, IP address, MAC Address, Authentication Type, Login Time, Logout Time, Computer Name, Physical Login Port, VLAN, Total Bytes/Packets In/Out and all application flows.

In addition, a 'dashboard' is available which contains three tabs for the default reports – Network Awareness, Security Incidents, and User Sessions.

- Network Awareness
  - Top 10 User Sessions by Total Bytes
  - Top 10 User Sessions with Most Blocked Packets
  - Top 10 Destinations
  - Top 10 Websites
  - Top 10 Applications by Flow Count
  - Bottom 10 Applications by Flow Count
  - Top 10 Applications by Total Bytes
- Security Incidents
  - Total Active, Authenticated and Unauthenticated users, Authentication Failures, Policy Incidents, Malware Incidents, Incidents for unauthenticated users, Posture Incidents, Top User Roles with Incidents

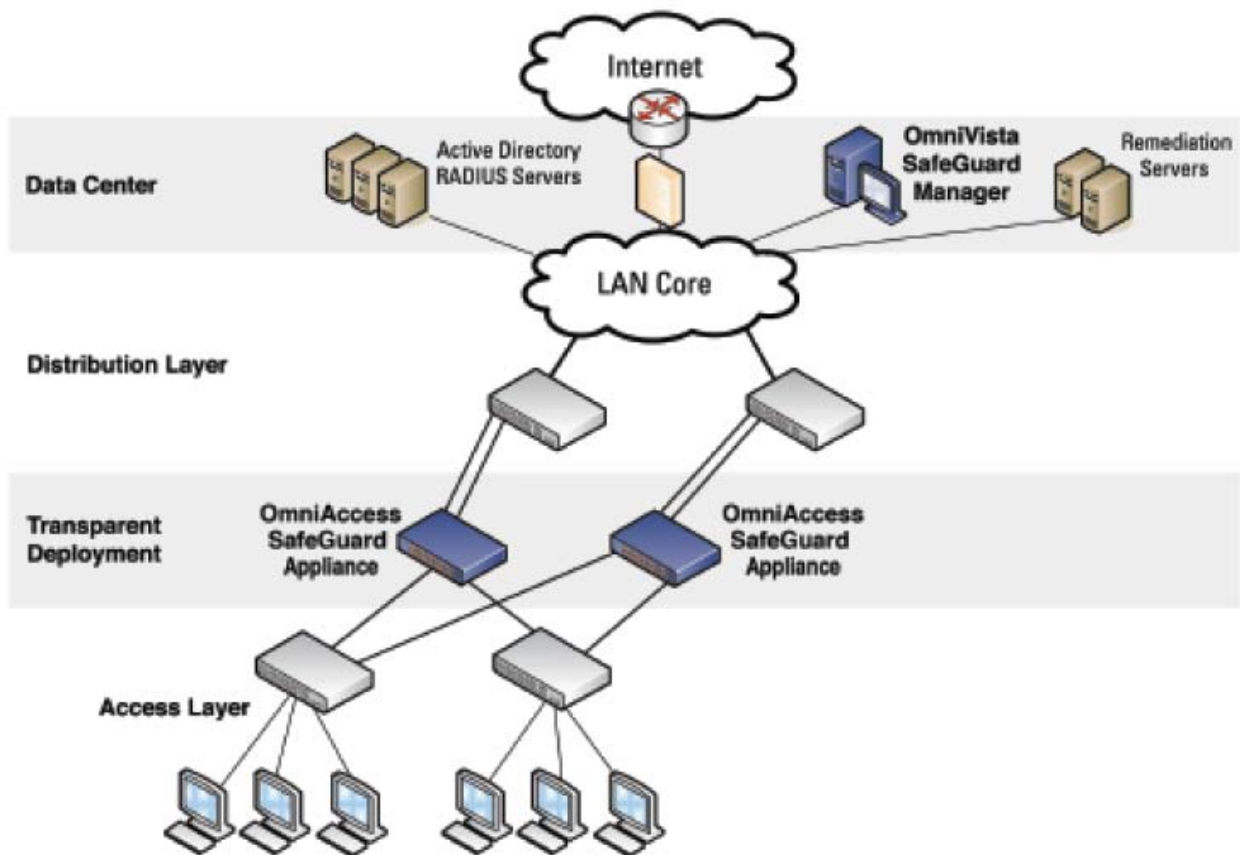
- User Sessions with Incidents
  - Authentication Failures, User Sessions with Policy Incidents, User Sessions with Malware Incidents, Unauthenticated User Sessions with Incidents, Posture Incidents, Top User Roles with Incidents.

Dynamic / customized reports are also available.

### 6.1.1 Network architecture

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

Alcatel-Lucent response: the SafeGuard solution is comprised of appliances (OAG-1000 and OAG-2400) and the appliance manager. The OmniAccess SafeGuard Appliances works with existing LAN infrastructure and authentication databases (Active Directory, LDAP) to provide the control capabilities.



A typical installation would look like this:

The OmniAccess SafeGuard appliances are designed to receive the LAN closet uplink traffic and pass it on to the Distribution layer and/or Core Ethernet switches.

OmniVista SafeGuard Manager is the application which pushes policy definitions to the appliances and pulls appliance information – aggregating and generating reports on the LAN/User traffic characteristics.

The Alcatel-Lucent OmniAccess SafeGuard silicon architecture provides the foundation for the SafeGuard Appliances’ capabilities. This custom hardware includes a 128-core processor and two programmable ASICs that work together to perform deep packet inspection at **4 Gbps (OAG-1000)** or **10 Gbps (OAG-2400)**. The programmability of the hardware enables Alcatel-Lucent to keep pace with changes in applications and security requirements.

### 6.1.2 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.

Alcatel-Lucent response: the SafeGuard solution is comprised of appliances (OAG-1000 and OAG-2400) and the appliance manager. The following table summarizes the OmniAccess SafeGuard Appliances ‘ performance and interfaces.

Model	OAG-1000	OAG-2400
Interface Ports	4 secure port pairs of 10/100/1000 SFPs  SFPs available in singlemode, multimode and copper	10 secure port pairs of 10/100/1000 SFPs  SFPs available in singlemode, multimode and copper
Extensibility Ports	2 extensibility ports for mirroring or HA, one rear management port	4 extensibility ports for mirroring or HA, one rear management port
Throughput	4 Gbps	10 Gbps
Maximum Active Users	800	2,000
VLANs	4,096	4,096

Supported		
Latency Average	30 microseconds	30 microseconds
Protocols	300+ Visualized, 30+ decoded or identified heuristically	300+ Visualized, 30+ decoded or identified heuristically

The SafeGuard appliance silicon architecture consists of the SafeGuard Processor, a 128-core CPU with massive parallel processing, and the SafeGuard Accelerator and Visualizer programmable ASICs.

The SafeGuard processor provides multithreaded technology with 128 cores. The ability to simultaneously process so many discrete flows is essential to providing deep packet inspection and control for networking applications, which do not exhibit the kind of predictive behavior that OS or other desktop applications display. The CPU architecture is also innovative in its memory design, enabling much faster access to the CPU's memory so that policy enforcement does not slow LAN throughput.

Only SafeGuard's patent-pending silicon architecture is capable of delivering breakthrough secure processing throughput and the flow acceleration needed to fully visualize and control LAN-based communications. The silicon architecture enables Layer 2-7 deep packet inspection at 10 Gbps full-duplex throughput rates for traffic flowing from users and the network core.

### 6.1.3 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.

Alcatel-Lucent response: the SafeGuard solution does not use ports to identify the application. Instead, it performs deep packet on the payload to decode the application used. However, if the university would like to filter on protocol/port, the following excerpt describes how to create a policy which relies on port/protocol.

To create a policy that matches the IP protocol of the traffic. It can be any of the following:

- any—Wildcard, which matches TCP or UDP protocols and application
- tcp—TCP

You can specify protocol port number and the port operation:

1 to 65535—End port or the start of the end port

GE—Greater than or equal to

NE—Not equal to

LE—Less than or equal to

range—Destination TCP port range

out-of-range—Out of the destination TCP port range

- udp—UDP

You can specify protocol port number and the port operation:

1 to 65535—End port or the start of the end port

GE—Greater than or equal to

NE—Not equal to

LE—Less than or equal to

range—Destination UDP port range

out-of-range—Out of the destination UDP port range

- AND logical operator

You can make a UDP or TCP protocol condition more specific by using the AND logical operator with an L7 application filter to application group. For example, you could specify 'tcp 80 AND application-group web' to define that the traffic is web and that it only runs on TCP port 80.

#### 6.1.4 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. "

Alcatel-Lucent response: the SafeGuard solution identifies the application and enforces policies based on the traffic to policy match. This flexibility allows the IT department to allow FTP traffic, but to restrict what files the FTP application can actually retrieve or place.

#### 6.1.5 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.

Alcatel-Lucent response: the SafeGuard solution is comprised of two types of products – appliances and management console.

The management console – OmniVista SafeGuard Manager – can reside practically anywhere in the network. Its duty is to receive traffic / user data from the appliances and broadcast policies to the appliances. The management console also generates the reports and keeps the appliance logs, time stamped to the network time.

The appliance sits between access switches and the distribution or core layer, aggregating uplinks from wiring closets and enforcing access policies on all traffic. A transparent device, the appliance requires no changes to network design or user behavior, simplifying deployment and lowering IT's cost of operations.

Additionally, the appliance supports high-availability and resiliency modes. Enterprises that have dual-homed wiring closet switches can deploy two appliances as peers — the two platforms share authentication state and preserve user authentications in case of failover. In addition, the appliance itself supports two failure modes. IT can set the device to fail to pass-through, where all LAN traffic will traverse the appliance untouched, or fail to block, where all traffic is stopped. The Controller also includes redundant power supplies and fans.

The appliances possess 'paired' SFP ports – in-flow and out-flow, In-flow ports are from the user to the network, Out-flow ports are from the network to the user. When installing the SafeGuard appliances, the fiber or copper from the LAN closet are connected to the in-flow port and the fiber or copper connected to the distribution or core switch are connected to the out-flow ports.

If the university would like to employ endpoint posture validation, a dissolvable agent will be pushed to each device – whether or not the device/user has successfully authenticated.

Policy configuration can be accomplished via a industry standard like command line or a GUI.

#### 6.1.6 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.

**Alcatel-Lucent response:** the SafeGuard solution can identify file types, however its main method of identifying illegal traffic is based on application signature. Therefore, there are no external databases or signatures that need to be accessed or kept current in order for this solution to operate optimally.

#### 6.1.7 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 technology is capable of performing (even if “turned off” by the user or system administrator).

Alcatel-Lucent response: the SafeGuard appliance performs 'deep packet inspection' to identify the application. OmniVista SafeGuard Manager marries the IP/MAC addresses to the user and logs details of all flows through the network.

#### 6.1.8 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.

Alcatel-Lucent response: the SafeGuard appliance can detect hundreds of applications, including P2P and legitimate file transfer protocols (FTP, CIFS, HTTP(S)). Applications include:

##### **Business Apps**

- Oracle TNS
- SAP R/3
- VOIP
- SIP
- H.323
- Cisco SCCP (Skinny)

##### **Web/Mail**

- HTTP
- SMTP
- POP3
- IMAP

##### **File Transfer**

- FTP, FTP-Data, TFTP
- CIFS/SMB/NetBIOS

##### **Network Services**

- DNS
- DHCP/BOOTP
- Kerberos
- SUNRPC
- MS-RPC
- RADIUS

##### **Connectivity**

- SSH

- Telnet
- VNC
- RTSP
- MS-Media

#### **IM**

- MSN
- Yahoo
- AOL

#### **P2P**

- BitTorrent
- eDonkey 2000
- Gnutella
- WinNY
- eMule
- Kazaa
- AppleJuice

#### **6.1.9 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.

Alcatel-Lucent response: the SafeGuard appliance can base its enforcement on the application, not just the data payload.

- (ii) Circumvention efforts by users ( i.e. port tunneling, proxy servers, fragmented packets, etc).

Alcatel-Lucent response: the SafeGuard appliance can base its enforcement on the application, not just the data payload. Flow based policies can be created to bar access to proxy servers as they become known.

- (iii) Denial-of-service or other attacks against components of the technology.

Alcatel-Lucent response: the SafeGuard appliance uses heuristics to determine DoS attacks and will stop that activity as soon as it is discovered. Working in concert with Alcatel-Lucent switches, we can submit a MAC based ACL or MAC based quarantine VLAN rule to all Alcatel-Lucent switches which would bar traffic from that device.

**6.1.10 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.

Alcatel-Lucent response: Prior to General Availability release, all software is tested thoroughly via our SQA (software quality assurance) procedures. This process normally takes between 6 – 9 weeks. Bugs and feature compliance are fully reported and where possible remedied prior to release.

OmniAccess SafeGuard products (appliance and network management software) is generally available, has been on our price list for over 18 months and has been installed in K-12, Higher Education, Finance and State/Local government accounts throughout the world.

**6.1.11 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.

Alcatel-Lucent response: the following table summarizes our competitive stance:

<b>Competitor</b>	<b>Competitor Strengths (Why choose them?)</b>	<b>Alcatel-Lucent Differentiator (Why choose us?)</b>
Cisco	Market presence in LAN switching Complete end-to-end solution	<ul style="list-style-type: none"> <li>▪ Non-disruptive introduction of advanced NAC functionalities. No modification to the existing LAN / WLAN infrastructure.</li> <li>▪ Integrated solution covered under a single management application. Cisco's equivalent solution requires 3 different types of equipment, 1 Cisco specific Authentication server and 3 different management applications all contributing to a very high Opex.</li> <li>▪ True day zero protection.</li> </ul>

		<p>Cisco Secure Agent was designed to run on end points and abnormal behavior. However, its adoption of the CSA has been very limited and very difficult for those who chose it. Cisco has currently no real day zero offer for the enterprise.</p> <ul style="list-style-type: none"> <li>▪ Price point of the Alcatel-Lucent solution compared to a complete NAC/FW/IPS/Quarantine Cisco Solution.</li> </ul>
HP	OEM of Vernier Authentication appliance (same as Extreme)	<ul style="list-style-type: none"> <li>▪ Less than 1 Gbps of throughput (general CPU appliance)</li> <li>▪ No IPS functionality</li> <li>▪ Basic statistical anomaly detection in XL edge switches</li> </ul>
Nevis networks	Signature based intrusion detection Performance	<ul style="list-style-type: none"> <li>▪ More flexible authentication (covers 802.1x and Microsoft Domain Authentication snooping)</li> <li>▪ More flexible host integrity check with support for both ActiveX and Java</li> <li>▪ More mature product</li> </ul>

### 6.1.12 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).

**Alcatel-Lucent response:** the customer should supply the server for the management software.

### 6.1.13 Comparison with Hypothetical Scenario

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

Alcatel-Lucent response: could not find the referenced hypothetical scenario. However the solution would work as follows:

- User boots up computer and logs in to network. SafeGuard passively sniffs the wire and determines user identity, MAC and IP addresses. Compares user identity to known roles and marries the policies for that role with the user.
- Optional dissolvable agent is downloaded and runs on the computer, reporting the posture of the computer and whether any forbidden applications exist on the machine (optional).
- User violates a policy. SafeGuard can hijack user's session, forcing them to a university authored web page that explains why they are there and what to do about it.
- User remedies problem. SafeGuard let's traffic flow from that application or to that destination.

## 6.2 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.

### 6.2.1 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.

Alcatel-Lucent response: the solution is application identity based. False positives would be very rarely seen, if ever.

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.

Alcatel-Lucent response: the SafeGuard solution can be configured to fail open. On average, 30 microseconds of latency are introduced.

The campus can decide how and who they want violation notifications sent to.

The solution can deny both file and application level access.

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.

Alcatel-Lucent response: programmable ASICs allow for threat detection evolution. This would be delivered via software updates or upgrades and would be routine in applying them.

Currently, Alcatel-Lucent is working on integrating this technology into our LAN switches, however that capability is not forecast to available until 2010. Currently, we are limited to 1 Gbps connectivity. Upon integration with the LAN switch, we will then have the ability to provide a 10 Gbps connection to the core direct from the appliance/switch.

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.

Alcatel-Lucent response: Understood. These capabilities are available, in addition to the ability to require two people to review logs instead of just one.

### 6.2.2 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.

Alcatel-Lucent response: the OmniAccess SafeGuard solution provides all of the above features, including white listing.

### 6.2.3 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.

**Alcatel-Lucent response: the OmniAccess SafeGuard solution operates without regard for VLAN or subnet.**

### 6.2.4 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.

**Alcatel-Lucent response: Understood. The OmniAccess SafeGuard solution supports multiple topologies and designs, does not possess a single point of failure – if the appliance ‘dies’ traffic flows as if the device were not there, can be configured to allow P2P application usage by select individuals (whitelisting) and can have different actions for infringements.**

### 6.2.5 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.

**Alcatel-Lucent response: Understood and comply.**

### 6.2.6 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.

**Alcatel-Lucent response: Understood and comply.**

### 6.2.7 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.

Alcatel-Lucent response: Understood and comply.

### 6.3 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.)

Alcatel-Lucent response: Understood. Patents have been applied for with regard to multi-core inspection.

### 6.4 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.

Alcatel-Lucent response: Alcatel-Lucent (ALU) is the combination of Lucent Technologies and Alcatel SA. These two telecommunications giants merged in December 2006 with the intent of providing their customers with affordable, leading edge solutions. Corporate Headquarters are based in Paris, France, with North American regional headquarters in Murray Hill, NJ and Kanata, ON. ALU has posted 2007 revenues of just under 18 Billion dollars, with over 70,000 employees, and operates in over 130 countries.

Higher Education customers include UCLA, Penn State, Harvard, University of Connecticut, Gordon College, Quinnipiac University, City College of San Francisco and Alamo Community College District.

### 6.5 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.

Alcatel-Lucent response: Demonstration testing is an important consideration when trying to prove the merits of your solution. Alcatel-Lucent fully supports the ability of our customers to acquire solutions, have help in configuration and operation, provide access to technical support and then allow the customer ample time to evaluate. We provide this service at no charge. Usually we conduct evaluations in 30 day increments.

In order to accomplish a credible test (NAC, Visibility, User Access Control, and Threat Control), we would require the following:

OmniAccess SafeGuard 2400 or 1o00 – 1 qty  
OmniVista SafeGuard Manager – 1 qty  
Layer 2 Ethernet Switches (Access Switch) – 2 qty  
Layer 3 Ethernet Switch (Core) – 1 qty  
Active Directory Server – 1 qty

*with the following components:*

- Domain Controller
- Internet Authentication Server (IAS)
- Internet Information Server (IIS)
- FTP Server

Windows XP Systems (to simulate two users: Bob / Alice) – 2 qty

*with the following components:*

- Mozilla FireFox
- QuickTime plugin

Linux System (for threat generation) – 1 qty

**The testbed also requires:**

- Internet Access
- Domain Name Resolution (DNS) server

## 6.6 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.

Alcatel-Lucent response: in order to maintain current software, customers will need to purchase maintenance. The maintenance agreement does not need to be Premium, a simple Basic maintenance agreement will provide the customer with access to all software updates and technical support.

Pricing information is as follows (this is un-discounted pricing):

<i>Model No</i>	<i>Model Description</i>	<i>List Price</i>
OAG-1000-R-A	OmniAccess 1000 SafeGuard. Supports 10 Unpopulated Gigabit SFP cages [4 secure data port pairs + 2 Extensibility Ports]. Ships with the base Authenticated User License (400 users). An Authenticated User License extension can be purchased separately. Supports 2 built-in AC PSUs, 1 out-of-band Ethernet management port. Includes 1 Serial Cable, 2 Rack Mount Ears, 1 Set Screws, 1 Set Anti-Skid Rubber Feet, and 1 Disposable Antistatic Wrist Strap.	\$18,495.00
OAG-2400-R-A	OmniAccess 2400 SafeGuard. Supports 24 Unpopulated Gigabit SFP cages [10 secure data port pairs + 4 Extensibility Ports]. Ships with the base Authenticated User License (1,000 users). An Authenticated User License extension can be purchased separately. Supports 2 built-in AC PSUs, 1 out-of-band Ethernet management port. Includes 1 Serial Cable, 2 Rack Mount Ears, 1 Set Screws, 1 Set Anti-Skid Rubber Feet, and 1 Disposable Antistatic Wrist Strap.	\$28,495.00
OAG-SFP-GIG-LX	OmniAccess SafeGuard 1000Base-LX Gigabit Ethernet optical transceiver (SFP MSA). Supports single mode fiber	\$995.00
OAG-SFP-GIG-SX	OmniAccess SafeGuard 1000Base-SX Gigabit Ethernet optical transceiver (SFP MSA). Supports multimode fiber	\$345.00
OAG-SFP-GIG-T	OmniAccess SafeGuard 1000Base-T Gigabit Ethernet Transceiver (SFP MSA)	\$350.00
OAG-CF512A	Optional 512MB Compact Flash for the OmniAccess SafeGuard platforms	\$400.00
OAG-RM	OmniAccess SafeGuard platforms 19" spare rack mount brackets	\$45.00
OAG-1000-4C8CUG	OAG-1000 Authenticated User License extension (from 400 to 800 authenticated users)	\$5,000.00

OAG-2400-1K2KUG	OAG-2400 Authenticated User License extension (from 1,000 to 2,000 authenticated users)	\$9,000.00
OAG-DA-1C-PL	OmniAccess SafeGuard End point Posture Validation Agent - Campus License for up to 100 concurrent users	\$2,995.00
OAG-DA-1K-PL	OmniAccess SafeGuard End point Posture Validation Agent - Campus License for up to 1000 concurrent users. This license can be used on a single OmniAccess SafeGuard appliance, Across an HA pair, and multiple appliances so long as the following condition is met:- Licenses must be combined to meet or exceed the total number of machines that will be posture checked at that campus.- Total number of Machines must include the number of Employee machines, and contractor and guest machines combined.- This license may be combined with other licenses of different user capacities to accommodate the size of that campus.	\$9,995.00
OAG-DA-2C-PL	OmniAccess SafeGuard End point Posture Validation Agent - Campus License for up to 200 concurrent users	\$4,995.00
OV-OAG-10-25-UG	OmniVista SafeGuard Manager Upgrade License from up to 10 to up to 25 OmniAccess SafeGuard platforms	\$6,000.00
OV-OAG-10-50-UG	OmniVista SafeGuard Manager Upgrade License from up to 10 to up to 50 OmniAccess SafeGuard platforms	\$15,000.00
OV-OAG-25-50-UG	OmniVista SafeGuard Manager Upgrade License from up to 25 to up to 50 OmniAccess SafeGuard platforms	\$9,000.00
OV-OAG-5-10-UG	OmniVista SafeGuard Manager Upgrade License from up to 5 to up to 10 OmniAccess SafeGuard platforms	\$3,000.00
OV-OAG-5-25-UG	OmniVista SafeGuard Manager Upgrade License from up to 5 to up to 25 OmniAccess SafeGuard platforms	\$9,000.00
OV-OAG-5-50-UG	OmniVista SafeGuard Manager Upgrade License from up to 5 to up to 50 OmniAccess SafeGuard platforms	\$18,000.00
OV-OAG-SW-10	OmniVista SafeGuard Manager Software with license to manage up to 10 OmniAccess SafeGuard platforms	\$10,995.00
OV-OAG-SW-25	OmniVista SafeGuard Manager Software with license to manage up to 25 OmniAccess SafeGuard platforms	\$16,995.00
OV-OAG-SW-5	OmniVista SafeGuard Manager Software with license to manage up to 5 OmniAccess SafeGuard platforms	\$7,995.00
OV-OAG-SW-50	OmniVista SafeGuard Manager Software with license to manage up to 50 OmniAccess SafeGuard platforms	\$25,995.00

802745-00	One year - 7X24 phone support for OmniAccess 2400 SafeGuard. Includes e-service web access, software releases and repair and return of hardware to be completed in 10 business days from receipt. Excludes NMS and MSS software. SUPPORTbasic - OAG-2400	\$3,704.00
802746-00	One year - 7X24 phone support for OmniAccess 1000 SafeGuard. Includes e-service web access, software releases and repair and return of hardware to be completed in 10 business days from receipt. Excludes NMS and MSS software. SUPPORTbasic - OAG-1000	\$2,404.00
802747-00	One year hardware support for OmniAccess 2400 SafeGuard. Includes 7X24 phone support, software releases, e-service web access, advanced shipment for next business day arrival of replacement hardware. Excludes NMS and Authentication Services software. SUPPORTplus - OAG-2400	\$4,559.00
802748-00	One year hardware support for OmniAccess 1000 SafeGuard. Includes 7X24 phone support, software releases, e-service web access, advanced shipment for next business day arrival of replacement hardware. Excludes NMS and Authentication Services software. SUPPORTplus - OAG-1000	\$2,959.00
802749-00	One year hardware support for OmniAccess 2400 SafeGuard. Includes 7X24 phone support, software releases, e-service web access, same day 4-hour hardware replacement (labor and parts), 7 days a week, 24 hours a day. Please allow 30 days lead time from receipt of sales order. Excludes NMS and Authentication Services software. SUPPORTtotal - OAG-2400	\$7,124.00
802750-00	One year hardware support for OmniAccess 1000 SafeGuard. Includes 7X24 phone support, software releases, e-service web access, same day 4-hour hardware replacement (labor and parts), 7 days a week, 24 hours a day. Please allow 30 days lead time from receipt of sales order. Excludes NMS and Authentication Services software. SUPPORTtotal - OAG-1000	\$4,624.00
802751-00	One year software support for OAG-DA-1K-PL. Includes maintenance releases, 7X24 phone support and e-service web access. SER-SOFT-OAG-DA-1K-PL	\$1,656.00
802752-00	One year software support for OAG-DA-2C-PL. Includes maintenance releases, 7X24 phone support and e-service web access. SER-SOFT-OAG-DA-2C-PL	\$828.00

802753-00	One year software support for OAG-DA-1C-PL. Includes maintenance releases, 7X24 phone support and e-service web access. SER-SOFT-OAG-DA-1C-PL	\$496.00
802754-00	One year software support for OV-OAG-SW-5. Includes maintenance releases, 7X24 phone support and e-service web access. SER-SOFT-OV-OAG-SW-5	\$960.00
802755-00	One year software support for OV-OAG-SW-10. Includes maintenance releases, 7X24 phone support and e-service web access. SER-SOFT-OV-OAG-SW-10	\$1,320.00
802756-00	One year software support for OV-OAG-SW-25. Includes maintenance releases, 7X24 phone support and e-service web access. SER-SOFT-OV-OAG-SW-25	\$2,040.00
802757-00	One year software support for OV-OAG-SW-50. Includes maintenance releases, 7X24 phone support and e-service web access. SER-SOFT-OV-OAG-SW-50	\$3,120.00

## 6.7 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.

[Alcatel-Lucent response: product brochure attached to this response.](#)

## Conclusion

Alcatel-Lucent believes we can provide the Joint Task Force with the expertise and products to help protect intellectual property. The flexibility of the SafeGuard solution allows campuses to configure enforcement as they see fit, report on what they want, and implement in a non-disruptive manner – regardless of the infrastructure.

We look forward to helping the entertainment and higher education communities achieve their goals.