by Diane Crawford

from washington

Two Bills Equal Forewarning

U.S. Justice Department attorney Mark Rasch sums up the ongoing efforts to strengthen computer crime legislation with an old Hill aphorism: "Those who like sausage, and have respect for the law, should never watch either being made."

In question are two House bills reintroduced to the 101st Congress to amend title 18 of the U.S. Criminal Code. Proponents of H.R. 55, *Virus Eradication Act* and H.R. 287, *Computer Protection Act* are confident the bills successfully tighten any remaining loopholes in the original statute and offer much more potent legal protection against computer crime. Critics, however, claim the acts are so laden with ambiguity that translations may render many common practices illegal (*see boxes*).

In essence, H.R. 55 is designed to provide penalties for persons interfering with the operations of computers with programs containing hidden commands that can cause harm. Whereas, H.R. 287 would create civil and criminal penalties for persons (or organizations) which knowingly and maliciously alter computer hardware or software so as to disable a computer either through the loss of stored data or interference with its proper functioning.

As the coordinator for all Justice Department computer fraud cases prosecuted under section 1030 of the U.S. Criminal Code, Rasch is often asked to review and comment on new legislation in the field. He sees several problems in H.R. 55, primarily its attempt to address certain parts of the problem, but not the entire problem. The real test, he points out, is the phrase "knowing or having reason to believe (a program) may cause damage" because the interpretation can include every piece of software in America.

"Frequently, statutes are written that criminalize things that should not be criminal," Rasch explains. "You want to write them broad enough so that they deal with the problem you want to deal with, and narrowly enough so that they don't criminalize a whole class of activity that might otherwise be protected."

The Virus Eradication Act was originally introduced last July—months before the Internet worm or West German spy ring incidents—to a less-than-enthusiastic Congress, recalls Douglas Riggs, legislative assistant to H.R. 55 author Wally Herger (R-CA). Since then the bill, and Congressional membership, have been somewhat reorganized and recent computer crime stories have heightened political interest.

"There is a lot the bill cannot address initially in terms of its language," Riggs explains. "We are just offering a base on which we could expand when we go into hearings. We think we've come up with something that is the best possible solution at this point as we see it."

There are no sanctions for unauthorized access in H.R. 55, and the omission was intentional. If a person, authorized or not, creates a virus that intentionally endangers a single file—which could mean anything from loss of time to loss of business because of customers losing trust in a company—that person has committed a crime and will be held accountable.

The purpose of the proposed bill is to introduce specific legislation against viruses into section 1030, the 1986 Computer Fraud and

Excerpts from H.R. 55: Virus Eradication Act

(Whoever) knowingly:

(A) inserts into a program for a computer, or a computer itself, information or commands, knowing or having reason to believe that such information or commands may cause loss, expense or risk to health or welfare . . . to users who rely on information processed on such computer; and

(B) provides (with knowledge of the existence of such information or commands) such program or such computer to a person in circumstances in which such person do not know of the insertion or its effects; if inserting or providing such information or commands affects, or is effected or furthered by means of, interstate or foreign commerce.

Civil remedy: Whoever suffers loss by reason of violation of (this) subsection may, in a civil action against the violator, obtain appropriate relief. In a civil action under this section, the court may award to a prevailing party a reasonable attorney's fee and other litigation expenses.

Abuse Act. The broadness of the bill, Riggs explains, is due to the fact that the term *virus* is still difficult to define and probably destined for obsolescence.

Fortifying the Criminal Code against acts of malicious computer sabotage is also the impetus behind H.R. 287, authored and introduced in the House by Tom McMillen (D-MD) subsequent to H.R. 55. Although sabotage can be prosecuted under the current law, it is not presented explicitly in the code and therefore is difficult to try.

The goal of H.R. 287 is to impose stronger criminal and civil fines on persons who maliciously invade a computer system. "This is not about a person who accidently stumbles into a system and messes things up," says a spokesperson for Rep. McMillen. "The bill is specifically worded to indicate that malice and motivation must be proven."

As beneficial as legislation against computer crime might appear, Jay J. BloomBecker warns that talk is cheap. As chair of ACM's Legal Issues in Computing board and director of the National Center for Computer Crime Data, Los Angeles, BloomBecker warns that it's one thing to have more opportunity to go after those that have clearly broken laws, it's another thing to make those laws effective.

"In general, most of the discussion of computer crime law has been self-indulgent, self-aggrandizement by lawyers who assume what the laws say will have some effect," he asserts. "The biggest fallacy is that the laws don't say anything until you put some money behind them to enforce them. For the most part, that hasn't happened yet on a state or federal level."

Excerpts from H.R. 287: Computer Protection Act of 1989

(A) Whoever willfully and knowingly sabotages the proper operation of a computer hardware system or the associated software and thereby causes the loss of data, impaired computer operation, or tangible loss or harm to the owner of the computer, shall be fined . . . or imprisoned not more than 15 years, or both.

(B) A party harmed by a violation of this section may in a civil action seek appropriate compensation for damages caused by that violation and, in the discretion of the court, may be reimbursed by the defending party for any or all legal expenses incurred in the course of the action.

Senate Gets Into Act

While Herger and McMillen await hearing dates for their bills on the House docket, the Senate has initiated some basic groundwork into its own investigation of computer security problems. On May 15, the Subcommittee on Technology and the Law of the Senate Judiciary Committee held its first hearing on the issue of computer viruses. The hearing, set to examine the scope of the threat posed by computer invasions, was chaired by Sen. Patrick Leahy (D-VT), and featured panelists William S. Sessions, director of the FBI, and Wily Hacker sleuth Cliff Stoll, of the Harvard-Smithsonian Center for Astrophysics. (See *Communications*, May 1988, p. 484.)

Sessions maintains that while existing federal statutes could use some tightening up and stronger enforcement, they are basically adequate from the FBI's perspective. He pointed out how the Computer Fraud and Abuse Act signed in 1984 was strengthened by 1986 amendments that expanded its crime-oriented base to include federal interest computers. (Those computers used exclusively by financial institutions or the U.S. government, or computers that are one of two or more located in different states and used in committing an underlying offense.)

The Bureau chief also noted that the educational benefits derived from the free flow of information must be balanced with the need to prevent criminal activity having the potential for millions of dollars in damage. Warns Sessions: "Once the balance tips to criminal activity, the FBI intends to pursue vigorously those who violate federal law through the creation and introduction of viruses."

Stoll detailed the integral role computer networks play in the academic and scientific environs, portraying them as intricate and as necessary as the streets, roads and highways that tie global communities together.

He touched on his own two-year experience tracking the West German hacker who was apprehended last spring, and ended by urging both government and industry to recognize their responsibility in protecting this vital resource of information. "Now, our electronic communities are threatened," Stoll stresses. "Vandals have spread computer viruses and worms. Foreign institutions have been robbed elec-

The FBI has found that computer crime is often one of the most elusive crimes to investigate. It may be invisible. It has no geographic limitation. The entire transaction may last less than a second.

FBI Director William S. Sessions
Addressing Senate hearing
May 15, 1989

tronically. Alas, our golden age of trust is ending."

Strength in Numbers

The ACM and other professional organizations can play a definitive role in the direction and effectiveness of computer crime legislation.

In his June 1989 President's Letter (*Communications*, p. 660) Bryan Kocher calls for computing professionals to take control of their industry before outsiders do. Although federal legislation assures consistent, higher quality regulations, Kocher fears a mishmash of nightmarish state laws. He is proposing that ACM and IEEE and other industry associations adopt and enforce standards for computing professionals.

BloomBecker agrees and has already made plans to suggest at his next board meeting that ACM and the IEEE jointly create a standard or bylaw that indicates how the organizations will respond and react to members involved in computer-related crime.

Rasch and Riggs urge computer associations to voice their comments on the issue of computer crime to local state representatives, and to the offices of Congressman Wally Herger (1108 Longworth, Washington, D.C. 20515. Phone: 202-225-3076), or Tom McMillen, (327 CHOB, Washington, D.C. 20575. Phone: 202-225-8090). The Senate Subcommittee on Technology and the Law (The Hart Office Building, Suite 815, Washington, D.C., 20510. Phone: 202-224-3406) has also issued an invitation to ACM to discuss computer crime concerns.

Riggs points out that Herger's office has already met with members of several industry trade organizations regarding H.R. 55, insisting it is the only way to create comprehensive laws against high-tech crime. "We've been trying to work as much as we can with people in the real world," he says. "D.C. is not the real world, and all too often we have a tendency here to think we have the best solution to any problem."

Sen. Leahy, addressing the Senate hearing, presses the issue with the ultimate scenario: "As a nation, we cannot afford data that scientists cannot trust. We cannot afford to have scientists refusing to use computer networks to share their discoveries, and thus, advance technology."