What is CALEA?

CALEA is the Communications Assistance for Law Enforcement Act. It requires providers of commercial voice services to engineer their networks in such a way as to assist law enforcement agencies in executing wiretap orders. On August 5, 2005, in response to a request by law enforcement, the FCC voted to extend CALEA to include all facilities-based Internet service providers. Facilities-based Internet service providers are defined as: “entities that provide transmission or switching over their own facilities between the end user and the Internet Service Provider.” Initially it was assumed that CALEA covered only Voice Over Internet Protocol (VOIP) traffic, but the FCC has clarified that the rule applies to all packet-based communications. Deadline for mandatory compliance is May 14, 2007. Because Pace University does provide Internet access (transmission and switching) via the majority of networked PCs, the University must evaluate applicability of and compliance requirements of this law.

What capabilities does CALEA require covered entities to provide?

Law enforcement could request, and the covered entity must provide:

1. All communications associated with an IP address or jack.
2. All communications associated with a person (user), wired at a specific location, wired on any authenticated access, or wireless.
3. Call-identifying information that is reasonably available before, during, or immediately after the transmission of a wire or electronic communication, and in a manner that allows it to be associated with the communication to which it pertains.

The covered entity must be able to expeditiously, unobtrusively, and secretly isolate and enable the government to intercept all wire and electronic communications of a targeted user, to or from equipment, facilities, or services of the covered entity, and to exclude any other communications not covered by the warrant/subpoena. The entity must also provide training and background checks on personnel, a 24 x 7 point of contact, document processes for interfacing with the law enforcement agency and maintain accurate records.
What entities are exempt from CALEA?

The FCC exempts private networks from CALEA, however, they do not explicitly define what constitutes a private network. The American Council on Education (ACE) interprets the private network provision for higher education institutions as:

A higher education or research institution should be fully exempt from CALEA if it satisfies two criteria:

1. Its network qualifies as a “private network,” and
2. It does not “support” the connection of the private network to the Internet. In practical terms, this means that an institution should be exempt where it restricts the use of its network to particular classes of users (e.g., students, faculty, and administrators), and where the institution relies on a third party (such as a commercial ISP or a regional network) to provide the transmission and switching facilities used to route traffic to the Internet, rather than self-supplying such facilities.

THE APPLICATION OF CALEA TO HIGHER EDUCATION NETWORKS, ACE, July 2006

A Strategy for CALEA Compliance – Full Exemption

Under current guidelines, there are essentially three strategies for CALEA compliance; full compliance as a ‘public broadband internet’ provider, full exemption under the ‘private network’ clause if the connection is supported by a commercial ISP, or partial exemption (complying only at the gateway) by qualifying as a ‘private network’ that ‘supports’ its connection to the Internet. Based on the costs and workload requirements, Pace University’s best option for compliance is to pursue full exemption as a private network.

Full exemption under the ‘private network’ exemption is the least expensive and least workload intense option—providing that current interpretation and guidance from Educause, ACE, and the ALA is accurate. To qualify as a ‘private network’, Pace University must restrict Internet access to ‘particular classes of users’ and must rely on an external ISP to ‘support’ the connection to the Internet.

The ACE opinion specifically lists students, faculty, and administrators as particular classes of users, and there is likely justification for other classes who receive intermittent or occasional access. Some examples of these other classes of users are: Library users; Corporate and Community Services customers using the Internet while holding training, conferences, and meetings at the University; Career Planning and Placement customers using PCs while seeking assistance with career guidance; and University Job Applicants using PCs to apply for University employment. There are likely other classes of users that still need to be identified.

The second provision to qualify as a private network, ‘support’ the connection to the Internet, is not as clear; it primarily depends on where the border of the network vs. the Internet is defined. Pace University’s Internet connectivity is provided by 2 ISPs, Verizon and FastLinks. Currently, these ISPs own and support the Routers/Gateways—the transmission and switching facilities used to route traffic to the Internet—that support Pace University’s connection to the Internet.
public Internet. According to the ACE opinion, because Pace University’s ISPs ‘support’ the connection, Pace University qualifies for full exemption.

An ambiguous area that needs further clarification by the FCC is the impact of PCs that may be used by the general public for Internet access. There are a limited number of PCs in various areas of the University that do provide this access. While some degree of public Internet access may be permitted, the current prevailing opinion is that the more public access provided, the more likely an institution will not qualify for private network status. Currently, the FCC has not clarified the amount or degree of public access permitted—or even if public access is a CALEA consideration. If the FCC rules that restriction of public access is a key provision for ‘private network’ status, Pace University will develop and implement an authentication process to ensure these PCs are only accessible to users who fall into one of the identified classes of users.

In summary, as long as the ACE interpretation is validated, and after the question of the impact of PCs providing Internet access to the general public is addressed by the FCC (and authentication process implemented if required), Pace University qualifies for CALEA exemption under the private network clause.

Even though we are exempt from CALEA under the private network clause, Pace University is committed to upgrading its network technology to comply with the intent of CALEA – to be able to uniquely identify personnel to IP addresses within the University’s networks. To this end, we are moving to enable said protocols by replacing non-compliant networking hardware with upgraded technology that will support 802.1X authentication protocol, necessary for end user identification.