October 19, 2001

Dear Congressman:

As the Co-Chairs of the U.S. Technology Policy Committee of the Association for Computing Machinery (USACM), we are writing to you concerning the House and Senate Conference to reconcile the differing anti-terrorism bills, H.R. 3108 and S.1510. As computer scientists and technologists from industry, academia, and government, we would like for you to be aware of our concerns as you consider legislation that affects the U.S. computing community and information infrastructure.

We are concerned that both Section 814 of H.R. 3108 and Section 809 of S. 1510 extend the definition of terrorism to acts currently considered vandalism or "ordinary" criminal behavior, and possibly to innocent behavior by scientists and technicians. Among these are acts specific to computing systems, covered under the Computer Fraud and Abuse Act (18 U.S.C. 1030, et seq.). We strongly advise you resist these extensions of the law. Although it may be tempting to consider what potential terrorists may do and include all of those possibilities within revised laws, there are many problems with such an action.

First and foremost, there is the problem of making too broad a definition of terrorism in a manner that casts ordinary criminal behavior as terrorism. For example, web site defacement is criminal, but is also non-violent in nature and, although annoying, is unlikely to result in any significant physical damage, injury or death. If defacing web pages becomes a terrorist act -- and one that is committed dozens of times a day already -- then it may lead to inflated reporting of terrorism incidents (with a concomitant loss of public confidence), and a diffusion of law enforcement resources to respond to them when more urgent incidents need attention. We have similar concerns with other behavior that would be included in the definition of terrorism under this proposal, including collecting passwords, writing email viruses, and some of the physical acts that are also proposed for coverage. In our view, some of the actions that could be included in such a broad definition of terrorism do not come any closer to it than spray-painting comes to suicide bombing.

Second, extending terrorism offenses to cover those who may be thought to assist terrorists is too inclusive (Section 806 of S. 1510 and Section of 805 of H.R. 3108). For instance, if someone publishes a technical article that describes security weaknesses or provides a tool that tests a system for security flaws, it is conceivable that a criminal might use those items to break in to a system. If someone provides public access to a wireless network, or a free account for WWW pages, criminals might use those services to break into computers, as has already happened. Just as we don't hold aircraft designers responsible for hijackings, we don't want to risk the possibility that law-abiding citizens who wrote the books, designed the software, or ran the computers used to commit an act of terrorism could be confronted with life imprisonment.

Third, criminal acts that are truly terrorist in nature will likely be covered by other provisions of the act, and by existing statute -- there is no need to define these additional offenses. If a group of terrorists plan a bombing and including a web defacement or system break-in as part of their plan, they could be prosecuted as terrorists under the conspiracy and bombing portions of their activities. There is no need to include the computer misuse as explicit terrorist acts.

In conclusion, we are unalterably opposed to terrorism and criminal behavior. We are also firm in our belief that laws should be balanced and precise in their coverage. We do not foresee any value, but we do foresee potential harm, in incorporating so many existing crimes under this expanded definition of terrorism.

The ACM is a leading society of computer professionals in education, industry, and government. The USACM facilitates communication between computer professionals and policy-makers on issues of concern to the computing community. Please contact Jeff Grove, the Director of the ACM Washington Policy Office at (202) 659-9711 if you have any questions or if

we can be of assistance to your efforts.

Sincerely,

Barbara Simons, Ph.D.
Eugene H. Spafford, Ph.D
Co-Chairs
U.S. ACM Public Policy Committee
Association for Computing Machinery

About USACM:

USACM is the U.S. Public Policy Committee of the Association for Computing Machinery (ACM). ACM is the leading nonprofit membership organization of computer scientists and information technology professionals dedicated to advancing the art, science, engineering and application of information technology. Since 1947, ACM has been a pioneering force in fostering the open interchange of information and promoting both technical and ethical excellence in computing. Over 70,000 computer scientists and information technology professionals from around the world are members of ACM.