A major purpose of the Technical Information Center is to provide the broadest dissemination possible of information contained in DOE's Research and Development Reports to business, industry, the academic community, and federal, state and local governments.

Although a small portion of this report is not reproducible, it is being made available to expedite the availability of information on the research discussed herein.

LA-UR-84-650
CONF-8404109--1

LA-UR--84-650

DE84 007468

Los Alamos National Laboratory is operated by the University of California for the United States Department of Energy under contract W-7405-ENG-36

TITLE: ATTACKS ON COMPUTERS: CONGRESSIONAL HEARINGS AND PENDING LEGISLATION

AUTHOR(S): David Bailey

SUBMITTED TO: IEEE 1984 Symposium on Security and Privacy, Oakland, CA, April 30-May 2, 1984.

DISCLAIMER

Los Alamos National Laboratory
Los Alamos, New Mexico 87545

FORM NO 836 R4

ATTACKS ON COMPUTERS:

CONGRESSIONAL HEARINGS AND PENDING LEGISLATION

by
David Bailey

Los Alamos National Laboratory
Los Alamos, New Mexico 87545

ABSTRACT

During the First Session of the 98th Congress, several days of hearings were held on the activities of computer enthusiasts including the Milwaukee 414s and others. The First Session also saw the introduction in the House of six bills dealing with various aspects of computer crime. A summary of those hearings, along with a summary of the pending computer crime bills, will be presented.

INTRODUCTION

During the summer of 1983 it was revealed that a number of youths from Milwaukee had gained access to computers in various parts of the country using the capabilities of Telenet, a nationwide digital communications network. The event quickly became the summer media event. It was reported in virtually every newspaper and television news program in the country. Interviews were conducted on national television programs, and Johnny Carson included the incidents in his monolog.

But what really happened? How serious was the problem? Who was doing this, and how good were they? What are the real vulnerabilities, and what can be done about them? In September, October, and November, the Congress held hearings to find out. This paper is a report on those hearings and a description of proposed computer crime legislation that has been introduced in the 98th Congress.

THE HEARINGS

Fact-finding hearings were held in the House of Representatives by the Committee on Science and Technology's Subcommittee on Transportation, Aviation, and Materials. Chaired by Representative Dan Glickman of Kansas, Representative Glickman held three days of hearings in September and October. These were followed by two days of hearings by the U.S. Senate's Subcommittee on Oversight of Government Management chaired by Senator William Cohen of Maine. The dates of these hearings and the witnesses are shown in Appendix I.

In his opening statement on the first day of hearings Representative Glickman cited the pervasiveness of computers in modern society and the lack of awareness of the ways in which computers can be improperly used. In citing the reasons for the hearings, he said,

> "As we shall learn today, there is an entire underground culture of people known as computer hackers who continuously try to defeat the security measures programmed into modern computers. Beyond this, computer systems are vulnerable to a variety of intentional and unintentional actions that can result in errors, interruption of service, or unauthorized access to and manipulation of confidential information.
>
> To gain a better understanding of these threats and vulnerabilities, the Subcommittee is today beginning an in-depth series of hearings that we hope will not only lead to such an understanding but also will identify steps that need to be taken to prevent abuse of the rapidly growing technology.

Except as specifically cited, the quotations in this paper are taken from the prepared statements of witnesses at the hearings. These statements are included in the hearing transcripts available from the committees involved. The hearing transcripts were not available at the time of writing.

Senator Cohen's press release announcing hearings of his subcommittee asserted that sophisticated criminals, rather than hackers, are the real problem.

> "The frequency of computer crime, which the FBI has named as the fastest growing form of larceny in the United States, is growing much faster than the government's efforts to thwart the problem. We are not just dealing with clever kids who are having fun with their home computers, we are faced with a sophisticated form of crime and misuse which can cause losses in the billions of dollars each year.

The first day of hearings was a circus. The first two witnesses were Neal Patrick, one of the Milwaukee 414s, and Jim McClary, Division Leader of the Operational Security and Safeguards Division at Los Alamos. As a potential confrontation between victim and attacker it provided a great deal of drama, and it was truly a media event. Approximately 20 television cameras filmed the proceedings, and the clicking of the still cameras was occasionally so loud that the speakers could not be heard. During subsequent hearings the drama subsided enormously and by the end of the Senate hearings the proceedings had become routine.

The hearings revealed that computer crime is a very complex issue, one that we do not yet understand very well. They showed that there is little agreement about what computer crime is and virtually no meaningful information about how much of it there is. There is also little agreement about what should be done.

Although the attacks by hackers provided the impetus for the hearings, little time was actually devoted to the problems they can cause. However, one subject that arose several times was the moral and ethical question of whether

the acts of the 414s (and others like them) were wrong (it is fairly clear that these acts are not illegal). Victims are in agreement that this kind of activity is wrong, but others, including some members of congress, are not so sure.

The hearings did publicize the potential security and privacy problems inherent in the use of computers. However, the testimony of the witnesses did not illuminate the threats to and vulnerabilities of computer systems very well, as Representative Glickman had hoped, nor did they support Senator Cohen's statement. The hearings showed that we do not have an accepted notion of what computer crime is. Thus, we do not have a clear idea of how much computer crime there is.

The discussion that follows will select a few of the major themes from the hearings rather than trying to report everything in chronological order.

THE NATURE AND EXTENT OF THE PROBLEM

Definitions

Most of the witnesses did not explicitly say what they meant by *computer crime* or *computer-related crime*. However, they all had at least an implicit idea of what they meant, and lack of a definition did not seem to prevent anyone from discussing how much of it there is. In fact there are several proposed definitions which would lead to widely varying estimates of the number of such crimes. For example, Donn Parker, a Senior Management Systems Consultant at SRI International, offered a frequently heard definition.

> "Computer crime is ... any crime in which the criminal required special knowledge of computers or data communications for its perpetration."

This definition does not require that the computer actually be used in the crime. It would, however, include fraudulent income tax returns prepared to avoid computerized IRS audit limits known to the preparer.

Susan Nycum, an expert on computer law and a partner in the national law firm of Gaston, Snow and Ely Bartlett, wants to broaden this even further to allow for special knowledge by anyone.

> "... computer crime is defined as any illegal act where a special knowledge of computer technology is essential for its perpetration, investigation, or prosecution."

Ms. Nycum's definition would count as a computer crime an act in which the perpetrator did not use a computer or even know anything about one simply because the police or the prosecutor had to know something about computers. This would seem to be too broad a definition.

John Keeney of the Department of Justice included the Rifkin case in his list of computer crimes. Stanley Rifkin, who is acknowledged to be a computer expert, transferred $10.8 million to his own account using knowledge about the bank's wire transfer procedures, an authorization code that was tacked to a bulletin board, and a telephone. This implicit definition is very broad. It would appear to make speeding a computer crime if the car was driven by a programmer.

All three of these definitions, broad or narrow, beg the question by defining computer crime in terms of acts that are already illegal for some other reason. Pending legislation, for example H.R.1092, The Federal Computer Crimes Act of 1983, being considered in the House of Representatives, tries to create a more basic definition, but it runs into other problems in H.R.1092, fines or imprisonment are imposed for

> "whoever uses, or attempts to use, a computer with intent to execute a scheme or artifice to defraud, or to obtain property by false or fraudulent pretenses, representations, or promises, or to embezzle, steal, or knowingly convert to his use or the use of another ..."

This definition is at least not circular, but it still has some difficulties, particularly with the definitions of *computer* and *use*. A *computer*, according to H.R.1092

> "means an electronic, magnetic, optical, hydraulic, organic, or other high-speed data processing device or system performing logical arithmetic, or storage functions, and includes any property, data storage facility, or communications facility directly related to or operating in conjunction with such device or system; but does not include an automated typewriter or typesetter, a portable hand-held calculator, or any computer designed and manufactured for, and which is used exclusively for routine personal, family, or household purposes and which is not used to access, to communicate with, or to manipulate any other computer."

Among other anomalies, this definition leaves us with the odd situation of an electronic device that heretofore has been used exclusively for games and the family budget (and is, therefore, not a computer), which is now used to commit a crime. Suppose, for example, I calculate tables and print sales literature showing how much money you will make by investing in my phony land sales scheme. I have not attempted a computer crime because the device I used is (or was) not a computer. We will encounter worse problems if we allow the device to be magically transformed into a computer the moment it is used in a crime.

The description of the acts covered in H.R.1092 did not appear to be circular, but once we include the definition of a computer, we see that it is. We are back in the situation of determining that some event was a computer crime after we already knew that it was a crime for some other reason.

More important is the question of whether we want events like the one in the land sales example to be computer crimes. I think not. It was simply a fraud in which the computer was involved in a non-essential way. It is beyond the scope of this paper to offer a complete new definition of computer crime. However, I suggest that it should cover acts in which the computer is essential -- acts which could not have been committed without the use of a computer. And, the perpetrator of the crime should be the one who used the computer, not someone else.

The definition of the word *use* also causes some problems. In H.R.1092, to *use* a computer means

> "to instruct, communicate with, store data in, or retrieve data from, or otherwise utilize the logical, arithmetic, or memory functions of a computer, or, with fraudulent or malicious intent, to cause another to put false information into a computer."

This makes practically every welfare fraud a computer crime. They all depend on convincing some welfare representative that you are entitled to benefits when you aren't, and the information you provide is always entered into a computer. These frauds should not be classed as computer crimes.

As a final example of the difficulties involved in trying to pin down what is meant by the terms *computer* and *computer crime*, I include some definitions from the Colorado computer crime bill. Colorado has simpler definitions which avoid the problem with the word *use* but are not much more successful with *computer*.

> "To *use* means to instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or computer network.
>
> *Computer* means an electronic device which performs logical, arithmetic, or memory functions by the manipulations of electronic or magnetic impulses, and includes all input, output, processing, storage, software, or communication facilities which are connected or related to such a device in a system or network."

This definition of a computer is at first pleasing because it is so much simpler than the federal definitions, but it includes too much. It not only includes hand-held calculators but also such innocuous devices as digital watches, fuel injection systems, blenders, and elevators. It, too, is too broad a definition.

The acts proscribed by the Colorado law include not only the use of a computer in a fraud, but also cover the activities of the 414s with the statement that:

> "Any person who knowingly and without authorization uses, alters, damages, or destroys any computer, computer system, or computer network ... or any computer software, program, documentation, or data contained in such computer ... commits computer crime."

This has the right elements, but it allows too many extraneous events to be included. For example, bombing a computer center is included. It also includes intentional destruction of my digital watch, stepping on my calculator, and torching my new automobile.

We can now begin to see some of the elements of a computer crime definition. It should include that the computer was used in an essential way to commit the act and that it was used by the perpetrator of the act. And, the acts proscribed should include the kind of electronic trespassing practiced by the 414s and others like them.

The definition of a computer must not be so broad that it includes calculators, human brains, and electronic devices embedded in other products such as blenders and automobiles. But, it should not restrict things so as to allow a particular device to wander in and out of computerhood depending on how it was last used.

How Much Computer Crime Is There?

Many of the experts testifying provided information about the extent of computer crime. But, since everyone had a different definition of what computer crime is, the indications of the amount of it varied widely. For example, E. J. Criscuoli, Executive Vice President, American Society for Industrial Security said:

> "Computer-related crimes and abuses are a serious and growing problem. According to the Chamber of Commerce of the United States, criminals, armed with computer technology, defraud the public out of more than $100 million annually. The computer criminal poses a growing threat to both business and government."

Donn Parker didn't say how much there is, but did conjecture that:

> "there is an escalation of all kinds of business and white collar crime, not only computer crime, caused by the increasing use and dependence on computers and data communications. By escalation I mean that the frequency of crimes is diminishing while the size of each loss is increasing."

On the other hand, Robert Courtney, an independent consultant in data processing systems management said:

> "I have no reason whatever to believe that there has been a significant increase in white collar crime as a consequence of the introduction of computers into our recordkeeping processes."

People often cite unverified statistics on the extent of computer-related crime. However, as Susan Nycum pointed out, "no one knows the extent of computer crime and abuse." Testimony by FBI Deputy Assistant Director Floyd Clarke indicates three reasons for this.

> "The first of these issues is that a computer is an instrumentality of some other form of traditional crime, for instance theft or larceny. It is much like a gun, a knife, or a forger's pen. The second issue is ... that there does not exist ... one generally recognized and accepted definition as to what computer related crime is. Therefore, we do not have an objective standard to measure the trends of computer related crime. Lastly, in view of the FBI's current structure of management by program, rather than by case, there is no method in place now to observe the statistical dimensions of computer related crime."

Although no one really knows how much computer crime there is, one speaker was willing to place an upper bound on the amount of computer crime. Robert Courtney:

> "There is no possibility that the damage resulting from criminal conduct involving computer-based systems will ever be able to even approximate the losses to mistakes."

Who Commits Computer Crime?

There was greater agreement on the sources of computer crime than on the amount of it. Many of the witnesses felt that outsiders, particularly the casual outsiders who provoked the hearings in the first place, are not the problem. The biggest problem to be faced comes from the people authorized to use the system, and the cure is not more technology, it is proper use of the controls that are already available. For example, Willis Ware of the Rand Corporation:

> "In the commercial sector, the technical threat is at present minimal. The big threat is people within the systems themselves. ... We need only the corporate will to address the problem, and the corporate commitment to put the issue on the same level of concern as protecting other valuable resources. By implication, we also need the corporate commitment to spend the modest sums needed."

Mr. Courtney agreed. In his view it is not even the sophisticated insiders who are the greatest source of problems.

> "There is a ... misconception about ... the people who do engage in computer-related crime. The vast majority of those committing these crimes are non-technical, clerical and administrative, and operational people who simply abuse the limited system capabilities made available to them. ... The people who steal from accounts receivable are not in payroll, they are in accounts receivable."

The FBI's experience according to Mr. Clarke, also shows that insiders rather than outsiders are the sources of computer crime.

> "... it appears from our experience that this is more of a human problem than a technological one. In most instances where we have been involved in an investigation of computer related crime the crime was perpetrated by someone who had access to the computer and authorization to use it."

Richard Kusserow, Inspector General of the Department of Health and Human Services, discussed the result of a recent study of "Computer-Related Fraud and Abuse in Government Agencies" which he conducted for the President's Council on Integrity and Efficiency. He was charged by the Council to provide it with a perspective on the nature and scope of computer-related fraud and abuse in government agencies. Specifically, they wanted to know whether computer-related fraud and abuse are a problem in the government, and, if so, what its characteristics are. For the purposes of the study the following definitions were used.

> "*Computer-related fraud* involved an illegal, intentional act designed to deceive or misrepresent in order to obtain something of value. The computer must have been used to perpetrate or cover-up the act.
>
> *Computer-related abuse* involved the misuse, destruction, alteration, or disruption of data processing resources. Although the abuse is intentional and improper, it does not necessarily imply violation of a specific law or the presence of misrepresentation."

The overriding finding of the study is that "we still do not know the scope of computer-related fraud and abuse in government." However, of the 172 cases considered, 89 fraud cases and 103 abuse cases, Mr. Kusserow reports that

> "Most of the perpetrators of either fraud or abuse were non-supervisory, federal employees. Four out of five of the fraud perpetrators earned $20,000/year or less, while half of the abuse perpetrators earned over $20,000/year. Most of the fraud perpetrators (62%) were functional users of the computer systems, while an almost equal percentage (59%) of the abuse perpetrators were data processing personnel."

Mr. Kusserow would seem to be saying that experiences within government are about the same as the experiences in the private sector.

The other representatives of the government do not see computer security in technological terms either. Better technology was almost never mentioned as a solution to the problems of computer-related crime and abuse. In fact, the government witnesses almost all stressed that computer security is a management problem.

These statements run counter to the information we usually get. We are often told, even in government regulations, that technical personnel, especially system programmers, are a big threat. Mr. Courtney, at least does not believe this.

> "The technically competent personnel do often have capability for doing great harm, but they very rarely do. ... Of several hundred cases involving dishonest employees with which I am intimately familiar, only seven were committed by technical personnel. Of these several hundred cases, I do not know of a single one which did not go to prosecution for want of appropriate legislation."

The dissenting voice in this otherwise widespread agreement about the sources of computer crime comes from Mr. Criscuoli, who sees a growing conspiracy.

> "The picture of the lone computer thief, armed with the knowledge of modern science and motivated by the challenge of beating the system, is devoid of reality. The lone thief poses only a secondary threat to our computer systems. The real and serious threat comes from the professional criminal. ... Studies of computer-related crime indicate that [the] professional criminal has demonstrated an uncanny ability to identify weaknesses in the system and therefore circumvent security measures. A well-organized conspiracy by professional computer criminals can pose a serious threat to an organization's computer system. ... Organized crime also causes serious concern. ... Another threat to computers (often overlooked) is terrorism."

The Hackers

Three hackers testified during the hearings. The first witness was Neal Patrick, a seventeen year old senior at Rufus King High School in Milwaukee. He was followed by Geoffrey Goodfellow who now works at SRI International. The opening of the Senate hearings included Susan Headley, also known as Susan Thunder, from California.

Two interesting points emerged: the ethical question of the propriety of using other people's computers, and the question of intent to defraud. Most hackers do not believe that there is anything wrong with benign exploration of a computer system, whether they are authorized to use it or not. For example, Neal Patrick was asked when he was first aware that he had done something wrong. His answer was, "when the FBI showed up at my door."

When Susan Headley was questioned by Senator Cohen about the activities of the group she participated in, she stated that they had access to credit information, that they had changed credit ratings, and that they had shut down portions of the telephone system. Asked whether she ever thought any of this might be illegal, she responded that the group wasn't after material gain and that the question had never been raised.

Geoffrey Goodfellow, a "reformed" hacker now employed at SRI International, exhibits the same basic feelings in his testimony. While he states the he deplores the unsanctioned entry and "rummaging" of computer systems, he also places most of the responsibility on the operators of computer systems. For example,

> "...computer site administrators are not taking reasonable and prudent measures to protect their computer systems from even the most casual methods of circumvention. ... The way I view 'reasonable and prudent' measures of protection from the *casual* penetration is by drawing a paradigm with the way DoD classified information is handled.
>
> With respect to the handling and use of classified information, it is the responsibility of the organization to which you belong, in conformance with DoD guidelines, to provide you with rules and regulations in the handling of information. It is also the responsibility of your organization to provide you with a safe place (i.e. a vault) to store said information and to provide adequate safeguards (such as alarm systems, security personnel and patrols) to prevent unauthorized access.
>
> The same methodology should be taken to heart by administrators of computer systems. It's their

responsibility to provide reasonable and prudent measures to prevent unauthorized access attempts from gaining access to the system."

Mr. Goodfellow went on to note that system users also have a responsibility to protect sensitive information. He then stated his belief that we should train our children that entering someone's computer system unbidden is as bad as entering someone's house. The point is that today this is not seen as unethical.

Young people are not the only ones who are confused about the ethics of hacking on other people's systems. It appears that we are all uncertain. Several witnesses and members of congress viewed the 414's activities as being analogous to joyriding. Others felt that an unprotected computer is an attractive nuisance. Representative Carney of New York, during his questioning of Jim McClary, indicated that he saw no difference between the actions of the 414s and those of an authorized user who keeps a football pool on the computer. These views, which are all somewhat different, suggest that we have not yet had time to develop ethical standards in this new area. If we cannot agree about which activities are wrong, it is very hard to see how we will write suitable legislation.

The other interesting point that emerged from the hearings concerns malicious intent. The federal statute most widely used in the computer crime area is interstate fraud by wire. In order to successfully prosecute a case using this law, the prosecutor must show an intent to defraud. This requirement is also present in most of the proposed legislation. The hackers, in explaining what they do, universally claim that they have no malicious intent. They simply want to learn, to find out what computers are out there and how to get into them. In many cases, particularly through Telenet access, they don't even know whose computer they have accessed. It will not be easy to convince a jury that someone who doesn't know whose computer he is using set out with an intent to injure the owner of the computer.

Proposed Remedies

Six bills have been introduced in the House of Representatives to attempt to solve "the computer crime problem." They are listed in Appendix II together with brief descriptions.

Several of these bills are very similar in language and intent. H.R.1092, H.R.4259, and H.R.4384 all modify title 18 of the U. S. Code to criminalize acts committed on or with a computer which are intended to harm the owner of the computer. These bills do not contain a clause covering trespass, and, so, would not have helped in prosecuting acts like those of the 414s. The criminal titles of these bills have been discussed earlier in the section on definitions.

H.R.4384 and H.R.4259 also have additional titles. Both would establish computer security research grant programs in the Department of Commerce, and both would establish an Interagency Committee on Computer Fraud and Abuse. The committee would be chaired by the Attorney General and would include the Secretaries of Commerce, Defense, and Treasury, the Chairman of the Federal Communications Commission, and the Director of the Federal Bureau of Investigation. It would act as a clearinghouse in compiling statistics on computer fraud and abuse and information on protective techniques. It would also be responsible for coordination of all federal computer security research and development, and it would make recommendations to federal departments and agencies for improving the security of federal computer systems. This section was opposed by Mr. Keeney (Department of Justice).

H.R.3075 is directed entirely toward small business. It directs the Administrator of the Small Business Administration to establish a "Small Business Computer Crime and Security Task Force" and a resource center within the Small Business Administration. The resource center would keep small businesses informed about the perils of computing, and would do other things suggested by the task force. The task force would define the nature and scope of computer crimes committed against small businesses, evaluate the effectivness of state legislation and available security equipment, and help the National Bureau of Standards develop guidelines for computer security in small businesses.

H.R.3075 has no criminal section, but it does define computer crime as

"(I) any crime committed against a small business concern by means of the use of a computer; and

(II) any crime involving the illegal use of, or tampering with, a computer owned or utilized by a small business concern.

The bill takes what may be the most reasonable way out of the definition problem by not attempting to define terms like *computer*.

H.R.3570 is aimed primarily at combatting credit card fraud. However, almost as an afterthought, it prohibits "use of a computer with intent to execute a scheme to defraud." Like H.R.3075, it includes no definitions of *computer* or *use*.

H.R.4301 is by far the simplest of the proposed legislation. It includes no definitions, but does manage to exclude most calculators and embedded processors. It provides that:

"Whoever willfully uses a computer capable of being programmed and reprogrammed in the course of normal operations, in a manner not authorized by the owner of that computer, shall, ... in addition to any other punishment provided for the course of conduct ..., be fined not more than $100,000 or imprisoned not more than ten years, or both. ... the court shall not suspend the sentence ... or give ... a probationary sentence, nor shall the term of imprisonment run concurrently..."

Mr. Keeney stated that the Justice Department prefers the approach taken in H.R.1092, which amends a different portion of title 18, to the approach taken in this bill.

Several witnesses suggested the formation of a National Commission similar in nature to the Privacy Protection Commission created by the Privacy Act of 1974. While this seems to be a prescription for studying the problem rather than doing anything about it, it may be the best course of action at present. We have not achieved anything like a consensus about or even whether there is a problem, and the proposed legislative remedies all seem to have severe defects. A National Commission might be able to define a problem to be solved and propose some legislation to solve it.

Prognosis

The first session of the 98th Congress included more activity on computer crime than has previously occurred. However, this does not mean that legislation will result. The Subcommittee on Civil and Constitutional Rights of the Committee on the Judiciary in the House of Representatives held hearings on the last day of the session. These hearings covered bills H.R.1092, H.R.4384, and H.R.4301.

The most interesting testimony came from Representative Glickman who chaired the previous three days of hearings in the House. His summary of the previous hearings was that

the subject is extremely complex involving questions of privacy and proper management as well as vulnerabilities in systems. He urged caution, saying that the Congress should not attack the problem piecemeal. He stated that Office of Management and Budget leadership is "terribly weak", that we need to take another look at privacy and wiretapping laws, and advocated a national commission to study problems of privacy and system vulnerability.

Mr. Glickman did conclude that there is a real problem to be solved: the abuse of information. However he felt that the current bills merely scratch the surface of the problem by concentrating on the instrumentality of the abuse rather than the abuse itself.

The witnesses from the executive branch were not particularly supportive of any of the legislation. For example, Mr. Keeney from the Department of Justice said that the government feels some sense of urgency and has a task force at Justice which is studying the problem. They believe that legislation is needed and plan to make a recommendation but they have not yet reached a decision.

The Congress has been considering bills on computer crime since Senator Abraham Ribicoff introduced his bill, S.1766, in 1977 in the 95th Congress. The current H.R.1092 is very similar to Senator Ribicoff's original bill. None of these bills has received favorable action in committee, and it does not seem likely that the 98th Congress will act on any of the pending legislatic . Given the lack of support by the executive branch, and the defects in the legislative proposals, this may be the right thing to do. In any case, protection is still our responsibility, and we cannot expect any new legal tools soon.

APPEN' IX I

Hearings on computer crime were held by two committees of the House of Representatives and one committee of the Senate during the first session of the 98th Congress. The hearing dates and witness lists are shown below.

House Committee on Science and Technology, Subcommittee on Transportation, Aviation, and Materials

September 26, 1983 Witnesses
- Neal Patrick
  Computer Enthusiast
  Wisconsin
- Jim McClary
  Division Leader
  Operational Security and Safeguards
  Los Alamos National Laboratory
- Donn Parker
  Senior Management Systems Consultant
  SRI International
- Geoffrey Goodfellow
  SRI International
- Steve Walker
  Trusted Information Systems

October 17, 1983 Witnesses
- Joseph Wright
  Deputy Direct'
  Office of Management and Budget
- Warren Read
  Direct r
  Information Management and Technology
  General Accounting Office
- John Lyons
  Acting Director
  National Bureau of Standards
- Melville Klein
  Director
  Department of Defense Computer Security Center
- Floyd Clarke
  Deputy Assistant Director
  Federal Bureau of Investigation
- Richard Shriver
  Assistant Secretary
  Department of the Treasury

October 24, 1983 Witnesses
- Willis Ware
  The Rand Corporation
- Gen. Jack Hancock
  Senior Vice President
  Wells Fargo Bank
- Julius Cohen
  Director of Technology
  Grumman Aerospace Corporation
- Robert Morris
  Bell Laboratories
- Elmer Clegg
  Vice President
  Honeywell Information Systems

Senate Comittee on Governmental Affairs, Subcommittee on Oversight of Government Management

October 25, 1983 Witnesses
- Susan Nycum
  Partner
  Gaston Snow & Ely Bartlett
- Susan Headley
  Computer Enthusiast
  California
- Robert Courtney
  President
  Robert Courtney, Inc.
- E. J. Criscuoli
  Executive Vice President
  American Society for Industrial Security

October 26, 1983 Witnesses
- Joseph Wright
  Deputy Director
  Office of Management and Budget
- Richard Kusserow
  Inspecter General
  Department of Health and Human Services
- Warren Reed
  Director
  Information Management and Technology
  General Accounting Office
- John Keeney
  Deputy Assistant Attorney General
  Department of Justice
- Richard Shriver
  Assistant Secretary
  Department of the Treasury
- John Lyons
  Acting Director
  National Bureau of Standards

House Committee on the Judiciary

November 18, 1983 Witnesses
- Representative Dan Glickman
- Representative Bill Nelson
- Representative Dan Mica
- Representative Lawrence Coughlin

- John Keeney
  Deputy Assistant Attorney General
  Department of Justice
- Floyd Clarke
  Deputy Assistant Director
  Federal Bureau of Investigation
- James Falco
  Florida State Attorney

APPENDIX II

Six bills have been introduced in the 98th Congress dealing with computer crime. They are briefly described below. The designation *H.R.1092* means the 1092nd bill introduced in the House of Representatives during the current session. S.1733 refers similarly to a bill introduced in the Senate.

1. S.1733 and H.R.1092, the Federal Computer Systems Protection Act, introduced by Senator Paul Trible and Representative Bill Nelson. This bill would amend title 18 of the U. S. Code to make a crime the use, for fraudulent or other illegal purposes, of any computer owned or operated by the United States, certain financial institutions, and entities affecting interstate commerce.

2. H.R.3075, the Small Business Computer Crime Prevention Act, introduced by Representative Ron Wyden. This bill would amend the Small Business Act to establish a Small Business Computer Crime and Security Task Force.

3. H.R.3570, the Counterfeit Access Device and Computer Fraud Act of 1983, introduced by Representative William Hughes. This bill would amend title 18 of the U. S. Code to provide penalties for the counterfeiting of access devices (credit cards) and provide penalties for computer frauds.

4. H.R.4259, the Computer Fraud Prevention and Home Computer Promotion Act of 1983, introduced by Representative Dan Mica. This bill would establish a computer security research program and an Interagency Committee on Computer Crime and Abuse, provide criminal penalties for computer abuse, and provide a credit against income tax for computers purchased by individuals for educational, professional, and other nonrecreational purposes in the home.

5. H.R.4301, introduced by Representative Lawrence Coughlin. This bill would amend title 18 of the U. S. Code to provide penalties for computer related crime.

6. H.R.4384, the Computer Fraud Prevention Act of 1983, introduced by Representative Dan Mica. This bill would establish a computer security research program and an Interagency Committee on Computer Crime and Abuse, and provide criminal penalties for computer abuse.