

**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**

15 MAY 2008

# Contents

<b>1</b>	<b>Introduction.....</b>	<b>3</b>
<b>2</b>	<b>Scope of the Technology Task Force.....</b>	<b>4</b>
<b>3</b>	<b>Objectives of the Request for Information.....</b>	<b>4</b>
<b>4</b>	<b>Background and Information.....</b>	<b>4</b>
	4.1 Problem to be Addressed.....	4
	4.2 The Requirements of Higher Education.....	5
<b>5</b>	<b>Logistics .....</b>	<b>6</b>
<b>6</b>	<b>Submission Requirements.....</b>	<b>6</b>
	6.1 Features of the Technology .....	6
	6.1.1 <i>Network architecture</i> .....	10
	6.1.2 <i>Scalability</i> .....	11
	6.1.3 <i>Protocol identification</i> .....	11
	6.1.4 <i>Granularity of protocols</i> .....	12
	6.1.5 <i>Product Configuration and Installation</i> .....	12
	6.1.6 <i>Content identification</i> .....	14
	6.1.7 <i>Examination of network packets or file content</i> .....	15
	6.1.8 <i>Distribution systems</i> .....	15
	6.1.9 <i>Resilience of the technology to countermeasures</i> .....	15
	6.1.10 <i>Testing and installed base</i> .....	16
	6.1.11 <i>Competitive approaches</i> .....	16
	6.1.12 <i>Third-party components</i> .....	17
	6.1.13 <i>Comparison with Hypothetical Scenario</i> .....	18
	6.2 Performance with respect to the Requirements Described in the 2007 Workshop Report .....	19
	6.2.1 <i>Identifying Infringing Traffic at the Campus Border</i> .....	22
	6.2.2 <i>Responding to Infringing Traffic at the Campus Border</i> .....	23
	6.2.3 <i>Identifying Infringing Traffic Local to the Campus Network</i> .....	24
	6.2.4 <i>Responding to Infringing Traffic Local to the Campus Network</i> .....	25
	6.2.5 <i>Supporting the Campus Judicial System</i> .....	25
	6.2.6 <i>Avoiding Disruption of All Non-infringing Traffic.</i> .....	25

6.2.7	<i>Considerations for Purchase and Operations</i> .....	25
6.3	Intellectual Property .....	26
6.4	Corporate Characteristics and Resources .....	26
6.5	Pilot Testing.....	26
6.6	Commercial Terms .....	27
6.7	Additional Information.....	28
<b>7</b>	<b>Confidentiality</b> .....	<b>28</b>
<b>8</b>	<b>Conflicts of Interest</b> .....	<b>29</b>
<b>9</b>	<b>Readership and Dissemination</b> .....	<b>29</b>
<b>10</b>	<b>Miscellaneous</b> .....	<b>29</b>
10.1	No Obligations.....	29
10.2	Neutrality.....	29

## **1 Introduction**

The Joint Committee of the Higher Education and Entertainment Communities was created in 2002 to discuss and address matters of mutual concern, including the use of university networks for copyright infringement, and to address the problem of unauthorized file sharing on university and college campuses throughout the United States. Since its inception, the Joint Committee has worked to foster cooperation between higher education and the entertainment industry in reducing unauthorized file sharing through educational efforts; developing and enforcing effective and appropriate institutional policies; adopting legal online digital delivery services; and in investigation and use of technologies to assist in network management.

To further these efforts, the Joint Committee’s Technology Task Force is releasing this Request for Information (RFI), seeking information from vendors about their products and their ability to respond to network requirements identified as the result of a technology workshop held in April 2007. Please see the following report for more information on the workshop’s conclusions:  
<http://www.educause.edu/ir/library/pdf/CSD5170.pdf>. The goal of this RFI process is to capture up-to-date information from vendors that reflects their ability to respond to the requirements of the workshop report. It is expected that vendors will also provide information on products currently being marketed that address one or more aspects associated with the technological control of copyright infringement. The results of this RFI process will be shared on the Web and throughout the higher education, vendor, and entertainment communities. It is expected that this effort will aid vendors in reaching potential customer campuses and will help campus leaders to understand the current

landscape of potential solutions and to find particular vendor contacts for their campus needs.

## **2 Scope of the Technology Task Force**

The Technology Task Force (TTF) established by the Joint Committee is comprised of members and staff from both the higher education and entertainment communities, and is charged with the exploration of ways in which technology can reduce unauthorized file sharing on campus networks. The TTF will compile information provided by vendors in response to this RFI and provide a written report to the Joint Committee.

Neither the Task Force, nor the Joint Committee, will recommend or certify any technologies or services. Rather, the purpose of the RFI is to gather knowledge concerning existing technologies and how they may be used to reduce illegal file sharing.

## **3 Objectives of the Request for Information**

The goal of this RFI is to identify and document information on all available technologies that may be used by universities and colleges to address issues of unauthorized distribution of copyrighted material on campus networks. Any company or individual (referred to in this RFI as a “vendor”) is invited to provide this task force with information on currently or soon-to-be available technologies that can address any or all of the issues associated with copyright infringement on campus networks. It is desirable for such technologies to be compatible with the various requirements of college and university environments (as described in section 6.2 below).

It is expected that the Joint Committee will distribute a version of this information to representatives of universities and colleges, some of whom may then elect to run pilot tests on one or more of the technologies.

## **4 Background and Information**

A group of campus networking experts, technology vendors, and entertainment industry representatives convened in Washington, DC on April 19<sup>th</sup> and 20<sup>th</sup>, 2007, to discuss, define and document university requirements for technological solutions that identify, filter, and/or block infringing file transfers on campus networks.

### *4.1 Problem to be Addressed*

A number of requirements were identified during the two-day workshop arising primarily from discussions amongst the higher education participants.

They agreed, for example, that sharing of copyrighted files without legal authority is an unacceptable use of campus network resources. It was agreed as well that higher education can and should support the efforts of rights-holders to enforce their intellectual property rights, though specifically to what extent and by what means would vary from campus to campus based on a broad range of factors and interpretations.

Higher education participants believe that campus networks must remain stable, cost-effective, efficient, and reliable conduits for all legal content and activities. They also

believe technology vendors will find it challenging but not impossible, to meet those requirements and limit infringing file sharing while maintaining the basic goals for the network.

#### *4.2 The Requirements of Higher Education*

The Workshop Report documents the requirements that were identified by the Higher Education participants. Requirements were documented in several areas associated with a campus network. They included:

- Identifying infringing traffic at the campus border
- Responding to infringing traffic at the campus border
- Identifying infringing traffic local to the campus network
- Responding to infringing traffic local to the campus network
- Supporting the campus judicial system
- Avoiding disruption of all non-infringing traffic
- Considerations for purchase and operations

A summary of the requirements is provided below in section 6.2. To review the details of these requirements see the Workshop Report at <http://www.educause.edu/ir/library/pdf/CSD5170.pdf>.

Vendors responding to this RFI should note how their technology addresses or meets the requirements identified in the Workshop Report.

#### *4.3 Issues and Example Approach*

Respondents are invited to provide information regarding both components of solutions and integrated solutions.

For information purposes, an example approach is described below. Respondents should not limit themselves to this hypothetical scenario since it is meant to only represent one potential approach. All technology approaches are welcome to be submitted without any prior preference.

**Example approach:** Higher education attendees at the April, 2007 workshop substantially agreed that one possible approach held promise for widespread adoption because it addressed many of the requirements that had been identified during the two days of discussion. Furthermore, it did so in a way that could be very flexible and adaptable to the needs of the individual campus. A description of the approach and the reasoning behind it may be found at <http://staff.washington.edu/gray/papers/copyright-enforcement.html>. Although this approach appealed to many of the April 2007 workshop attendees, it should not be viewed as the only approach that might work or be acceptable in the broader higher education community. It does, however, provide a guide to how to be sensitive to the desires and requirements of colleges and universities.

## 5 Logistics

Responses to this RFI should be sent by close of business on 15 June 2008 to the Technology Task Force of the Joint Committee of the Higher Education and Entertainment Communities. The representatives of that committee for the purpose of receiving the responses to the RFI are shown below.

Responses should be provided to both Mark Luker and Bruce Block in electronic format in Microsoft Word, Adobe Portable Document Format (PDF), or HTML.

Mark Luker EDUCAUSE 1150 18 <sup>th</sup> St. NW Suite 1010 Washington, D.C. 20036 USA Tel. +1 (202) 872 4200 Fax. +1 (202) 872 4318 Email: mluker@educause.edu	Bruce Block Block & Associates 12512 Palatine Court Potomac, Maryland 20854 USA Tel. +1 (240) 381 8547 Fax. +1 (301) 983 4652 Email: brucejayblock@hotmail.com
---	---

A briefing was scheduled for April 30, 2008 in Los Angeles at UCLA. The purpose of that workshop was to: fully explain the goals of the Joint Committee; present an understanding of the issues associated with unauthorized file sharing on University campuses; and present an understanding of the RFI and respond to vendor questions. If a vendor needs additional information, please submit questions by email to either of the above individuals. Questions submitted by any individual vendor and the answers thereto will be provided to all interested parties. It is anticipated that documentation of the submissions will take place during the four weeks following submittal of the RFI responses. .

## 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.

## Bradford Campus Manager

College, university, and K-12 computer networks are evolving rapidly to give students, faculty, and staff anytime, anywhere access to exploding multi-media content. Supporting PCs, laptops, handhelds, and gaming devices, education networks are extremely vulnerable to disruptions from skilled hackers, rogue users, and accidental intruders.

Bradford Networks' Campus Manager delivers the three key elements of effective network access control – identity management, endpoint compliance and usage policy enforcement – in a single integrated solution.

Designed for educational institutions, Campus Manager's out-of-band architecture leverages existing network and security infrastructures to deliver automated security services without costly infrastructure upgrades.

Campus Manager automatically identifies authorized users and verifies computer and device configuration compliance before granting network access. If users fail to gain access, Campus Manager provides remediation options so non-compliant users can update their systems themselves.

Campus Manager then continuously enforces security policies, records detailed historical data to document network activity, and generates reports for security threat analysis and regulatory compliance.

Additional resources for information on Bradford Campus Manager:

### Product Overview

[http://www.bradfordnetworks.com/board/board.cgi?id=CM\\_Brochures&action=view&qul=29&page=1&go\\_cnt=0](http://www.bradfordnetworks.com/board/board.cgi?id=CM_Brochures&action=view&qul=29&page=1&go_cnt=0)

### Product Datasheet

[http://www.bradfordnetworks.com/board/board.cgi?id=CM\\_Brochures&action=view&qul=49&page=1&go\\_cnt=0](http://www.bradfordnetworks.com/board/board.cgi?id=CM_Brochures&action=view&qul=49&page=1&go_cnt=0)

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.

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.

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.

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.**

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.**

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.

### Network Access Control (NAC)–

Bradford Campus Manager fits into a class of technology best known as Network Access Control, or NAC. A truly innovative and comprehensive NAC solution, Campus Manager delivers an extensive range of capabilities over and above those typically associated with NAC technology. As such, it provides benefits of several of the benefits of other classes of technology listed above, including *device auditing, activity monitoring and reporting, and user management and communication* (including graduated levels of response and actions).

Campus Manager’s primary function is to deliver the three key elements of effective network access control, which include identity management, endpoint compliance and usage policy enforcement. As a result of the innovative approach Bradford has taken, Campus Manager delivers these three “pillars” of NAC and much more.

### **Identity Management**

Campus Manager provides registration, authentication, and role-based access options for precise identity management of users and devices on the network. Registration identifies and tracks each device (by MAC address and/or host name) and each user by user ID. Authentication incorporates user name and password information, and can utilize IEEE 802.1X functionality (with or without supplicants). Campus Manager also integrates with authentication systems and directory services like RADIUS, Active Directory, LDAP, Kerberos, and Sun ONE.

Campus Manager creates an advanced 7-point identity profile linking the user name, user role, device name, MAC address, IP address, physical network access point, and access time for each user and device connection. This provides the ability to effectively monitor, locate, control, and resolve access problems down to the exact point of access of each user and device on the network.

Campus Manager’s unique “GetOut/StayOut” feature lets network managers quickly locate suspicious or “at risk” users or devices and automatically take actions to limit or disable their network connectivity based on pre-defined access policies.

### **Endpoint Compliance**

Campus Manager validates that PCs, laptops, handhelds, and other devices on the network meet the minimum required security standards to keep the network safe and secure. Campus Manager performs registry-based assessments on each endpoint device prior to the device being allowed on the production network.

Endpoint assessment is performed using persistent or dissolvable software agents. The persistent agent is installed on the endpoint device for continuous monitoring, while the dissolvable agent is a run-once executable that is suitable for students' laptops or other devices not owned and managed by the institution.

Persistent and dissolvable agents check and verify the following:

- Operating system type, patch levels, and hotfixes
- Anti-virus applications, engine, and definition version levels
- Anti-spyware applications, engine, and definition version levels
- Prohibited/required applications
- File presence/status
- Process activity
- Endpoint drivers

Devices that fail one or more policy checks can be placed in a secure quarantine VLAN where users can self-remediate without the need for helpdesk intervention. In addition, Campus Manager allows remote validation of devices, further enhancing security and reducing IT staff cycles by allowing users to validate their devices prior to arriving on location.

### **Usage Policy Enforcement**

Many institutions have acceptable use policies for their networks to ensure high performance and availability, and to enable compliance with mandated regulations such as CALEA, FERPA, and GLBA. These policies address bandwidth usage, gaming, illegal file downloading, and P2P applications. Campus Manager provides the tools needed to effectively enforce these policies. Whether Campus Manager is tracking unwanted activities like excessive bandwidth usage, malicious acts, denial of service attacks, or discovering rogue servers and devices, network administrators can quickly identify threats, isolate risks, and take corrective action.

When the corrective action is user or device isolation, Campus Manager simultaneously supports four isolation methods (802.1X, MAC-based RADIUS authentication, DHCP, and VLAN steering via SNMP/CLI) while providing a consistent user experience. During device isolation, devices are automatically prevented from connecting to both wired and wireless ports.

Campus Manager also integrates with a wide range of in-line, deep packet inspection solutions such as intrusion detection/prevention systems, firewalls, web content filters, and traffic shapers to identify and act on threats as they occur. Alarms and traps from deep packet devices trigger Campus Manager to initiate appropriate notification, problem isolation, and corrective actions at the offender's point of network access.

Campus Manager correlates user identity to network identity, so no matter how many different machines are used to access the network and no matter if a user has a single or multiple IP or MAC addresses, Campus Manager provides a logical representation of users on the network and prevents users from changing their network identities in order to bypass network access and usage policies.

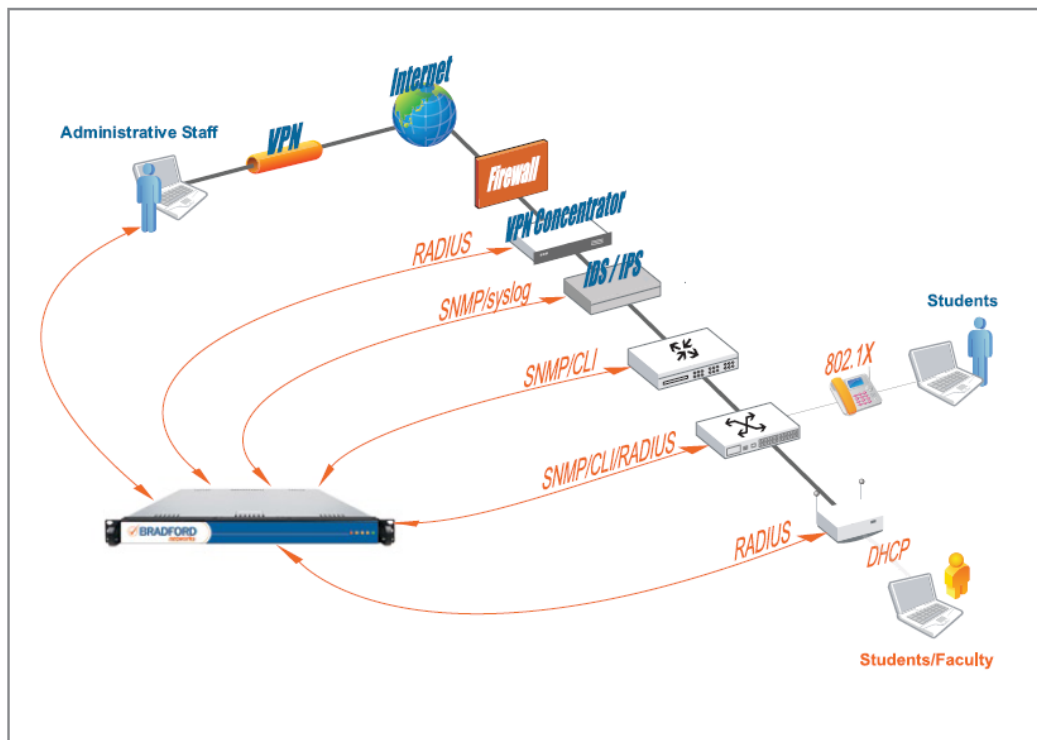
### 6.1.1 Network architecture

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

#### Out-of-Band with Edge Enforcement

Campus Manager is an appliance-based solution in which appliances are deployed **out-of-band** from production network traffic such that they do not introduce potential performance bottlenecks or single points of failure in the network.

Campus Manager appliances are typically deployed in data centers for ease of management and physical access to the appliances, but they can be deployed *anywhere* in the network as long as IP connectivity to network devices is provided.



**Bradford Campus Manager's Out-of-Band Architecture**

Campus Manager's **out-of-band** architecture utilizes current network configuration and traffic data from switches, wireless access points, and other infrastructure equipment to create a logical representation of the network. Campus Manager then correlates network infrastructure data with user identity information. This includes extensive automated network device discovery using a protocol-independent process (SNMP, CLI over SSH, CLI over Telnet) to access each device in the network and identify its unique security features, such as Alcatel's group mobility, or Cisco's private isolated VLANs.

When unregistered/unauthorized users or devices attempt to access the network, or when other policy violations are detected, Campus Manager determines the policy-based actions needed and executes corrective action via CLI, SNMP, or RADIUS

commands to the corresponding network equipment to address the threat at the point of network access. This is what is referred to as **edge enforcement**, as policy enforcement occurs at the edge of the network (e.g., switch port or wireless access point).

Additional resources for information on Campus Manager's out-of-band architecture:

Whitepaper: Selecting An Approach For NAC Enforcement: Five Key Issues

[http://www.bradfordnetworks.com/board/board.cgi?id=CM\\_WhitePaper&action=view&gul=52&page=1&go\\_cnt=0](http://www.bradfordnetworks.com/board/board.cgi?id=CM_WhitePaper&action=view&gul=52&page=1&go_cnt=0)

Whitepaper: Out-of-Band Architecture Enforces NAC at the Network Edge

[http://www.bradfordnetworks.com/board/board.cgi?id=CM\\_WhitePaper&action=view&gul=51&page=1&go\\_cnt=0](http://www.bradfordnetworks.com/board/board.cgi?id=CM_WhitePaper&action=view&gul=51&page=1&go_cnt=0)

Additional Whitepapers:

[http://www.bradfordnetworks.com/board/board.cgi?id=CM\\_WhitePaper](http://www.bradfordnetworks.com/board/board.cgi?id=CM_WhitePaper)

### 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.

Campus Manager's high performance architecture delivers unmatched scalability and flexible, effective access control in any environment. The Campus Manager family includes a range of Network Sentry appliance platforms, allowing solutions to be tailored based on the number of concurrent users, the number of network devices, authentication methods used, and access policy complexity. A single pair of Network Sentry appliances provides centrally-managed network access control for environments of up to 12,000 concurrent network connections. Additional appliances can be added to scale to environments of tens of thousands of connections.

Due to Campus Manager's innovative out-of-band architecture, *production network traffic does not pass through* Network Sentry appliances, so the appliances do not introduce potential performance bottlenecks or single points of failure in the network.

Much of the "work" done by Network Sentry appliances is done *before* active network connections are established. User and device identity are verified and device security posture and policy compliance is assessed prior to allowing network access. Once these processes occur and appropriate network access is enabled for a user/device, Network Sentry appliances do not impede traffic flow in any way – so there is no performance degradation or network latency.

### 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.

As Campus Manager is implemented *out-of-band* from the flow of network traffic, it does not directly analyze traffic or identify particular protocols in use. However, Campus Manager has the ability to integrate with 3<sup>rd</sup>-party devices that do feature in-line traffic analysis capabilities. The benefit of integrating with these devices is that Campus

Manager can enhance their security functionality by taking responsive actions at the point of access to the network (refer to previous discussion of “edge enforcement”).

For example, if a 3<sup>rd</sup>-party security device in the network detects inappropriate traffic or unauthorized protocols in use and communicates the source (IP) address for this traffic to Campus Manager, Campus Manager can in turn resolve the IP address with an associated device (MAC address), user, and location (point of access). Campus Manager can then take appropriate responsive action at the point of access (switch port or wireless access point) – such as quarantining the offending device or disconnecting it from the network.

#### 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.”

As discussed in response to 6.1.3 above, Campus Manager is implemented *out-of-band* from the flow of network traffic and does not directly analyze traffic or identify particular protocols in use.

Alternatively, using comprehensive endpoint assessment capabilities, Campus Manager is able to detect any/all unauthorized applications installed on endpoint devices such as PC’s and laptops, and can take responsive actions to limit or prevent network access *before* these endpoint devices are even able to transmit or receive traffic on the network.

In addition unauthorized applications, Campus Manager is also able to detect active processes, file types, specific filenames, and other things including: operating system type, patches, and hotfixes; anti-virus applications and definitions version; anti-spyware applications and definitions version; and more.

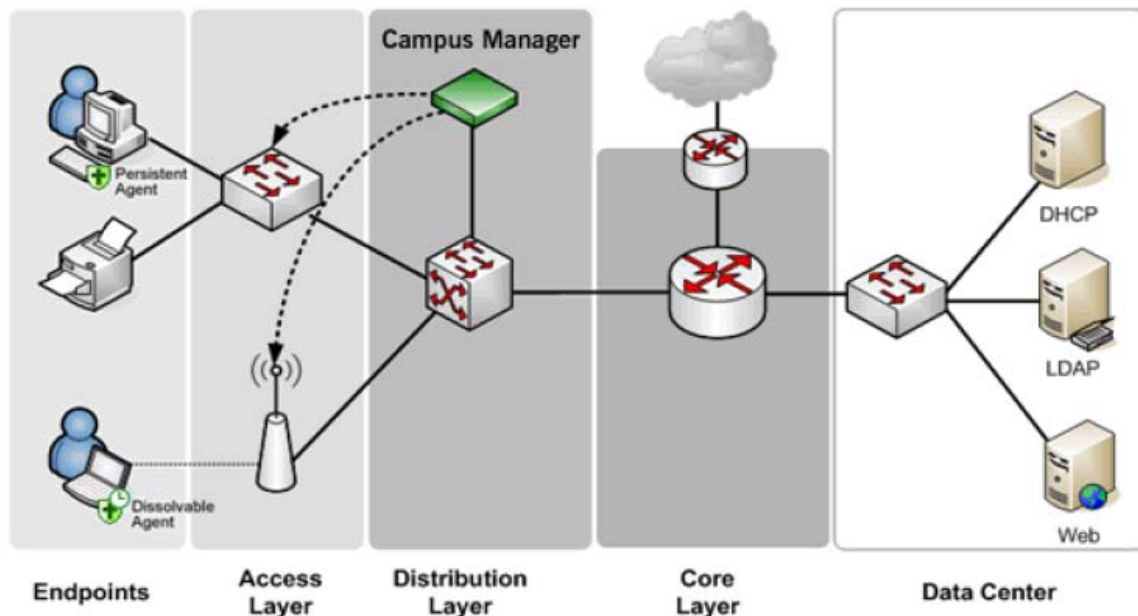
Campus Manager can also provide continuous monitoring of endpoint devices for ongoing policy enforcement after network connectivity is established. For example, if unauthorized applications or files are downloaded or installed at some time after a device is allowed access to the network, Campus Manager is able to detect this and can take appropriate responsive actions automatically.

Response actions may include notifying the user of the policy violation, notifying security and/or network administrators of the policy violation, or limiting or disabling network access, among other potential actions. Response actions can be customized as required by the organization.

#### 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.

Campus Manager consists of hardware appliances installed in the network and optional software agents that are run on endpoint devices using Windows, Mac OS, or Linux operating systems.



### Deployment of Bradford Campus Manager

Campus Manager *Network Sentry* appliances are connected to the network via two physical Ethernet interfaces. One interface provides management and configuration access to the Network Sentry appliance. The second interface allows the appliance to communicate with network and security infrastructure devices on the network, such as switches, routers, wireless access points and/or controllers, VPN concentrators, firewalls, and other devices.

As Campus Manager leverages the entire network infrastructure for enforcement of security policy, its implementation involves integration with a number of other products and processes in the network environment. For example, integration with network infrastructure devices involves configuration of such things as SNMP community strings and/or other means of establishing secure communications between these devices and Network Sentry appliances. The ability to “quarantine”, or isolate, endpoint devices that violate network usage policy is typically achieved with the use of Virtual LANs (VLANs); as such, there is some configuration of VLANs required on the wired and/or wireless network infrastructure.

Integration with existing authentication and directory services such as eDirectory, Active Directory, and LDAP-based services allows Campus Manager to leverage those systems for verification of user identity and group/role membership such that access policies can be enforced based on identity and/or role (among other factors).

Each implementation of Campus Manager is unique in many ways, as security policies and associated policy enforcement actions will vary from one organization to another. Bradford Networks has a number of highly skilled and experienced engineers on staff who work directly with our customers and lead the installation and implementation of Campus Manager. Generally, installation and implementation work is completed in 1 to 5

days, depending on factors such as the size of the network environment and the complexity of the security policies to be implemented and tested.

Installation and implementation of Campus Manager requires little to no downtime on the network. Out-of-band Network Sentry appliances are non-intrusive and are connected to the network and configured without requiring any network downtime. Configuration changes to network infrastructure devices may in some cases (depending on vendor and model) require rebooting or resetting those devices, which can introduce brief periods of downtime for individual network segments.

Light-weight software agents are included with Campus Manager for endpoint devices using Windows, Mac OS, and Linux operating systems. The use of these agents is optional, but recommended in order to achieve the maximum benefits of the Campus Manager NAC solution. Bradford offers both *persistent* and *dissolvable* agents with Campus Manager. Persistent agents are installed on endpoint devices and run “in the background” with no user setup or maintenance required. Dissolvable agents are downloaded and run “on-demand” by users and then automatically deleted from endpoint devices after completing all compliance checks required by the organization.

Both agent types, persistent and dissolvable, perform the same level of compliance checks. The key differences are as follow. Persistent agents are installed only once, are virtually transparent to the user after installation, and can provide continuous device monitoring after installation. Dissolvable agents are downloaded and run “on-demand” (frequency is determined by the organization), and as such do not provide continuous monitoring capabilities.

#### 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 vender should indicate what information, if any, is captured and reported for further analysis and actions.

Software agents (discussed in 6.1.5 above) included with Campus Manager allow it to identify a wide range of things on endpoint devices, including: operating system type, patches, and hotfixes; anti-virus and anti-spyware applications and definitions versions; required and prohibited applications, processes, file types, filenames, and more. In addition, custom registry scans can be performed to enable highly-customizable endpoint device assessment. External content databases are not utilized, as all policy configuration details and endpoint checks to be performed are maintained within the Network Sentry appliances.

Campus Manager records and archives comprehensive profile and activity data for every user and device that accesses the network, including connection logs, scan results, and much more. This critical data lets security and network managers analyze user activity patterns, identify emerging trends, and document individual user actions for policy enforcement and regulatory compliance reporting to satisfy CALEA, FERPA, and GLBA requirements. Standard reports include registrations, registration failures, scan results, and connection logs and can be scheduled or created on an ad-hoc basis. If custom

reports are needed, a data definition language (DDL) for the reporting database has been published by Bradford Networks to make the data accessible to external reporting tools like Crystal Reports.

#### *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).

As discussed in previous sections, Campus Manager is implemented *out-of-band* from the flow of network traffic and does not directly analyze traffic or examine / open packets or file content on 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.

As discussed in previous sections, Campus Manager is implemented *out-of-band* from the flow of network traffic and does not directly analyze traffic. As such, it functions independent of the particular distribution systems/protocols in use.

#### *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.

As Campus Manager does not directly analyze network traffic, it functions independent of file compression, data encryption, etc.

Campus Manager can detect the *presence* of file sharing software on endpoint devices before and/or after network access is established, and can take appropriate actions in response to illegal / unauthorized software being detected. If such software is found on an endpoint device before or after network access is granted, Campus Manager can take a range of response actions, including:

- Notify the user and/or network or security administrator of the policy violation
- Restrict network access (e.g., disable internet connectivity, rate limit traffic, etc.)
- Deny network access (or disable network access if already connected)

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

Same as response to (i) above.

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

#### *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.

#### **Testing**

Discussion of specific testing procedures employed by Bradford Networks requires a non-disclosure agreement (NDA) as this is considered to be sensitive information for competitive reasons. Every product release is subjected to rigorous internal testing for quality assurance. Bradford also employs extensive “beta” deployments with select customers in order to test new releases in “real-world” network environments and to solicit input/feedback from customers who are actively using the technology.

#### **Case Studies / Real-World Deployments**

Numerous case studies are available on Bradford’s website, depicting how Campus Manager applies in real environments at educational institutions worldwide:

[http://www.bradfordnetworks.com/board/board.cgi?id=CM\\_CaseStudy](http://www.bradfordnetworks.com/board/board.cgi?id=CM_CaseStudy)

#### **Installed Base**

Bradford Networks has been shipping its NAC technology commercially to educational institutions since 2002. Well over 400 customers worldwide use Bradford’s products to secure over 1 million students, faculty, staff and other users on their networks.

Bradford is currently shipping its fourth major software release (Version 4.0) for Campus Manager which features significant enhancements over previous versions of software. Customers using previous versions are able to upgrade their existing systems at no additional cost as long as they have a current maintenance support contract.

#### **Features & Specifications**

Details of features, specifications, and ordering information for Campus Manager can be found in the product datasheet available on Bradford’s website:

[http://www.bradfordnetworks.com/board/board.cgi?id=CM\\_Brochures&action=view&qul=49&page=1&qo\\_cnt=0](http://www.bradfordnetworks.com/board/board.cgi?id=CM_Brochures&action=view&qul=49&page=1&qo_cnt=0)

#### *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.

### **Bradford Advantage: Out-of-Band Architecture with Edge Enforcement**

Bradford Networks offers the only appliance-based NAC solution in which appliances are deployed fully **out-of-band** from production network traffic in all network environments. Bradford's solution functions out-of-band in both wired and wireless LANs, and in environments using network infrastructure equipment from virtually any vendor.

Bradford's out-of-band architecture is superior as it enables greater flexibility, scalability, and security, and does not introduce potential performance bottlenecks or single points of failure in the network.

Further, Bradford's architecture leverages the network infrastructure for enforcement of access policy, such that enforcement occurs at the point of access (the network *edge*). As discussed in previous sections, **edge enforcement** is highly secure and effective, as it stops at-risk or out-of-compliance users and devices *before* they can transmit traffic on the network.

### **The Competition: "In-line" or "Hybrid" Approaches**

Many competing NAC solutions employ "in-line" (or "in-band") technology which requires all network traffic to pass through a standalone appliance for inspection in much the same way that a firewall or IPS does. In-line NAC solutions have several drawbacks:

- poor flexibility: the need for in-line appliances to see all network traffic dictates where appliances can be installed in the network
- poor scalability: the need to see and process all network traffic means that a single appliance can typically handle only a relatively small network environment; therefore numerous appliances are required in large environments
- low network performance: because in-line appliances need to see and process all network traffic, they become performance "bottlenecks" (or congestion points) in the network and can degrade network performance – both in terms of throughput and latency
- low network reliability / availability: because all network traffic must pass through an in-line appliance, the appliance becomes a single-point-of-failure for the network segments it serves; should the appliance fail, network traffic may cease
- high management/maintenance burden: the need to deploy numerous in-line appliances in large networks increases the deployment complexity and results in a greater burden on network and/or security staff to deploy, manage, and maintain an increasing number of appliances
- high acquisition costs & operational costs: the need to deploy numerous in-line appliances in large networks increases acquisition costs (more hardware to buy; more expensive support contracts) as well as ongoing operational costs (more hardware to deploy, manage, and maintain)
- low security: in-line appliances are typically deployed further inside the network (at traffic aggregation points in the distribution layer or core layer) and they either "filter" or "forward" network traffic at that point; this is far less secure than **edge enforcement** solutions (discussed above and in previous sections)

Other competing NAC solutions employ “hybrid” approaches in which out-of-band appliances are deployed in some environments and in-band appliances are deployed in others. Hybrid solutions have the same drawbacks as in-line solutions, since in-line appliances are part of these solutions (and often a large part). Cost and complexity are even greater drawbacks for hybrid solutions, as the mix of approaches leads to even more hardware to buy and more hardware to deploy, manage, and maintain).

### **Architecture Comparisons**

An excellent resource for understanding the different NAC architectures discussed above is available on Bradford Networks’ website. It is a whitepaper written by Joel Snyder, a leading independent analyst with extensive knowledge and experience pertaining to NAC and other security technologies.

Whitepaper: Selecting An Approach For NAC Enforcement: Five Key Issues

[http://www.bradfordnetworks.com/board/board.cgi?id=CM\\_WhitePaper&action=view&qul=52&page=1&go\\_cnt=0](http://www.bradfordnetworks.com/board/board.cgi?id=CM_WhitePaper&action=view&qul=52&page=1&go_cnt=0)

### **Industry Recognition**

Bradford Networks is also recognized as a leader and innovator in the market for NAC solutions by leading analysts including Gartner, and by leading industry publications including SC Magazine.

- Bradford Networks rated "Positive" in Gartner’s MarketScope for NAC 2008
- Bradford Networks Named SC Magazine Innovator of the Year 2007 for NAC

These and other positive reviews are available on Bradford Networks’ website:

<http://www.bradfordnetworks.com/index.html>

<http://www.bradfordnetworks.com/news/news.html>

#### *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).

Campus Manager *requires* no third-party components to function, but does allow integration with a number of other components in the network environment to enhance campus-wide security and policy enforcement capabilities.

For example, integration with network infrastructure devices such as switches, wireless access points and controllers, VPN concentrators and other devices allows Campus Manager to extend policy enforcement and access control capabilities right to the point of network access (at the network *edge*).

Integration with existing authentication and directory services such as eDirectory, Active Directory, and LDAP-based services allows Campus Manager to leverage those systems for verification of user identity and group/role membership such that access policies can be enforced based on identity and/or role (among other factors).

Further, integration with third-party security devices that perform in-line traffic analysis (such as IDS, IPS and other systems) allows Campus Manager to enhance their security functionality by taking responsive actions at the point of access to the network (refer to previous discussion of “edge enforcement”).

### 6.1.13 Comparison with Hypothetical Scenario

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

Campus Manager fits into the category of “technical policy enforcement strategies” discussed in *Issues and Example Approaches* – section 4.3 of this document and the associated information referenced there (<http://staff.washington.edu/gray/papers/copyright-enforcement.html>).

In particular, Campus Manager aligns best with the “second approach” discussed:

- a component to map available information from the above (typically an IP address --possibly dynamic-- and a reliable timestamp) into a user identity.*
- a component to take action, e.g. notification or blocking.*

Unique functionality within Campus Manager allows organizations to establish a detailed 7-point identity profile associated with all users and devices on the network using information including user name; user role; device name; MAC address; IP address; network access point; time. The combination of any or all of these details can be used in assessing user and device compliance with network usage policies, as well as actively enforcing appropriate policy compliance.

The discussion of technical approaches referenced in section 4.3 presents the following perceived challenges with such approaches:

- many sensors in many places in the institutions network (widely perceived as impractical).*
- sensors placed at institutional borders, which need to accommodate very high-speed network links, and which will not see local/intra-institutional traffic (much less, intra-subnet traffic).*

Contrary to the perceived challenges of the two items above, Campus Manager employs an innovative architecture that minimizes or eliminates these concerns:

- Campus Manager’s highly-scalable out-of-band architecture minimizes the number of hardware appliances that need to be deployed in the institution’s network. A pair of *Network Sentry* appliances provides centrally-managed network access control for environments of up to 12,000 concurrent network connections. Additional appliances can be added to scale to tens of thousands of connections.
- Campus Manager *Network Sentry* appliances are not required to be placed at institutional borders or “in-line” with network traffic, so they do not impede network performance or introduce potential points of failure in the network topology.

Further, Campus Manager *Network Sentry* appliances operate **out-of-band** (as detailed in previous sections) and can be placed anywhere in the network, while still providing effective network-wide access control. As the appliances function without having to actively “see” or “inspect” actual network traffic flows, they have the advantage of working even when traffic flows are encrypted, and regardless of network topology.

The discussion of technical approaches referenced in section 4.3 also presents a number of concerns and constraints with potential “magic box” technology approaches including *philosophical, legal, cost/benefit, and operational* considerations.

While the first two are non-technical considerations, Campus Manager goes a long way in terms of addressing concerns in the latter two – *cost/benefit* (ROI) and *operational* considerations

*Cost/Benefit concerns (questionable ROI)*

- *a. Concern about deployment costs, which in large schools could be huge if intra-LAN traffic needs to be monitored.*

Campus Manager’s highly-scalable **out-of-band** architecture minimizes the number of hardware appliances that need to be deployed, so deployment costs are far lower than with other solutions that require “in-line” monitoring of high volumes of network traffic.

- *b. Concern about administrative costs associated with operations and adjudication.*

Campus Manager minimizes administrative costs by (a) requiring fewer hardware appliances to be deployed and managed, (b) allowing appliances to be physically located anywhere in the network for ease of management, and (c) automating network access control functions that otherwise can be very labor-intensive for IT staff.

- *c. Whack-a-mole phenomenon, which tends to significantly limit the lifetime of any technical solution.*

Campus Manager is highly customizable and can be easily adapted to address new and emerging security threats and/or “innovative” attempts by users to bypass security measures.

- *d. Encryption, which makes deep packet inspection impossible, thus making \*network\* level identification moot (although it may not preclude \*application\* level identification from the “edge” of the network.)*

As Campus Manager does not directly analyze network traffic, it functions independent of file compression, data encryption, etc. Campus Manager detects the *presence* of file sharing software (or other unauthorized/non-compliant applications) on endpoint devices before and/or after network access is established, and can take appropriate enforcement actions in response to the software being detected. Traffic encryption does not impede this functionality in any way.

- *e. Device-to-device sharing via ad hoc networking is a growing concern for rights holders, but is not a problem higher-ed can solve via technical means.*

Campus Manager also has the ability to detect specific file types, file names, active system processes and other things on endpoint devices that can be strong evidence of unauthorized file sharing activity, and can take appropriate enforcement actions in

response to what is detected – such as warning the user, notifying an administrator, or automatically limiting or disabling network access.

*Operational concerns ("Messing up the network")*

- *a. Performance: few "traffic disruption appliances" can cope with the performance requirements often found within research universities (e.g. uncompressed HD videoconferencing).*

Campus Manager's **out-of-band** architecture allows it to enable network-wide access control and policy enforcement without needing to be "in-line" with network traffic. As such, it does not impede network performance or introduce potential points of failure.

- *b. MTTG --Mean Time To Glitch: unintended collateral damage, or even intentional consequences that lead to complaint calls to the Network Operations Center (NOC).*

Campus Manager's enforcement actions are fully customizable by each institution and can be implemented in ways that will minimize potential for such "glitches".

In fact, Campus Manager effectively *automates* network access control functions that otherwise can be very labor-intensive for IT staff. Many of Bradford's customers indicate that Campus Manager significantly *reduces* their operational burden and *reduces* calls/requests received by their NOC and/or Help Desk staff.

For example, after implementing Campus Manager, Columbia University Medical Center in New York documented a **66% reduction in Help Desk calls** associated with users registering devices and logging onto the network. A full case study for Columbia's implementation of Campus Manager can be accessed on Bradford's website:

[http://www.bradfordnetworks.com/board/board.cgi?id=CM\\_CaseStudy&action=view&gul=54&page=1&go\\_cnt=0](http://www.bradfordnetworks.com/board/board.cgi?id=CM_CaseStudy&action=view&gul=54&page=1&go_cnt=0)

- *c. MTTD --Mean Time to Diagnosis: some content monitoring/blocking designs make it difficult to know what has happened or diagnose the problem when a customer calls the NOC... the user experience might be similar to that resulting from other potential network faults.*

As detailed in previous sections, Campus Manager records and archives comprehensive profile and activity data for every user and device that accesses the network, including connection logs, compliance scan results, and much more. This data lets security and network managers analyze activities and diagnose issues more easily if users call with questions or complaints. More importantly, logging and reporting capabilities provide a vast amount of historical data that is useful to identify emerging trends, document individual user actions for policy enforcement and regulatory compliance reporting to satisfy CALEA, FERPA, GLBA and other requirements.

- *d. Violating "Principle of Least Surprise" --policy enforcement points that disrupt network traffic should tell end-users what they are doing and why their action may be failing.*

Policy enforcement actions taken by Campus Manager are highly-configurable and can include simply notifying the user of the policy violation, notifying security and/or network administrators of the policy violation, or limiting or disabling network access, among other potential actions.

In cases where actions are taken to limit or disable network access, Campus Manager allows a number of ways to inform end-users about policy violations that occurred, as well as corrective actions the users themselves can take to remediate the situation and regain full network access without having to involve NOC or Help Desk staff.

For example, users can be directed to a “captive portal” (web page) providing detailed information as well as links to appropriate instructions and/or remediation resources.

- *e. Impact on innocents: our residence halls have some non-students in them (sometimes spouses, sometimes staff, sometimes others), and technical constraints to inhibit copyright infringement by the target class might unreasonably constrain (non-infringing) activities of others (e.g. at UWashingon our “no servers in dorms” policy enforcement via ACLs is problematic for some who need certain protocols to work a certain way for access to their employer’s network).*

Campus Manager enables customizable *role-based* access control policies which allow institutions to enforce different policies based on a number of important criteria including user name, user role, device name, MAC address, IP address, physical network access point, and access time for each user and device connection.

Using this 7-point identity profile (discussed in previous sections), a combination of any or all of these details can be used in determining appropriate network usage policy. For example, different access policies can be defined and actively enforced for students, faculty, staff, and other users.

## 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.

As discussed previously, Campus Manager’s **out-of-band** architecture allows it to enable network-wide access control and policy enforcement without needing to be “in-line” with network traffic. As such, it does not impede network performance or introduce potential points of failure.

Much of the “work” done by the appliances is done *before* active network connections are established. User and device identity are verified and device security posture and policy compliance is assessed prior to allowing network access. Once these processes occur and appropriate network access is enabled for a user/device, *Network Sentry* appliances do not impede traffic flow in any way – so there is no performance degradation or network latency.

### 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.

Campus Manager's out-of-band architecture is not susceptible to the *false positives* often associated with "in-line" devices that intercept and analyze network traffic. Further, it can be configured to allow critical traffic from specific network devices and/or users.

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.

Campus Manager integrates cleanly with existing campus networks and is capable of "failing open" such that network traffic continues to flow in the case of a system failure. Further, Campus Manager appliances are available with redundant hardware features such as redundant power supplies and disk drives, and appliances can be deployed in "high availability" configurations in which primary and secondary appliances provide enhanced fail-safe protection.

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.

Campus Manager is highly customizable and can be easily adapted to address new and emerging security threats and/or "innovative" attempts by users to bypass security measures. Updates to the system are able to be applied automatically, and major software upgrades can be installed remotely to further enhance product functionality. Campus Manager's out-of-band architecture allows it to function largely independent of network speed/bandwidth (e.g., 1-10-100 Gbps).

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.

Campus Manager logs comprehensive profile and activity data for every user and device that accesses the network, including connection logs, scan results, and much more. Log data is able to be automatically archived on the Campus Manager appliance, and can be exported to other devices for long-term, secure storage.

Standard reports can be generated that include registrations, registration failures, scan results, and connection logs and can be scheduled or created on an ad-hoc basis. For

custom reporting, a data definition language (DDL) for the reporting database has been published by Bradford Networks to make the data accessible to external reporting tools like Crystal Reports.

### 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.

As discussed previously, when policy violations are detected by Campus Manager the system determines appropriate policy-based actions needed and executes corrective action via CLI, SNMP, or RADIUS commands to the corresponding network equipment to address the threat at the point of network access. This is what is referred to as **edge enforcement**, as policy enforcement occurs at the edge of the network (e.g., switch port or wireless access point).

Additionally, response actions may include notifying the user of the policy violation, notifying security and/or network administrators of the policy violation, or limiting or disabling network access, among other potential actions. Response actions can be customized as required by the organization, including the ability to define “white lists” of users and/or devices that will not be blocked from the network.

Campus Manager also has the ability to integrate with third-party devices that feature in-line traffic analysis capabilities, and to enhance their security functionality by taking responsive actions at the point of access to the network (refer to previous discussions of “edge enforcement”).

For example, if a 3<sup>rd</sup>-party security device in the network detects inappropriate traffic or unauthorized protocols in use and communicates the source (IP) address for this traffic to Campus Manager, Campus Manager can in turn resolve the IP address with an associated device (MAC address), user, and location (point of access). Campus Manager can then take appropriate responsive action at the point of access (switch port or wireless access point) – such as quarantining the offending device or disconnecting it from the network.

### 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.

Campus Manager provides the extensive *identity management* and *endpoint compliance* functions discussed previously in wired and wireless LAN environments, as well as for VPN remote access connections. User and device identification and endpoint compliance assessment can be enabled network-wide for all users and devices on all

network segments/subnets, or can be isolated to specific segments – or even to individual users or devices – depending on the requirements of the institution.

#### 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.

Campus Manager provides the extensive *usage policy enforcement* functions discussed previously in wired and wireless LAN environments, as well as for VPN remote access connections. Policy enforcement can be enabled network-wide for all users and devices on all network segments/subnets, or enforcement can be isolated to specific segments – or even to individual users or devices – depending on the requirements of the institution.

#### 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.

As detailed in previous sections, Campus Manager records and archives comprehensive profile and activity data for every user and device that accesses the network, including connection logs, compliance scan results, and more. This data lets security and network managers analyze activities and diagnose issues, and provides a vast amount of historical data that can be used to document individual user and/or device actions for policy enforcement and regulatory compliance reporting. Additionally, automated notifications can be configured to alert security and/or network administrators of policy violations.

#### 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.

Campus Manager enables fully-customizable access control and policy enforcement, such that the institution can *pre-define* all user and device policies and configure the appropriate enforcement actions to be taken in cases where policy violations occur. The flow of non-infringing traffic is not impeded as Campus Manager is deployed out-of-band from network traffic.

### 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.

Once implemented, Campus Manager functions very predictably and automatically manages and enforces network usage policy and access control for all users and devices (as defined by network and/or security administrator during implementation).

Operation of the solution is virtually transparent to the majority of users/devices (e.g., those in compliance with network usage policies). As outlined in previous sections, Campus manager features extensive logging/auditing capabilities and is highly scalable to meet the needs of even the largest institutions in a cost-effective manner.

Acquisition costs for hardware appliances, software licenses, services and ongoing maintenance (support) contracts for Campus Manager are very straightforward and predictable. Campus Manager solutions involve the purchase of one or more hardware appliances, user licenses, installation/implementation services, and annual maintenance contracts.

### 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.**)

Bradford's network access control architecture is currently patent-pending.

### 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.

Bradford Networks is dedicated to solving the security challenges facing enterprise establishments, educational institutions, and government organizations by developing innovative network access control (NAC) solutions for wired, wireless and VPN networks that deliver automated security services leveraging existing network infrastructures and investments.

Founded in 1999, Bradford Networks is privately-held and headquartered in Concord, NH, USA. Bradford recently received its second round (Series B) of funding with an investment of \$8 million received. This adds to \$2 million received in an earlier round of funding in 2006. Detailed information on Bradford's lead investors and funding received to date is available on our website:

Investors: <http://www.bradfordnetworks.com/company/investors.html>

Series B Funding: <http://www.bradfordnetworks.com/news/media060408.html>

Series A Funding <http://www.bradfordnetworks.com/news/media082106.html>

Bradford currently employs 60 full-time personnel and plans to expand to approximately 100 employees over the next 12 months, as the company continues to expand its operations.

Bradford's proven NAC solutions have been commercially available since 2002, and current customers include over 400 education institutions and enterprises in the U.S., UK, and other regions.

Bradford's Campus Manager NAC solution currently secures over 1 million students, faculty, staff and other users at education institutions worldwide, with individual deployments scaling to over 40,000 users on a single campus network.

## 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.

Bradford Networks offers a flexible range of options for institutions to access *real-world* implementations of its Campus Manager product, including the ability to conduct on-site product evaluations.

To begin with, Bradford is able to provide numerous references with names and contact information of institutions worldwide that are currently using Campus Manager. Many of these customers are happy to show other prospective customers how they use the product and to discuss their implementation in detail.

For those institutions further along the path toward implementing a NAC solution, Bradford Networks offers a unique Try-&-Buy Program providing the ability to purchase

and implement Campus Manager with no risk, by allowing customers to return the product if it fails to meet their expectations within the first 30-days after deploying it.

In select cases, Bradford also offers free product evaluation in which Campus Manager can be deployed and tested on-site.

## 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.**

Campus Manager is sold as an appliance-based solution which requires one-time purchase of the following:

- one or more Network Sentry hardware appliances
- user-based software licenses
- installation/implementation services
- one year of maintenance service (renewable annually thereafter)

Recurring costs for annual maintenance contracts include comprehensive technical support and hardware replacement options, as well as software updates and new releases. There are no other recurring costs paid to Bradford Networks by the customer.

## 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.

Additional information about Campus Manager and Bradford Networks is available on our website at <http://www.bradfordnetworks.com>.

## 7 Confidentiality

This RFI solicits detailed information including information about the vendor's intellectual property. The vendor, in response to this RFI, **should not provide information that requires the protection of a nondisclosure agreement.**

It is anticipated that an understanding of the capabilities of vendor technologies, gleaned from the response to this RFI, will be communicated to organizations affiliated with the Joint Committee of the Higher Education and Entertainment Communities. The vendors may or may not be given the opportunity to review and comment upon the documentation of **its individual technologies** prior to the release of such documentation, so the vendors' response to this RFI should be as complete as possible. Material that is considered proprietary or confidential can be referred to, but not included in the vendor's response to this RFI.

## **8 Conflicts of Interest**

The vendor should disclose any potential or existing conflict of interest that it may have in either its response to this RFI or in the conduct of pilot testing at campuses that elect to participate in such tests. Conflicts of interest should also be noted with respect to any other products or services that may be required in order to deploy the vendor's technology for this project.

## **9 Readership and Dissemination**

The results of documenting the responses to this RFI will be reported by the Technology Task Force to the Joint Committee of the Higher Education and Entertainment Communities. The committee will share the information more widely in the form of a knowledge base. **It cannot be guaranteed that the information in the knowledge base concerning the technology responses to this RFI will be limited to those parties.**

## **10 Miscellaneous**

### *10.1 No Obligations*

The Technology Task Force of the Joint Committee of the Higher Education and Entertainment Communities reserves the right to cancel this RFI at any time. Technologies may or may not be selected for pilot or evaluation testing at the discretion of individual campuses.

### *10.2 Neutrality*

The Technology Task Force of the Joint Committee of the Higher Education and Entertainment Communities will neither recommend nor approve any response to this RFI. The task force will not endorse specific business models or technologies. Evaluation and testing that may be conducted by individual campuses of selected technologies will in no way indicate a preference for any technology or vendor over another competing technology or vendor.