The Institute of Electrical and Electronics Engineers-
United States Activities
1828 L Street, NW, Suite 1202
Washington, DC 20036
T: (202) 785-0017; F: (202) 785-0835

The Association for Computing
U.S. Public Policy Office
666 Pennsylvania Ave., SE
Suite 302 B
Washington, DC 20003
T: (202) 544-4859
F: (202) 547-5482

July 3, 1997

The Honorable John McCain
Chairman
Senate Commerce, Science & Transportation Committee
241 Russell Senate Office Bldg.
Washington, DC 20510

Dear Mr. Chairman:

The U.S. Public Policy Office for the Association for Computing (USACM) and The Institute of Electrical and Electronics Engineers-United States Activities (IEEE-USA) note with considerable dismay the Senate Commerce, Science and Transportation Committee's recent approval of S. 909, the "Secure Public Networks Act."

We share many of the concerns of the Committee members regarding problems of national security and law enforcement. However, we believe that the "Secure Public Networks Act," as approved by the Committee, leads U.S. encryption policy in the wrong direction. The proposed bill stands in opposition to the scientific and professional opinions of many experts who believe that national security and public safety will be weakened by the mandated introduction of constrained or recoverable-key encryption. We also believe that such action will hinder U.S. competitiveness in international markets, establish a dangerous precedent for the future, and endanger cherished civil liberties in the U.S. and elsewhere in the world. Since no hearings were held on the bill, the Committee may not have had full information on its implications. We believe the bill will have a serious, negative and long-term impact on society in general and on our organizations and their members. We are keenly interested in supporting significant consideration of the important issues involved, and we would very much like to provide technical and scientific input on this issue. Many of our members are internationally-recognized experts in the area of information security and encryption, and several have significant experience with law enforcement and national security issues. We would be happy to put you in contact with some of these experts should you desire more information on the points we outline in this letter.

In what follows, we briefly outline some of the reasons why so many experts believe such a bill is harmful if it became law.

First, the bill is economically harmful. Voting to restrict strong cryptography would damage America's dominance in information technologies.

Secure software and hardware is available overseas. Mathematical acumen exists around the world; the U.S. can neither control nor contain it. Software companies will continue to be forced to seek talent elsewhere. The widely-used, strong cryptographic algorithm IDEA, for example, was developed in Europe. U.S. software and hardware suppliers can incorporate IDEA into their products, but only if those products are confined to use in the U.S. Export controls have obviously not hindered the worldwide spread of encryption products based on IDEA and produced outside the U.S. These controls have merely prevented U.S. providers from participating in that global market. Customers throughout the world have the sophistication to understand the need for strong cryptographic products and they will continue to seek to buy them wherever they are sold. The result will be an increasing loss of jobs and revenues in an area where the U.S. once held the dominant position. It is conceivable that our own industry and civilian sector might eventually become dependent on foreign cryptography products should U.S. firms continue to be prohibited from open competition in this arena.

Second, this bill threatens cherished civil freedoms. Information technologies make data surveillance possible and increasingly affordable. The best technical protections available to the individual depend upon cryptography. There is also an unfortunate history of a few law enforcement agents and government officials using their positions and access to violate the law and the rights of citizens. Strong encryption is the only practicial means available to law-abiding citizens to defend themselves against these infrequent, but all-too-real abuses.

The wording in the proposed bill for organizations with Federal funding to rely on a mandated form of encryption will be burdensome and may lead to severe invasions of privacy. For instance, if a library or university were forced to implement such encryption, how could the organization ensure that its users were actually employing the system? The only sure method would be to "snoop" on the messages to see if they were breakable under the mandated scheme. Otherwise, users would be able to substitute their own encryption instead of, or in addition to, the mandated form, thus rendering this bill meaningless but still costly to implement. This raises serious questions about privacy -- and more importantly -- First Amendment considerations.

Third, the criminal element will not be hindered by any legislation similar to the one proposed. The referenced bill provides no provisions that would actually deter criminals from employing strong encryption obtained from other sources. Drug cartels, terrorists, pornographers and others who might use encryption in criminal enterprises are already violating laws with penalties much more severe than any that might be imposed for using unauthorized encryption technologies. Meanwhile, law-abiding citizens would be forced to rely on technologies that might not protect their private information against "crackers" and potential blackmailers. As in the physical world, the best public safety results from crime prevented through good practices, rather than crimes solved. Without strong cryptography Americans cannot lock their electronic doors, but must instead remain vulnerable. Thus, constraining cryptography might help law enforcement solve a small number of crimes, but it will do nothing to prevent opportunities for even more crimes, thereby reducing overall public safety.

Fourth, constraints on strong cryptography will jeopardize national security. Requiring or encouraging weakened technology leaves the United States vulnerable to information warfare from other nation-states, techno-anarchists and terrorists, and from organized criminal elements. It is vital that telephone systems, medical health care systems, utility systems, and other control mechanisms affecting every sector of the economy be made more secure and not restrained from using improved security. Our national security depends on the reliability of our national infrastructures and critical systems, particularly those based on computer and communications technology. To legislate the use of untested mechanisms that present weakened protection, or that have a single point of failure and attack, will unnecessarily endanger those critical institutions and the people who depend on them. Those same forces arrayed against our national interests will be freely able to obtain stronger cryptography technology from the many other countries that do not place restrictions on its development and sale.

Fifth, information technologies change quickly. We don't want to require enabling legislation whenever advances in technology increase the vulnerability of current key lengths. The recent cracking of 56-bit DES in the RSA challenge shows that distributed computing power is now available to break this key length, thus identifying a need for larger keys. A breakthrough in mathematics, such as increasing the speed of factoring numbers, would require a prompt response, such as increasing key lengths or changing algorithms. The proposed legislation would severely discourage such changes. Additionally, by preventing the initial acquisition of strong encryption technology, the need for near-term upgrades to defeat improved cracking techniques is almost assured, as are the extra financial burdens.

As a last point, consider the implicit message sent by passage of this act or any like it. The U.S. has long been a vocal proponent of freedom of speech and other civil rights for citizens around the world. Why should any other nation's leaders heed further such rhetoric if the U.S. adopts the proposed bill? If some foreign nation with a history of oppression were to pass the same legislation so as to eavesdrop on their citizens' communications for purposes of identifying human rights activities, we would register strong disapproval. With passage of legislation such as the "Secure Public Networks Act" the U.S. loses the moral high ground in any future such scenario.

In summary, our professional position is that passage of the "Secure Public Networks Act" or similar legislation is ill-advised; we urge you to defeat this bill. Instead, we encourage passage of legislation such as Senator Conrad Burns' Pro-CODE bill, or Representative Bob Goodlatte's SAFE bill as a better, more effective aid to national security, law enforcement and civil rights.

IEEE is the world's largest technical professional association with 320,000 members worldwide. IEEE-USA promotes the career and technology policy interests of the more than 220,000 electrical, electronics and computer engineers who are U.S. members of the Institute. The Association for Computing (ACM) is an international non-profit educational and scientific society with 76,000 members worldwide, 60,000 of whom reside in the U.S. USACM strives to promote dialog on technology policy issues among U.S. policy makers, the general public, and the technology community.

If you need additional information, please contact Deborah Rudolph in the IEEE-USA Washington office at (202) 785-0017 or Lauren Gelman in the USACM Public Policy office at (202) 544-4859 or (202) 298-0842.

Sincerely,

Barbara Simons, Ph.D.
Chair, U.S. Public Policy
Committee of ACM Board
Activities Board

Paul J. Kostek
Vice Chair
United States