

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)	
)	
Communications Assistance for Law)	ET Docket No. 04-295
Enforcement Act and Broadband Access and)	
Services)	RM-10865

**REPLY COMMENTS OF
University of Maryland, College Park**

Introduction and Summary

The University of Maryland (“University”) respectfully submits these reply comments in response to the Further Notice of Proposed Rulemaking adopted in the above-captioned docket.¹ The University supports the comments filed by the Higher Education Coalition and submits this reply to amplify several points based on its own experience and circumstances.

The University supports the goals of the Commission to re-evaluate services provided by telecommunications carriers to ensure that court-ordered electronic surveillance remains effective. As the technology changes for providing traditional voice and data service, new mechanisms are needed to ensure that law enforcement agencies can successfully discharge their responsibilities under federal law. However, campus networks operated by higher education institutions are private networks, not public networks, since these networks are not offered for use by the general public, and are used to support the University’s information service for research and education. Applying the Communications Assistance for Law Enforcement Act (CALEA) to these private networks is not what Congress intended. The University also

¹ *Communications Assistance for Law Enforcement Act and Broadband Access and Services*, First Report and Order and Further Notice of Proposed Rulemaking, ET Docket No. 04-295, FCC 05-153 (rel. Sept. 23, 2005) (“*Order*”).

maintains that the University's private network is exempt from CALEA since this network as a whole implements the University's research and education information service. The University's private network is composed of local services (e.g. authentication service, streaming service, and Web service) which work together to form the University's information service. Thus CALEA should at most apply to the boundaries of the University's private network where the private campus network connects to the public Internet and not to sub-components within the University's private network.

The University of Maryland maintains that there is no demonstrated need and no rationale to have this capability in place within an 18 month period. The number of requests for electronic surveillance received by the University is very small and the University can effectively cooperate with law enforcement agencies with our current network infrastructure while we evolve to a CALEA compliant architecture. Requiring compliance within 18 months will pose an undue hardship on the University and its students.

Applying CALEA to higher education networks will, most importantly, severely impact the teaching and research missions of higher education institutions due to the significant financial, labor and opportunity costs involved in becoming CALEA compliant in a short 18 month timeframe. A reasonable approach would be to require compliance within five years, so that CALEA compliant equipment can be procured when campus technology is refreshed in its normal cycle, rather than requiring replacement immediately.

Discussion

- 1. The FCC Should Clarify That Higher Education Networks Are Exempt from CALEA.**

Congress does not appear to have intended for CALEA to apply to private networks that implement interconnected information services such as those found in higher education networks. (CALEA Legislative History, House Report No. 103-827 at 20). The definition of “telecommunications carrier” does not include “person or entities insofar as they are engaged in providing information services” such as electronic mail providers, or on-line service providers. The University is a not-for-profit educational institution that does not permit the general public to access its network. Thus the University’s network is not a “common carrier for hire” under CALEA section 102(8) and is a private network. The University’s private network is composed of many different local services that together form the University’s information service. That is, requests for information may utilize one or more University-provided services (e.g. authentication service, data repository service, streaming service, computing service, Web service) to fulfill a single request. Thus local services connected by the University’s private network and invoked by information requests are the University’s information service and should be exempt from CALEA.

The University respectfully requests that the Commission review the compliance framework outlined in the original CALEA statute and consider an exemption for higher educational institutions as part of the outcome of the current Notice of Proposed Rule Making.

2. The University’s experience with surveillance requests demonstrates the absence of any need to quickly impose CALEA requirements on higher education private networks.

The University of Maryland enjoys an excellent record of law enforcement support and cooperation in matters involving local, state and federal compliance. The University has more

than 35,000 students and 12,000 faculty and staff and has partnerships and programs with such entities as the Department of Homeland Security, Department of Justice, Federal Bureau of Investigation, and National Security Agency to assist in federal law enforcement activities. The University also maintains its own law enforcement unit, the University's Department of Public Safety, which works collaboratively with the Maryland Montgomery County Police, Maryland Prince George's County Police, Maryland Anne Arundel County Police, Baltimore City Police, Baltimore County Police, Maryland State Police, Virginia law enforcement agencies, Washington D.C. Police and U.S. Capitol Police for incidents that involve the University and its constituents.

Despite its large size, the University only occasionally receives subpoenas involving law enforcement activities. Law enforcement requests seeking assistance with electronic surveillance are virtually non-existent. The University is aware of less than a handful of state or federal subpoenas seeking electronic surveillance assistance within the last five years.

Still, when a request for assistance is received, the University responds with diligence and dispatch using existing infrastructure and technology. The Office of Information Technology at the University of Maryland provides ongoing management and oversight of the University's voice and data networks and ensures network security and electronic communications integrity. Network specialists are available to respond in real time to any network emergency and are in a position to expeditiously assist any law enforcement request.

In short, there is no demonstrated need to extend CALEA to educational institutions, such as the University, which only rarely receives requests from law enforcement for electronic surveillance assistance and which are already prepared with existing infrastructure to quickly and reasonably assist law enforcement when such requests are received.

- 3. A broad application of CALEA would impose significant burdens on the University and divert funding from its critical educational and research mission and could substantially increase student tuition or fees, which would prevent some prospective students from attending the University. Furthermore, the lack of technological guidance from vendors and the benefit derived from the investment further dilutes the justification of the costs.**

The need to exempt higher education private networks is pronounced as there is currently little guidance from our network vendor on the extent of any necessary CALEA upgrades or even the availability of CALEA approved upgrade technologies, even though the Commission has mandated “full compliance” by all newly-covered CALEA entities within 18 months.

In this regard, estimating the cost of “full compliance” under the revised CALEA mandate is difficult at best. The complexity of technologies inherent to broadband access and the unknown extent of access that law enforcement may require make estimating the cost of the required upgrade virtually impossible. However the costs of “full compliance” are expected to be excessive and burdensome. For example, the cost of replacing existing switches, routers and wireless access points coupled with the required redesign of the University’s network will cost up to \$18M for a large research university like the University of Maryland as estimated by EDUCAUSE. In addition, implementing such upgrades within 18 months requires that the University replace all the equipment at virtually the same time and before the end of the equipment’s useful life rather than incrementally replacing equipment on an annual basis. This extra replacement cycle wastes precious funding, wastes staff time and poses an opportunity cost on major projects (including computer security projects) that will not be done due to the manpower requirements for the replacement effort.

In short, if the FCC were to apply CALEA broadly to higher education networks — contrary to the text of the statute — such a ruling would impose significant burdens that far

outweigh its benefits. The Commission accordingly should exempt higher education institutions and research networks from CALEA, if it considers them subject to the assistance-capability requirements in the first place. Moreover, if the FCC applies CALEA to higher education networks at all, it should construe the *Order* as applying at most to the Internet connection facilities at the boundary of the University's private network, for the reasons stated by the Higher Education Coalition.

Conclusion

The University of Maryland respectfully requests that the Commission clarify that private networks operated by higher education and research institutions are not subject to CALEA, or alternatively grant an exemption under Section 102(8)(C)(ii) of CALEA. If the Commission finds that the higher education private networks of information resources must be covered, then the time limit for compliance should be extended to five years to enable this capability to be incorporated into existing networks during normal technology refresh actions rather than imposing a significant financial burden of immediate replacement over the next 18 months.

Respectfully submitted,

Jeffrey C. Huskamp, Ph.D.
Vice President and Chief Information Officer
1122 Patuxent Building
Office of Information Technology
University of Maryland, College Park
College Park, MD 20742
Voice: (301) 405-7700

December 20, 2005