October 2, 2001

To: Members of the U.S. Congress, Congressional Internet Caucus
Fr: U.S. Policy Committee of the Association for Computing Machinery (USACM)
Contact: Jeff Grove, Director of Technology Policy, USACM, (202) 659-9711
Re: Legislative Recommendations to Secure the U.S. Computing Infrastructure

We understand that Congress is currently considering many legislative initiatives to address issues of security and law enforcement related to terrorism. We would like to put forth some suggestions for legislative initiatives that will help secure the U.S. computing infrastructure against malicious attacks, whether from terrorists or common criminals.

Many of the current security problems faced by both government and industry stem from the acquisition and use of software that is poorly designed, rushed to market, and/or inadequately tested. This software is often adopted for use based on price rather than quality or safety. Security personnel often point-out that they are forced to use COTS (commercial off-the-shelf) software with a poor history of security because of issues of cost and lowest bid.

We encourage Congress to consider legislative action that will:

- require Federal specification and evaluation of data processing software and equipment to include explicit requirements for standard security features and proof of comprehensive testing for faulty code;

- require that vendors disclose a full 3 to 5-year history of security flaws, patches and exploitations of the products (and similar products by the same vendors) proposed in response to Federal solicitations, and require that the evaluation of such proposals give significant consideration to these histories;

- allow Federal acquisition of computing services and equipment to be done from other than the lowest bidders if product security and safety are judged to be significantly stronger than that of the low bidders;

- disallow vendors from disclaiming liability for products coded with software practices that are well-known within the security and software engineering communities to be careless and dangerous;

- enable "software self defense" -- explicitly allow consumers to reverse-engineer software or hardware products if that reverse engineering is done to expose or repair software faults or design errors that reduce the safety or security of the products;

- enable "software community defense" -- invalidate any license or legal prohibition that restricts publication of benchmark studies, product reviews or other descriptions of the products or algorithms when that publication is made to expose or facilitate repair of flaws that reduce the safety or security of the products.

Page Two:
USACM Memo to U.S. Congress
October 2, 2001

Our national (and international) infrastructure depends on the correct functioning of our computing infrastructure. It is distressing that issues of cost have led the Federal government to acquire and deploy some COTS products in defense, law enforcement, and fiscal operations that are known to be buggy and difficult to secure. Unfortunately, ensuring safety and quality is more expensive, and there have been insufficient incentives for some vendors to pursue -- seriously -- better quality. We request that Congress consider helping to address this issue before we are further endangered. The Internet generally functions well as a cost effective means of data communication. That makes it imperative for those who use it - corporate and consumer alike - to take the initiative to see that the software they own and use meets their own real security and reliability needs.

The ACM is a leading society of computer professionals in education, industry, and government. The USACM Public Policy Committee, co-chaired by Dr. Barbara Simons and Dr. Eugene Spafford, facilitates communication between computer professionals and policy-makers on issues of concern to the computing community. For more information, please contact Jeff Grove, Director of the ACM Washington Policy Office at (202) 659-9711, or see the USACM policy web site at: <http://www.acm.org/usacm>.