94165

SMALL BUSINESS COMPUTER CRIME PREVENTION ACT, H.R. 3075

HEARING

BEFORE THE

SUBCOMMITTEE ON ANTITRUST AND RESTRAINT OF TRADE ACTIVITIES AFFECTING SMALL BUSINESS

OF THE

COMMITTEE ON SMALL BUSINESS
HOUSE OF REPRESENTATIVES

NINETY-EIGHTH CONGRESS

FIRST SESSION

WASHINGTON, D.C., JULY 14, 1983

Printed for the use of the Committee on Small Business

94165

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON : 1983

COMMITTEE ON SMALL BUSINESS

PARREN J. MITCHELL, Maryland, *Chairman*

NEAL SMITH, Iowa
JOSEPH P. ADDABBO, New York
HENRY B. GONZALEZ, Texas
JOHN J. LaFALCE, New York
BERKLEY BEDELL, Iowa
HENRY J. NOWAK, New York
THOMAS A. LUKEN, Ohio
ANDY IRELAND, Florida
IKE SKELTON, Missouri
CHARLES W. STENHOLM, Texas
ROMANO L. MAZZOLI, Kentucky
NICHOLAS MAVROULES, Massachusetts
CHARLES HATCHER, Georgia
RON WYDEN, Oregon
DENNIS E. ECKART, Ohio
GUS SAVAGE, Illinois
BUDDY ROEMER, Louisiana
NORMAN SISISKY, Virginia
FRANK McCLOSKEY, Indiana
ESTEBAN EDWARD TORRES, California
TOM J. VANDERGRIFF, Texas
JIM COOPER, Tennessee
JAMES R. "JIM" OLIN, Virginia
C. ROBIN BRITT, North Carolina
RICHARD RAY, Georgia

JOSEPH M. McDADE, Pennsylvania
SILVIO O. CONTE, Massachusetts
WILLIAM S. BROOMFIELD, Michigan
LYLE WILLIAMS, Ohio
JOHN HILER, Indiana
VIN WEBER, Minnesota
HAL DAUB, Nebraska
CHRISTOPHER H. SMITH, New Jersey
DAVID DREIER, California
GUY V. MOLINARI, New York
TOBY ROTH, Wisconsin
GENE CHAPPIE, California
SHERWOOD L. BOEHLERT, New York
MICHAEL BILIRAKIS, Florida
DAN SCHAEFER, Colorado

MAJOR L. CLARK III, *Staff Director*
THOMAS G. POWERS, *General Counsel*
LOIS LIBERTY, *Publications Specialist*
RAYMOND S. WITTIG, *Minority Counsel*

SUBCOMMITTEE ON ANTITRUST AND RESTRAINT OF TRADE ACTIVITIES AFFECTING SMALL BUSINESS

THOMAS A. LUKEN, Ohio, *Chairman*

HENRY B. GONZALEZ, Texas
ROMANO L. MAZZOLI, Kentucky
FRANK McCLOSKEY, Indiana

VIN WEBER, Minnesota
GENE CHAPPIE, California

LAWRENCE E. SABBATH, *Subcommittee Staff Director*
DAVID K. REHR, *Minority Subcommittee Professional Staff Member*

CONTENTS

APPENDIX

SMALL BUSINESS COMPUTER CRIME PREVENTION ACT, H.R. 3075

THURSDAY, JULY 14, 1983

House of Representatives,
Subcommittee on Antitrust and Restraint
of Trade Activities Affecting Small Business,
Committee on Small Business,
Washington, D.C.

The subcommittee met, pursuant to notice at 9:45 a.m., in room 2359–A, Rayburn House Office Building, Hon. Thomas A. Luken presiding.

OPENING STATEMENT OF CHAIRMAN LUKEN

Mr. Luken. This meeting of the Antitrust Subcommittee of the Small Business Committee will come to order.

We are here to take up the subject of small business computer crime, and with us today is the gentleman from Oregon, Ron Wyden, who has introduced the bill which we will consider, H.R. 3075.[1] There have been widespread reports in the media and also here on the abuse of computers.

Our witnesses today, which will be a cross section of those who have information and expertise on the subject, have indicated to members of the committee that losses from the white collar crime in this area are at least $100 million per year and could range as high as $1 billion. That is probably a gross underestimate, and it is certainly an underestimate of the potential for abuse as the use of computers increases and the technology advances.

It is evident that the scope of these crimes is not fully known. The importance of H.R. 3075 is not to attach a penalty to computer misuse, because we are somewhat skeptical as to whether we are at the point where we can define the crime and the remedy at this time.

Therefore, the purpose of H.R. 3075 is to determine the size of the problem, particularly as it affects small business. This Nation's small businesses do not have the ability today to respond to computer crime in the way that larger enterprises can. H.R. 3075 requires the Administrator to establish a task force of private and public sector members to develop guidelines for small enterprises to evaluate the security of their systems; this bill also provides for an SBA resource center to evaluate information on this subject to small business. We will proceed with the hearing, but first I would

[1] See p. 61.

like to call upon the author for any statement that he might want to make in introducing the bill, and these hearings.

Mr. WYDEN. Mr. Chairman, I would very much like to make an opening statement, but our colleague, the gentleman from Minnesota, is on a very tight schedule. I am very appreciative of the assistance, help and support he has given us with this legislation, so if the Chair would permit, let me yield to him.

OPENING STATEMENT OF HON. VIN WEBER, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MINNESOTA

Mr. WEBER. I thank the gentleman for yielding, and I won't take up a lot of the committee's time. I do have a conflict, unfortunately, at 10 o'clock, but I did want to come to say that I appreciate the efforts of the gentleman from Oregon in introducing H.R. 3075, which addresses a very real and serious problem. I will look with great interest at the transcript of the hearing today, because I do think we need more information on the exact scope of the problem and how to deal with it.

One thing seems fairly clear, though. This situation is fairly typical of a lot of small business problems. Measures to protect companies from computer crime are available but as is so often the case, the costs are prohibitive to small businesses. We find a situation where larger companies are able to protect themselves if they choose to do so, but the costs both in terms of money and expertise are too great for many of our small businesses. The legislation introduced by my colleague Mr. Wyden is a positive step forward in terms of addressing that need, and I am very supportive of your efforts. I look forward to being helpful on the bill, and I am sorry that I can't stay for the hearing today. I thank the gentleman for yielding.

OPENING STATEMENT OF HON. RON WYDEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OREGON

Mr. WYDEN. I thank the gentleman for his willingness to work with us. This is going to be a bipartisan effort. As the gentleman says, this is an area where large business frequently has few problems yet small business is quite another story. I know the gentleman's schedule is tight and I want to thank him again for taking the time to come.

I also want to express my appreciation to the Chair, the gentleman from Ohio as well. I know his schedule is extremely busy and they tell me a couple different subcommittees of the Commerce Committee are meeting virtually around the clock at this point, and I very much appreciate the Chair making time for us to have this hearing.

According to the legislative stopwatch around here we would like to have this bill on a fast track, and Mr. Chairman, I very much appreciate your giving us a chance to move this bill with an expeditious hearing.

Now anyone who has seen the movie "War Games" knows that infiltration of computer systems is no game at all. Pac Man, Donkey Kong, and Space Invaders are amusing pastimes for countless Americans. Data diddling, trapdoors, Trojan horses, superzapping, these are the tricks of the trade for computer criminals, but they are not amusing for small business and they are inflicting American businesses with massive losses every single year.

Part of the reason for these huge losses is that computer crimes are hard to detect and they are even harder to prevent. It is estimated that for every 1 computer crime detected that 99 go unnoticed. Businesses large and small are often reluctant to report computer crimes because they fear that there will be an erosion in their public trust. As a result, the opportunity for low-risk, high-yield crime is growing in this country as computer use becomes more widespread. In short, we have got a very serious problem on our hands, and all the signs indicate that it is going to get worse, which is why I have introduced H.R. 3075, the Small Business Computer Crime Prevention Act. This legislation is a practical attempt to protect this country's small businesses from what threatens to be one of the biggest businesses in the future, the underground industry of computer crime.

My legislation takes several steps in addressing this problem. First, it directs the Administrator of the Small Business Administration to establish a task force charged with outlining the scope of the problem and how it affects small business.

In addition, it directs the SBA to establish a clearinghouse so we can get out, all over this country, information to small business on the subject of computer crime. It also directs the SBA to develop guidelines that can support small business security efforts.

Now I would like to clarify several aspects of this legislation, what it means and what it doesn't mean. Now we are not asking the task force to reinvent the wheel. That is why the bill stipulates that the task force would be comprised of experts from the public and private sector who are already familiar with the technical and managerial components of information security.

Now I am aware that extensive research has been done on the general problem of computer crime in this country, but to the best of my knowledge, little has been done on the problem of computer crime as it affects small business. I think there are few mechanisms available to get practical information to small businesses so they can insure the integrity of their businesses in the most cost-effective manner possible.

One technical correction that I would like to make in the bill at some point, Mr. Chairman, is to cut the time for the task force's report. Instead of having it submitted 3 years after the bill's passage, I think we can easily make that 18 months.

The problem of information security is obviously not limited to just small business, yet small businesses for several reasons are uniquely handicapped in this area.

First, small businesses almost always have fewer in resources than larger firms, yet their vulnerability is often just as great, if not greater. The limited resources usually mean fewer and less specialized employees, which reduces the division of duties among departments and employees, one of the main defenses against losses by crime or mistake.

Second, smaller businesses tend to use smaller computer systems, which by and large have fewer, more limited security features designed into the system. Moreover, small businesses sometimes have little control over the bulk of the information system they employ. They usually lease their phones and communication lines. Often they lease or use time-shared computers owned by others, and many use packaged software that is bought off the shelf. This dependence puts comprehensive knowledge of computer security out of the reach of most small businesses.

Another factor is that small businesses are less able to absorb the losses of a computer crime than are the larger firms. An example is the small firm that was victimized by a dismissed employee. Before he left, the employee programed the company's computer to cancel its accounts receivable—6 months after he was gone. Half a year later the company found itself with no record of who owed it money and despite placing advertisements in the local paper, the company was forced to close its doors.

Finally, I would like to point out that we are talking about more than just cash flow losses. Inventories, personnel records, contract bid information, long-range company plans and programs, all of these can fall victim to the high-tech infiltrator.

Now this legislation is certainly not going to bring an end to all the computer abuse in this country, all the fraud and various ripoffs, and it is not going to put anybody behind bars. What it will do is give us a chance to engage in what is needed most—a preventive, active approach, rather than one that is reactive. It attempts to curb the keyboard criminal by providing small businesses with practical information about the unique threat that is posed by computer crime.

In that way, we will be able to aid small businesses in the development of safeguards that are going to reduce the likelihood of their becoming a victim in the first place.

Mr. Chairman, again I am very grateful to you for making available this opportunity to have a hearing on this bill, and I look forward to our witnesses.

Mr. LUKEN. Well, I thank the gentleman from Oregon, and I congratulate him sincerely. I think this is a major move, one that is necessary and one which is tardy already. Certainly the gentleman has done a very advantageous thing for us all in moving at this time, and hopefully this bill will pass as will the gentleman's suggestion of abbreviating the time for getting the report back so that we can take action on it and the Nation can devote its attention to it.

We will, therefore, call the first witness, Mr. August Bequai.

Mr. BEQUAI. Mr. Chairman, good morning.

Mr. LUKEN. Do you have a statement, Mr. Bequai?

Mr. BEQUAI. Yes, Mr. Chairman, I do.

Mr. LUKEN. If there is no objection, that statement will be received into the record of this committee, and you may proceed in any way you think will be helpful.

Mr. BEQUAI. Thank you, Mr. Chairman.

TESTIMONY OF AUGUST BEQUAI, ATTORNEY

Mr. BEQUAI. Thank you, Mr. Chairman. Mr. Chairman, in conformance with your request, I am pleased to testify before this subcommittee on H.R. 3075.

Today, as you have indicated, computer-related crimes are a real and growing problem in this country, and I might add also in Western Europe and the Soviet bloc and other parts of the world. Annual losses in the United States alone are said to exceed at least $100 million. Some experts place these losses as high as $1 billion. The truth of the matter is that we really don't know the full scope of the problem.

Computer-connected crimes can take various forms. I will, just in brief, mention some in an effort to save time: sabotage, vandalism, theft of services, property-connected crimes, theft of information, financial crimes. Computers are also vulnerable to electronic-interceptive attacks. Those are listed in my written statement. Thus I will skim through them.

I might add that computer-connected crimes are a problem for every modern organization. Small businesses especially, as you have indicated, Mr. Wyden, are vulnerable. Unlike the corporate giants, they lack the needed resources to institute adequate computer-connected security safeguards. They also lack the in-house expertise to investigate computer-connected crimes.

In addition, small businesses lack the resources to retain the costly services of private consultants. I might add in addition our law enforcement apparatus especially at the local and State level is really ill trained to address as of this day computer-connected crimes, and the majority of States I might also add have not as yet enacted any computer-related legislation to address this problem. Prosecutors especially at the local and State level often find themselves relying on outmoded laws to bring, if you will, culprits before justice. At the Federal level, as you well know, we still as yet do not have a Federal computer crime bill. I might add thus that legislation will be necessary in this area to address computer-connected crimes, especially those involving interstate and foreign commerce.

I should point out, though, that the problem of computer-connected crime has no quick fix. We tend to be a quick-fix society, but in this case it is going to take an effort on various fronts. No one statute I might add can address the entire problem. We need to address, as I see it, several areas.

To date we have no accurate data on the scope and dimensions of the problem. Both the public and private sectors often sweep these crimes under the rug.

Training is another area that we must address. Law enforcement at every level, especially again at the local and State level, needs training in this area. Our police, prosecutorial, and judicial machinery, needs to be brought, if you will, into the modern electronic age.

The criminal sanctions, we need laws that specifically address this problem. At present, we find ourselves as I indicated oftentimes relying on old and outdated statutes. Now, H.R. 3075, as I see it, does constitute an effort to address some of the above. A task force could assist in defining the scope of the problem, especially as it impacts on the small businessman.

To date, no effort has been made, as you have indicated, Mr. Wyden, to address the problem of computer-connected crimes in the area of small businesses. The task force can also recommend some guidelines to encourage small businesses to safeguard their computers from criminal attack. However, I should point out that we should take steps to insure that the task force does not turn out to be, as is unfortunately sometimes common in Washington, just another drain on the taxpayers' limited resources. We should guard, and I think, Mr. Chairman, you pointed out this, against unnecessary studies and an army of consultants ready to offer their services.

We are increasingly becoming a cashless society. No business today can long survive without the assistance of computer technology. Likewise no business can long survive if its computers fall prey to criminals.

In closing, Mr. Chairman, I would like to thank you and your staff for offering me the opportunity to present this brief testimony, and I will be happy to answer any questions you might have.

[Mr. Bequai's prepared statement follows:]

Prepared Statement of August Bequai, Attorney

Mr. Chairman, in conformance with your request, I am pleased to testify before this Subcommittee on H.R. 3075 (the "Small Business Computer Crime Prevention Act"). Having authored five books, and more than 40 articles in the areas of white collar and computer crime, and having also lectured at many law enforcement and academic institutions on these topics, hopefully I can expand on some of the comments offered on this legislation.

Today, computer-related crimes are a real and growing problem in the United States. Annual losses to the private sector alone are said to exceed $100 million; some experts place these losses as high as $1 billion. However, the truth of the matter is that at present, we do not know the full scope, or dimensions of the problem.

Computer-related crimes can take numerous forms. Some of the more common are as follows:

Sabotage and vandalism.—Both are common and easily perpetrated. These usually involve a physical attack against the entire computer system or any of its subcomponents. These attacks can be motivated by political ideology, or by a perceived grievance of an employee. The more common motive, however, is economic. For example, a competitor may sabotage another's system so as to gain an economic advantage. Sabotage and vandalism may also occur in labor-management disputes when irate employees revert to destructive attacks against an employer's property.

Theft of services.—These usually involve the unauthorized use of someone else's computer. For example, a dishonest employee may use his employer's computer to keep track of his personal investments.

Property crimes.—These involve the theft of merchandise and other property through the use of a computer. A thief, for example, can use a firm's computer to place orders for various merchandise and have that property delivered to selected locations.

Data crimes.—These usually involve the copying of mailing lists and printouts, or the theft of programs and other valuable data.

Financial crimes.—In these instances, the computer is manipulated to aid the wrongdoer in perpetrating (sometimes complex and sophisticated) financial swindles. For example, a dishonest employee can direct payments to phony suppliers, ghost employees, and others.

Computers are also vulnerable to electronic interceptive attacks. For example:

Wiretaps usually involve connecting a tap directly to the telephone or teleprinter lines of a computer, in order to intercept and record messages.

Buggings, a criminal can place a bug in a computer facility.

Browsing involves the introduction of an unauthorized terminal into a system that does not authenticate terminal entry.

Piggyback entry involves the interception of messages from the computer to the user of the system. Data is added, altered, or deleted, and passed on to the user.

Computer-related crimes are a problem for every modern organization; small businesses, especially, are vulnerable. Unlike the corporate giants, they lack the needed resources to institute adequate computer security safeguards. They also lack the in-

house expertise to investigate computer-related crimes. In addition, small businesses lack the resources to retain the costly services of private consultants.

Further, because our law enforcement agencies have long neglected the problem of computer-related crime, the small businessperson can find little assistance from these sources. In addition, the majority of our states have not enacted, to date, any computer-related legislation to address the problem. Prosecutors are often forced to rely on outmoded laws. We fare no better at the Federal level; legislation will be needed to address computer-related crimes that involve interstate and/or foreign commerce.

It should be pointed out, however, that the problem of computer-related crime has no "quick fix." No one statute can or will address the entire problem. We need to address the following areas:

Scope of the problem.—To date, we have no accurate data on the scope and dimension of the problem. Both the private and public sector often sweep crimes "under the rug."

Training is needed.—Law enforcement at every level needs training in this area. Our police, prosecutorial, and judicial machinery needs to be brought into the modern electronic age.

Criminal sanctions.—We need laws that specifically address this problem. At present, we find ourselves relying on old and often outdated statutes, to tackle the electronic criminal. Once the defense bar becomes more versed in this area, we should witness growing and costly litigation in this area.

H.R. 3075 constitutes an effort to address part of the above. A Task Force (as detailed in this legislation) could assist in defining the scope of the problem as it impacts on the small business. To date, no effort has been made to address this specific area. It could also recommend guidelines to encourage small businesses to safeguard their computers from criminal attack. However, we should ensure that the Task Force does not turn out to be (as is common in Washington, D.C.) just another drain on the taxpayers' limited resources. We should guard against unnecessary studies and an army of consultants, ready to offer their services.

We are increasingly becoming a cashless society. No business can long survive in the coming years without the assistance of computer technology. Likewise, no business can long survive if its computers fall prey to criminals.

Mr. Luken. The gentleman from Oregon.

Mr. Wyden. Thank you, Mr. Chairman. Mr. Bequai, thank you very much for your excellent testimony and for the cooperation you have given my staff on this issue. I just have a couple of short questions.

Now in your testimony you state that we have got no accurate data on the scope and dimension of the computer crime problem in this country. Could you explain the reason that that is the case?

Mr. Bequai. Well, when you get into the area of white-collar crime in general, Mr. Wyden, as you well know, corporate America is rather reluctant to come forth and show its linen. When companies get taken if you will, whether they be small or large, and I have some such clients, they oftentimes are very reluctant to come forth and say I have been taken. They are fully aware of the fact that law enforcement in America is ill prepared to address the problem. Who do you go to? The county police? I can safely tell you, having had occasion to train people at that level, they are not really prepared to investigate white-collar crimes, especially I might add in computer-connected crimes. If you go to the State police you are going to run oftentimes into the same problem.

At the Federal level, with the exception of some special sections of the FBI and the Secret Service, we really don't have any training, so there really is no inducement for the businessman, whether he or she is small business or large, what have you, to come forth and say I have been taken, so it is going to be pretty difficult to develop data if your victims are rather reluctant to come forth.

We have estimated, educated estimates from the U.S. Chamber of Commerce, other private groups, but I think it is fair to say, and I think you will find that the other witnesses coming after me will agree with me, that we really don't have a handle on the figures.

Mr. Wyden. In your opinion, is the problem of computer crime going to increase in the years ahead? What is the prognosis for the years ahead?

Mr. Bequai. The prognosis is it is going to get worse before it gets better. I was in Europe a couple of months ago and I met with attorneys of the major European corporations and they agree with my prognosis, and Europe is starting to look bad, too. It is going to get worse before it gets better if we don't bring the law enforcement apparatus into the 20 century, and I especially stress the local and State apparatus, or we in the Federal system, we are going to be in trouble.

Mr. Wyden. Do you think that the research and the education efforts that are under way now are an adequate response to the problem?

Mr. Bequai. I very candidly don't really see any training at the local and State level right now, very little if any. I see some training at the Federal level, but I don't really see any money going at the State and local level to train law enforcement, and by that I throw in police agencies, prosecutors and what have you. In fact, the word that I hear is that funds have been cutoff at the local level, pretty much so, so I don't really see much happening today in this area.

Mr. Wyden. Just a couple of other quick questions, Mr. Chairman.

Do you know of any individual or group or anybody or any institution that has done a real analysis of what computer crime means to small business?

Mr. Bequai. I really don't know, no.

Mr. Wyden. The last one is are you aware of any individuals or company who has been taken to court for its failure to adequately secure their computer system?

Mr. Bequai. No, absolutely not. I don't know of any company. Civil or criminal? I mean I take it you mean both.

Mr. Wyden. We have heard some discussion that this was the case, and you are considered something of a guru in this area.

Mr. Bequai. You mean a victim being taken to court for failing to take adequate safeguards? Perhaps if one searches the literature you might find cases where victims may have been, if you will, sued, but not by the Government certainly. I don't know of any Government cases. I have stockholders, things of that sort.

Mr. Wyden. Thank you, Mr. Chairman.

Mr. Luken. Mr. Bequai, I have a feeling that you know a lot about this subject and I feel a little inadequate because of my limited knowledge of the technology to even try to bring it out in the form of questions. The gentleman from Oregon is knowledgeable, and I will invite him to continue the colloquy as we go along, at least for a few minutes longer. You listed here some of the common forms: sabotage and vandalism, theft of services, property crimes, data crimes and financial crimes.

I suppose data crimes is one of those that in the future will be expanding, one that we have difficulty even envisioning now?

Mr. Bequai. Yes, Mr. Chairman. You are right.

Mr. Luken. Will you describe that?

Mr. Bequai. Especially as we increasingly go into the electronic funds transfer system. Sure. Information as political scientists tell me is power, and he or she who controls the flow of information pretty much controls power.

I think it is fair to say that as we increasingly become an electronic cashless, paperless society, we are going to see more and more informational-connected crimes, like thefts of data, thefts of all sorts of things, mailing lists, confidential corporate secrets, trade secrets, everything from a to z, and the sad thing is right now it is pretty difficult really to prosecute some of these cases, and even when you do prosecute them, the courts and juries really don't lose much sleep over someone who has stolen corporate secrets.

Mr. Luken. As a former prosecutor, my experience is that white-collar crime has always been exceedingly difficult to define. It is relatively easy to define crimes of assault and burglary. We all learned in the first year of law school about felonious entry and things of that nature, but whenever we get into the white collar crime area there is difficulty. For example, currently there is a good deal of publicity about an item out of the White House. Whether that would be a theft——

Mr. Bequai. The Carter papers.

Mr. Luken. Of course; the debate situation, if that ever gets anywhere from the standpoint of a criminal action, it will be pretty difficult for those authorities to try to sift out what is a crime. What we are talking about here is fraught with all of those difficulties plus all of the unknowns and the complexities, but the mere fact that it is complex is not a reason to avoid it, or to cop out on the subject, and I congratulate the gentleman from Oregon for tackling it.

I think it is extremely important that we attempt to define it, and some of it can be defined. You have just mentioned the electronic transfer of funds. There will be a fantastic amount of money involved. Are you talking about embezzlement, too, when you say common theft of services? Would that be employees involved in that form of embezzlement?

Mr. Bequai. Sure. Most of these capers oftentimes involve insiders, employees.

Mr. Luken. There aren't any fingerprints on this.

Mr. Bequai. Well, there oftentimes can be, invisible if you will. You are not going to find a cadaver or find fingerprints. You are not going to find a smoking gun, things of that sort.

Mr. Luken. No corpus delecti?

Mr. Bequai. No. I might add, let me throw this figure out, Mr. Chairman, because I know of the concern for white-collar crime. When we talk about white-collar crime, I think it is important to point out we are talking about more than $40 billion a year. Regarding computer-connected crimes, the category of white-collar crime, if you look at the overall package you are talking about more than $40 billion, and I think it is fair to say they can easily employ computer technology to pull the old embezzlement, the old stock fraud schemes, all sorts of things, so your technology also lends itself as a vehicle to commit massive white-collar crime which can certainly easily tax the energy of local law enforcement and State law enforcement.

Mr. LUKEN. I assume that there isn't an acceptable universal definition of computer crime that you know of?

Mr. BEQUAI. No, there is none. I might add there is not to my knowledge an acceptable definition of organized crime either, but it does exist, and the same thing with computer crime.

Mr. LUKEN. There certainly isn't any that I know of, but perhaps organized crime is more nebulous than computer crime. With computer crime, after all, we do know what the technology is. With organized crime it is just a term. We can't agree on it. I think we can agree on what computer crime is if we can come to the same level of understanding, which is what the gentleman's bill is intending to do.

What comments do you have on that?

Mr. BEQUAI. I thought it was a good bill. I don't think, by the definitional aspect I don't mean the people out there, law enforcement, lawyers and what have you, that we are ignoramuses, we don't have an idea of what computer-connected crimes is. We do.

The point I am making is we don't have a one-paragraph definition that we all agree on, but we have a pretty good idea of what it is and how they are committed.

Mr. LUKEN. Do you have any recommendations regarding the legislation?

Mr. BEQUAI. Well, I would strongly support any effort to take a look at the problem. I would strongly support any efforts that would address the plight of the small business person in this area. I think it is fair to say that the large corporations, I think Mr. Wyden pointed out and I agree with him, have less of a problem if you will. They can retain the services of consultants. They can retain the services of investigators. They can buy the necessary equipment. If they fail, they fail for lack of will, not for lack of resources, whereas the small businessperson oftentimes fails for both, sometimes lack of will, and oftentimes lack of resources, so I think this bill would probably address some of the needs of the small business community.

Mr. LUKEN. Of course, perhaps a little aside the point, but the basic fact about computers is centralizing and synthesizing the information. This would make the large businesses vulnerable at least from time to time also, wouldn't it?

Mr. BEQUAI. Well, they certainly are vulnerable.

Mr. LUKEN. There might be numerous experts, but you end up with relatively few people who have all of the information within the few companies that they control.

Mr. BEQUAI. Sure, and I might add large corporations are not monoliths. Oftentimes you find the right hand doesn't know what the left hand is doing. At least that has been my experience, so they have the same problem, yes.

The only point I was making is that they do have resources that the small business community does not, and that is why I think H.R. 3075 would prove of assistance to the small business community.

Mr. WYDEN. Thank you, Mr. Chairman. Just a couple of other brief questions. Do you think, Mr. Bequai, that there is enough general awareness among small business that this is a problem right now?

Mr. BEQUAI. No, I don't think so, not from the literature I read, not from the people that I talk to. I think they are aware of the fact that there is a problem if you will, but I don't really think they fully understand the scope, the dimensions, and frankly oftentimes they are more concerned about the economics of the business.

Mr. WYDEN. So they usually find out after they run into a problem or after they have been taken?

Mr. BEQUAI. Exactly.

Mr. WYDEN. That was my general perception, too, so I think the first step of this whole undertaking has got to be an effort to try to just generally make people more aware of some basic things that can be done.

Mr. BEQUAI. I agree with that.

Mr. WYDEN. Now one of the things I wanted to ask you was, we put in place our task force. We generate some new awareness of the problem and small business knows that this is something they may be greatly interested in in the years ahead. A small businessperson, he or she might look up in the Yellow Pages under computer security or something else and they ask somebody to come out to the shop or something along those lines, and the person makes some recommendations and says do this, do that, do something else.

Would a small businessperson today, not knowing anything about the value of security services they were buying, couldn't they be totally taken? If you called somebody up and asked them to come out to your shop and recommend or couldn't they just be taken to the cleaners?

Mr. BEQUAI. That is a leading question!

Mr. WYDEN. Certainly. I apologize.

Mr. BEQUAI. I will go along with it, being a lawyer. I will say yes, you are absolutely right, and they would be taken to the cleaners six times over.

Mr. WYDEN. My perception is that you could have an idea where to look, but I think it is like a lot of technical areas, this one, of course, being of enormous importance. If somebody came out and told you A, B, or C, I think it would be very, very hard to judge the value of something like that.

Let me ask you one last one and let you go. Now in response to my first question you said we had no accurate data on the scope of the problem. The problem is going to certainly increase in the next decade. The research and education efforts aren't adequate, that you don't know of any group or person that is doing a study. Now that is a rather systematic analysis it seems to me of the problem. Is that essentially why you backed legislation?

Mr. BEQUAI. Yes, I think it is fair to say, and I agree with all the statements you made, sure.

Mr. WYDEN. I thank you very much for taking the time and for your help. It has been of great assistance. Mr. Chairman, at this point we just got a Federal Express——

Mr. LUKEN. Let's excuse Mr. Bequai first. You are getting on to another subject?

Mr. WYDEN. I was indeed.

Mr. LUKEN. Thank you very much, Mr. Bequai, and perhaps we can continue to work together as we move on in this. We are certainly very serious about it, and I hope that we will move the bill and/or something very akin to this bill, and we would look forward to your counsel as we move forward.

Mr. BEQUAI. Thank you, Mr. Chairman, and I would like to congratulate Mr. Wyden. I think any effort in this area is a positive step.

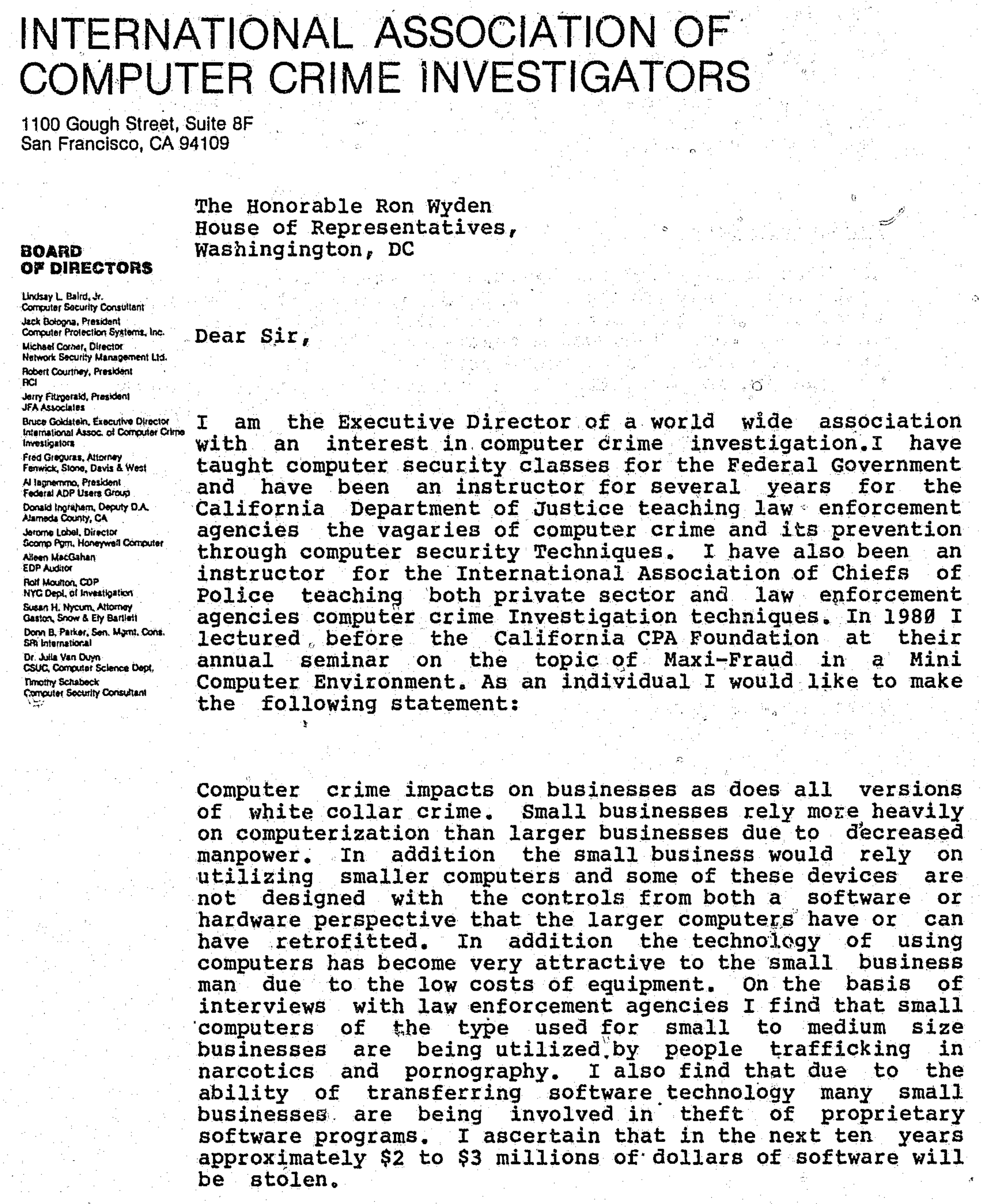
Thank you, sir.

Mr. LUKEN. All right. I recognize the gentleman from Oregon to introduce a document into the record. Is there any discussion which you may have on that?

Mr. WYDEN. Thank you very much, Mr. Chairman. Just very briefly, we got by Federal Express a letter from the International Association of Computer Crime Investigators from San Francisco, Calif. It is a very supportive letter of this legislation. I only ask that supportive letters be put into the record, and I would just ask unanimous consent that it could be introduced in the record.

Mr. LUKEN. Without objection, it will be. I had a chance to glance at it and I think the mere fact that there exists an organization called the International Association of Computer Crime Investigators, that there are other aspects to this movement for recognizing the need for action, and the document itself, the letter of support, will be accepted into the record.

[The letter from the International Association of Computer Crime Investigators follows:]



INTERNATIONAL ASSOCIATION OF
COMPUTER CRIME INVESTIGATORS

1100 Gough Street, Suite 8F
San Francisco, CA 94109

The Honorable Ron Wyden
House of Representatives,
Washingington, DC

Dear Sir,

I am the Executive Director of a world wide association with an interest in computer crime investigation.I have taught computer security classes for the Federal Government and have been an instructor for several years for the California Department of Justice teaching law enforcement agencies the vagaries of computer crime and its prevention through computer security Techniques. I have also been an instructor for the International Association of Chiefs of Police teaching both private sector and law enforcement agencies computer crime Investigation techniques. In 1980 I lectured before the California CPA Foundation at their annual seminar on the topic of Maxi-Fraud in a Mini Computer Environment. As an individual I would like to make the following statement:

Computer crime impacts on businesses as does all versions of white collar crime. Small businesses rely more heavily on computerization than larger businesses due to decreased manpower. In addition the small business would rely on utilizing smaller computers and some of these devices are not designed with the controls from both a software or hardware perspective that the larger computers have or can have retrofitted. In addition the technology of using computers has become very attractive to the small business man due to the low costs of equipment. On the basis of interviews with law enforcement agencies I find that small computers of the type used for small to medium size businesses are being utilized by people trafficking in narcotics and pornography. I also find that due to the ability of transferring software technology many small businesses are being involved in theft of proprietary software programs. I ascertain that in the next ten years approximately $2 to $3 millions of dollars of software will be stolen.

This is significant because the organizations that will be most affected will be those organizations that start up out of "garages" such as Apple Computer did. We are all aware of the great American dream that todays small business person has. That dream is one of becoming the next Atari or the next Visicorp. Both of these companies started up with very small capitalization.

Recommendations:

The technology and capabilities of small businesses are such that they could not afford to hire the personnel necessary to safeguard the assets that would reside in their computers. They would need some protection. I believe that your idea to study such problems has come of age. I commend you in your efforts on behalf on the small business community to create a task force of experts. The losses that could impact a small business from computer crimes such as embezzlement, or fraud could vastly decrease the total number of small businesses. I support your bill in its present form. I would like to be considered for the task force and lend whatever professional support I could offer.

In my role as the Chairman of the San Francisco Chamber of Commerce Crime Prevention Committee I found that small businesses are extremely vulnerable to all types of crime. The majority of business crimes can be dealt with Crime Prevention Units formed in local police departments, but some police departments are ill prepared to deal with computer crime on any scale.

Sincerely,

Bruce Goldst

Bruce Goldstein,
Executive Director

Mr. LUKEN. The next witness is Dr. Stuart Katzke of the Institute for Computer Sciences and Technology from the National Bureau of Standards. Is that correct, Dr. Katzke?

Dr. KATZKE. That is correct. Thank you.

Mr. LUKEN. All right. I believe we have a written statement from you, and without objection, it will be included in the committee hearing. We will ask you to proceed. We are interested in what you have to say, and we are not trying to suggest that you abbreviate it to the point, especially in this area where we all need education, that you don't tell us what we need to know.

TESTIMONY OF DR. STUART W. KATZKE, MANAGER, COMPUTER SECURITY MANAGEMENT AND EVALUATION GROUP, INSTITUTE FOR COMPUTER SCIENCES AND TECHNOLOGY, NATIONAL BUREAU OF STANDARDS, U.S. DEPARTMENT OF COMMERCE

Dr. KATZKE. Thank you. I am pleased to appear before you today to describe the National Bureau of Standards programs in computer security, and particularly those activities which may be of interest to small businesses.

Yes, I will excerpt from portions of my statement. Before I do that, I would like to comment on my concern this morning. When I came in here, I noticed the basic focus is on computer crime. Within our computer security and risk mismanagement program we consider computer crime only one aspect of the problem. We generally consider the computer security problem to include protecting the confidentiality of data, the integrity of data, and making sure that processing services as available so you can get your processing done in a timely way. Indeed you can lose confidentiality, integrity, or availability by both intentional acts which would include computer crime as well as accidental types of events. Very often, the same types of safeguards which prevent and detect computer crimes are effective for accidental events. In fact, some estimates indicate that accidental events that occur are even greater dollar-wise than computer crime is right now. I think it would be necessary for any task group, when it is formed, to make the small business people aware of the accidental types of problems, as well as, the computer crime aspects. With that in mind, I will talk a little bit about our computer security program, and, as I go through the specific areas of NBS' work, you might keep in mind that we have a much broader focus than just computer crime.

Mr. LUKEN. You say you have?

Dr. KATZKE. We do within the Institute of Computer Sciences and Technology.

Mr. LUKEN. What are they? Are you going to suggest that we broaden the areas that we are looking into?

Dr. KATZKE. Yes, I am.

Mr. LUKEN. Area of inquiry, and also the purposes of the task force?

Dr. KATZKE. I think it would be wise to consider that.

Mr. LUKEN. The only reason I am asking you at this point is if that is what you are going to go into, please do include it, any of those comments that you have.

Dr. KATZKE. I am going to talk specifically about our computer security and risk mismanagement program and the specific technical areas we are working in. I would like to point out that many of the safeguards or the areas we are working in apply equally to the accidental types of activities as well as intentional.

Mr. LUKEN. Fine. Will you go ahead? And then we will engage in any discussion afterwards.

Dr. KATZKE. All right. ICST's computer security program primarily assists Federal agencies in meeting their computer security responsibilities. However, private industry is making increasing use of our services and resources.

ICST's computer security activities include: Identifying the needs of the Federal agencies; identifying the best practices and methods that can be used to satisfy Federal agency needs; developing needed products for the Federal agencies, for example, Federal Information Processing Standards and Guidelines—I have supplied five copies of a number of our documents for the committee—and publicizing our activities to make Federal agencies and the public aware of the work we have done. In addition, we work with voluntary standards organizations, such as the American National Standards Institute; serve as technical consultants to Federal agencies; consult with State and local governments to make sure that, to the extent possible, our technical products are useful to them; and interact with private organizations such as the American Bankers Association and computer security special interest groups.

Some of our current technical activities which are relevant to the computer security concerns of Federal agencies and private organizations, including small business include:

Risk analysis is a procedure for estimating potential losses related to the use of or dependence upon ADP resources and services. The results of a risk analysis are used in the selection of cost-effective safeguards. We have published a guideline which describes a particular methodology that has been successfully used in private industry and forms the basis for many other methodologies.

Our work in the areas of certification and accreditation derive from two workshops jointly sponsored by the ICST and the General Accounting Office. Certification addresses the establishment and components of a program for performing technical evaluation of ADP systems. Based upon a technical evaluation, accreditation is the approval process which determines if the ADP system should be placed into operation. Three guidelines are planned in these areas.

Contingency planning is concerned with the planning and preparation that must be done to assure continuity of ADP services should an unexpected event occur. We published a FIPS guideline and followed that up with an executive guide. The executive guide is a brochure that is aimed at high-level management, takes no more than 15 minutes to read, since it is in the question/answer format, and is intended to convince high-level management of the need for contingency planning. One of the issues we are currently looking at is the selection of an ADP backup strategy from the many alternatives that are available.

In conjunction with our microcomputer lab we are looking at the security capabilities of small systems. We want to investigate the development of security enhancements to currently available microcomputers and the use of microcomputers for performing the security functions of other systems or as components of microcomputer-based systems.

One key requirement for both integrity and security is personal identification and authentication. That is, how can a computer system identify the users of the system? Over the past few years we have established a laboratory for personal identification in ICST. We have investigated fingerprint readers, handwritten signature readers, hand geometry readers, and palm readers. Two FIPS guidelines have been published to assist users in selecting personal identification/authentication methods. We are also considering the use of our computer integrity, security, and speech laboratory for investigating voice verification techniques as a means of authentication.

Passwords are still the most cost-effective method of personal identification when requesting services from an ADP system. We have recently completed a proposed standard on password usage which specifies 10 factors that must be considered when designing and implementing the password system.

Once an individual has been identified and his or her identity authenticated, the ADP system should control the individual's access to only those resources he or she is authorized to use and only for authorized purposes. A guideline on user access authorization is underway which will assist managers of ADP systems in establishing requirements for and implementing such control mechanisms.

In 1977, ICST published a data encryption standard which specified the cryptographic algorithm for the protection of unclassified but sensitive computer data. This standard is needed in order that networked computer systems have a secure means of communication. The standard has been widely used.

Integrity is the assurance that data has not been modified either accidentally or intentionally without authorization. While integrity is an important area in all communities, it is especially important in financial transactions. This standard uses the data encryption standard to put a seal on data so that it cannot be modified without being detected.

The open systems interconnection model of the International Organization of Standardization is a conceptual architecture for the standards required to interconnect information systems. We have been looking at integrity and security within that model.

I will be happy to answer any other questions you might have.

[Dr. Katzke's prepared statement follows:]

PREPARED STATEMENT OF DR. STUART W. KATZKE, MANAGER, COMPUTER SECURITY MANAGEMENT AND EVALUATION GROUP, INSTITUTE FOR COMPUTER SCIENCES AND TECHNOLOGY, NATIONAL BUREAU OF STANDARDS, U.S. DEPARTMENT OF COMMERCE

I am pleased to appear before you today to describe the National Bureau of Standards programs in computer security and particularly those activities which may be of interest to small business.

In order to put the computer security program in context, I would first like to tell you about the institute for computer sciences and technology (ICST) where this work is done. ICST is a center of technical expertise in information technology. We focus primarily on helping users make more effective use of computers and information technology. These activities were set forth in 1965 by Public Law 89-306 "Brooks Act" and affirmed in 1980 by Public Law 96-511 (Paperwork Reduction Act).

While our activities are focused toward the Federal Government user, our services, guidelines and standards are also used by and are of assistance to the private sector. Our activities keep us in touch with the needs of both industry and Federal users and stimulate the sharing of technical information between public and private sectors. We develop standards principally through participation in, and leadership of, voluntary industry standards activities, both national and international. Our staff members participate in about 60 standards writing committees where they are instrumental in developing standards that address users' needs.

We provide technical assistance to Federal agencies on a cost reimbursable basis and informal advisory and consulting activities for a broad spectrum of external organizations. ICST's computer security program primarily assists Federal agencies in meeting their computer security responsibilities. However, private industry is making increasing use of our services and resources.

ICST's computer security activities include:

(1) Identifying the needs of the Federal agencies. We do this through personal contacts, conferences, workshops, meetings and constituency projects (where we provide direct technical assistance to the agency). Senior management officials for Federal ADP standards, appointed by agency heads, help us identify standards and guidelines needs.

(2) Identifying best practices and methods that can be used to satisfy Federal agency needs. We use technical assessments, conferences, workshops, and other means.

(3) Developing needed product (e.g., Federal information processing standards and guidelines) for the Federal agencies. We examine existing practices and methods. Where these are not adequate, we may try to develop new practices and methods that seem feasible, and publish the results in NBS technical documents, as well as other professional and technical publications.

(4) Publicizing our activities by making the general public and Federal agencies aware of the work we have done.

In addition, we: Work with voluntary standards organizations, such as the American National Standards Institute;

Serve as technical consultants to Federal agencies;

Consult with State and local government to make sure that, to the extent possible, our technical products are useful to them; and

Interact with private organizations, such as the American Bankers Association and computer security special interest groups. We invite vendors and users to our workshops to help us review our products and activities and we visit organizations that have good security programs in order to learn from their experiences.

Some of our current technical activities which are relevant to the computer security concerns of Federal agencies and private organizations, including small business, include:

RISK ANALYSIS

Risk analysis is a procedure for estimating potential losses related to the use of or dependence upon ADP resources and services. The results of a risk analysis are used in the selection of cost-effective safeguards. We have published a guideline which describes a particular methodology that has been successfully used in private industry and forms the basis for many other methodologies.

CERTIFICATION AND ACCREDITATION

Our work in these areas derived from two workshops jointly sponsored by ICST and the General Accounting Office. Certification addresses the establishment and components of a program for performing technical evaluation of ADP systems. Based upon the technical evaluations, accreditation is the approval process which determines if the ADP system should be placed into operation. Three guidelines are planned in these areas.

CONTINGENCY PLANNING

This area is concerned with the planning and preparation that must be done to assure continuity of ADP services should an unexpected event occur. We have published a FIPS guideline and have followed that up with an executive guide. The executive guide is a brochure that is aimed at high-level management; it takes no more than 15 minutes to read (since it is in a question-answer format); and is intended to convince high-level management of the need for contingency planning. One of the issues we are currently looking at is the selection of an ADP backup strategy from the many alternatives that are available.

SECURITY OF SMALL SYSTEMS

In conjunction with our microcomputer lab, we are looking at the security capabilities of small systems. We want to investigate the development of security enhancements to currently available microcomputers and the use of microcomputers for performing the security functions for other systems or as components of microcomputer-based systems.

PERSONAL IDENTIFICATION

One key requirement for both integrity and security is personal identification/authentication (i.e., how can a computer system identify the users of the system?). Over the past few years, we have established a laboratory for personal identification in ICST. We have investigated fingerprint readers, handwritten signature readers, hand geometry readers and palmprint readers. Two FIPS guidelines have been published to assist users in selecting personal identification/authentication methods. We are also considering the use of our computer integrity, security and speech laboratory for investigating voice verification techniques as a means of authentication.

PASSWORD USAGE STANDARD

Passwords are still the most cost-effective method of personal identification when requesting services from an ADP system. We have recently completed a proposed standard on password usage which specifies ten factors that must be considered when designing and implementing a password system and which defines minimum security criteria for each of the ten factors that must be met in federal applications.

USER ACCESS AUTHORIZATION

Once an individual has been identified and his/her identity authenticated, the ADP system should control the individual's access to only those resources he/she is authorized to use and only for authorized purposes. A guideline on user access authorization is under way which will assist managers of ADP systems in establishing requirements for and implementing such control mechanisms.

DATA ENCRYPTION STANDARD

In 1977, ICST published a Data Encryption Standard (DES) which specified a cryptographic algorithm for the protection of unclassified but sensitive computer data. This standard is needed in order that networked computer systems have a secure means of communications. The standard has been widely used. Additional publications have been developed that support the use of the DES (e.g., DES modes of operation, guidelines for implementing and using the data encryption standard).

DATA INTEGRITY STANDARD

Integrity is the assurance that data has not been modified, either accidentally or intentionally, without authorization. While integrity is an important area in all communities, it is especially important in financial transactions. This standard uses the DES to put a seal on data so that it cannot be modified without being detected.

OPEN SYSTEMS INTERCONNECTION (NETWORK) SECURITY

The open systems interconnection model of the international organization of standardization, is a conceptual architecture for the standards required to interconnect information systems. We have been looking at integrity and security in that model.

I will be happy to answer any questions.

Mr. LUKEN. Well, thank you very much, Dr. Katzke. I wonder if I could ask one question.

What do you believe is the most difficult computer crime to guard against?

Dr. Katzke. Probably from somebody who is an authorized user of the system, somebody who works in-house, is trusted.

Mr. Luken. Someone who would be using it for their own benefit?

Dr. Katzke. That might be the ultimate aim, their own personal gain or financial gain.

Mr. Luken. Or in concert with others?

Dr. Katzke. Possibly; that makes it harder, but yes, it is possible. The important thing is that there has to be a management awareness of that problem. When an ADP system is involved, there must be the technical controls in place that can record access, whether authorized or not, and manager awareness to be checking on individual employees via auditors and other financial types of audits.

Mr. Luken. Then it would be a form of embezzlement, wouldn't it?

Dr. Katzke. As my understanding of embezzlement, I would think so.

Mr. Luken. It might be difficult or more difficult to prove than the more conventional or traditional forms?

Dr. Katzke. Very often there is a lack of technical controls and management awareness. It is very difficult to gain evidence when a crime is committed.

Mr. Luken. Would that be one of the things that the task force should address itself to?

Dr. Katzke. Absolutely.

Mr. Luken. It seems to me that if a potential embezzler who is an expert on the computer programs he is working on gets a smattering of law, he wouldn't have to be a genius to accomplish some form of embezzlement through the computer system without much risk, and actually may succeed in profiting illegally at the expense of the employer without risking criminal prosecution.

Dr. Katzke. In some cases that has been demonstrated, but on the other hand, the alternative is to use the technology to your best advantage in trying to put into place safeguards which can be used to prevent that kind of thing from happening. You can use a computer that is equally as powerful on the other side.

Mr. Luken. You mean to prevent the actual use of the computer? You can use the computer to prevent more traditional forms of embezzlement?

Dr. Katzke. That is correct. Well, to put into place safeguards which would prevent the embezzlement from occurring or at least be able to help you detect when it has occurred, in other words, using the computer as a tool to prevent crime.

Mr. Luken. Did you say you are looking at security capabilities of small systems?

Dr. Katzke. Yes; we are particularly concerned about those.

Mr. Luken. How far along are you in that?

Dr. Katzke. We are just starting off on that project.

Mr. Luken. Do you have any idea how long that will take?

Dr. Katzke. No; we are about to get into the next planning cycle and are trying to look at that problem in more detail.

Mr. Luken. You are looking at it within the Federal Government, too?

Dr. Katzke. Yes.

Mr. Luken. Looking at it both from the standpoint of computers within the Federal Government and the private sector?

Dr. Katzke. Mostly we are concerned with the Federal Government, but most of what we do is certainly applicable to private industry.

Mr. Luken. Do you feel that you have had any success in your activities with regard to the Federal Government?

Dr. Katzke. I believe so.

Mr. Luken. Could you describe that?

Dr. Katzke. I couldn't quantify that in any way. No, I could not.

Mr. Luken. Has this been an extensive thing that you have delved into with the Federal Government?

Dr. Katzke. Our program is directed primarily at the Federal agencies, yes, and we publish a number of guidelines and standards which Federal agencies should use for their computer systems. We provide advice to them on how to protect their ADP systems.

Mr. Luken. Of course, you have no investigatory role?

Dr. Katzke. No.

Mr. Luken. The gentleman from Oregon.

Mr. Wyden. Thank you, Mr. Chairman. Mr. Katzke, you have been very helpful and you have covered some of the things that were on my mind today. You have told us a little bit about how the National Bureau of Standards is trying to develop computer security guidelines.

I am pleased that you all are looking particularly at small computer systems. I just have a couple of additional questions.

Have any of the efforts that you all have undertaken over there been directed specifically at small business?

Dr. Katzke. No, they have not.

Mr. Wyden. Can you describe some of the practical steps that small business owners or managers can take to insure the integrity of their systems?

Dr. Katzke. Basically there are two areas: management safeguards and technical safeguards. Management safeguards primarily require awareness on the part of small business that there are a number of different types of events that can cause computer security problems which result in the three problems I have mentioned: loss of data confidentiality, integrity, and not having a system available when needed.

The other area is technical controls, basically personal identification authentication, user authorization and audit trails. These are the three major ones that most people consider. They include knowing who the user is—who is on that system—and positive identification of the user, whether it is a password, a magnetic card, something the person knows, or a physical feature.

Once the person has been authenticated, then you have got to control his access or have a mechanism which has a list, if you will, of the users and the objects on the system—data objects, files or whatever—and somehow a mechanism which says Mr. Smith is only allowed access to this kind of information, and in this certain way he can only read it as opposed to modify it, and then, besides that, you should have an audit trail, that is recordkeeping mechanisms of some kind, because Mr. Smith may be authorized to use data such and such but not for the specific purpose he used it for, like putting together a customer list.

Mr. Wyden. Let us say that most small businesses could understand those steps. I am not sure that they could just based on the answer you gave, but let's just say hypothetically that they could. Do you think they are implementing them right now?

Dr. Katzke. I really don't know. That would be hard for me to say. We have not had extensive contact with small businesses.

Mr. Wyden. So then at this point my next question is do you think there is a need to get practical information of this sort out to small businesses?

Dr. Katzke. You mentioned small business specifically, but based on my interaction with the Federal agencies and numerous private industry organizations, I would say, yes, it is a need for those communities as well. I would imagine for small businesses, too.

Mr. Wyden. Mr. Chairman, I should probably quit while I'm ahead at this point, but I wanted to ask just one other question. My understanding is the administration is neutral on this legislation at this point. Now you all are part of the Department of Commerce?

Dr. Katzke. That is correct.

Mr. Wyden. No position has been taken over there one way or another?

Dr. Katzke. Not that I know of.

Mr. Wyden. You are looking at it and there is discussion at this point. The administration is neutral on it?

Dr. Katzke. I have no information either way.

Mr. Wyden. Thank you. Thank you for your testimony. Thank you, Mr. Chairman.

Mr. Luken. Do you believe that there is much more attention needed to the subject?

Dr. Katzke. Absolutely, very definitely, in all phases of the computer security problem.

Mr. Luken. I don't want to lead you to an answer, but if the formation of the task force is proper, and the task force activities are properly focused, do you think it will do some good in an area where it is needed?

Dr. Katzke. I think exposure of the problem would do some good. Basically, one of the prime problems is an awareness problem on the part of people, particularly those users of small systems who are just getting into the computer areas and who have no knowledge about the computer in general, and in particular what can and what does happen. For example, a particularly small business where the whole business operation depends upon the use of that computer and its being available.

Mr. Luken. Don't we foresee such things as electronic transfer of funds?

Dr. Katzke. We are looking at much more computerized——

Mr. Luken. There being an explosion of the problem; isn't that what we are talking about?

Dr. Katzke. Yes.

Mr. Luken. Not just burgeoning; it could be a virtual explosion. More activities, as long as they are part of a concerted effort, would seem to me to be advantageous, and as we find often that activities in the small business field at least have a ripple effect. Most of our businesses are small business. Most of our jobs are in the small business area so that we are not talking about a minor part of the problem, we are talking about a major part of the problem.

Dr. Katzke. One of the major things that you very often see is that in corporations, as well as the Federal agencies, there is competition for resources. When it comes to putting out resources to protect ADP systems, it is like an insurance policy; there is a lot of competition. Private organizations as well as Federal agencies tend to bypass some of the proper security safeguards and controls. I think that is a mistake. It has to be emphasized that those are important areas that have to be considered when you are competing for resources even though there may not be a tangible demonstration of gain from those resources.

Mr. Luken. If there is nothing else from the members of the committee, then we thank you very much, Dr. Katzke, for your counsel here today, and we look forward to working with you as these matters progress.

Dr. Katzke. Thank you for inviting me. I enjoyed it.

Mr. Luken. Now we will have a panel of Donn Parker and Bobby Marrs and Sgt. Larry Faries, the assistant commander of the Maryland State Police Crime Prevention Unit.

We will hear them in the order in which we have called them, beginning with Mr. Parker. We do have a statement from you that has been submitted. Do you want that introduced into the record, into the committee's proceeding?

Mr. Parker. Yes, I do. Please enter it as if read.

Mr. Luken. All right then. You may proceed to summarize it, excerpt it, read it, or explain it in any way you think would be helpful.

PANEL CONSISTING OF DONN B. PARKER; LARRY FARIES; AND BOBBY MARRS

TESTIMONY OF DONN B. PARKER, SENIOR MANAGEMENT SYSTEMS CONSULTANT, INFORMATION SYSTEMS MANAGEMENT DEPARTMENT, SRI INTERNATIONAL

Mr. Parker. Thank you, Mr. Luken, for this opportunity. My name is Donn B. Parker. I am a senior management consultant at SRI, Intl. However, I am here speaking for myself and not for my employer or my clients.

I have been in the computer field for 30 years in programing management from the technical side of computer technology, not on the legal side. For the past 13 years I have been studying the problem of computer crime and computer security.

At SRI we have a collection of over 1,000 reported computer crimes, and we study these on a case-by-case basis. I am going to give you an idea of the nature of computer crime as much as we know of it and to describe a typical computer security situation in a small company and what we can conclude. I will discuss the need for H.R. 3075 and some recommendations for the bill.

Computers are proliferating as has been indicated, and therefore, we can guess that computer crime is also proliferating, but primarily the problem of computer crime is that computers are changing the nature of business crime.

Even though we don't know whether business crime is increasing or decreasing because of the use of computers, we certainly know that it is changing. It is changing because of the changing occupations of people in business: Programers, tape librarians, data entry clerks, and so on.

It is changing because the environments of business crime have changed. Now we find some crimes occurring inside computers, in computer rooms, and around terminals. The forms of assets have changed, and as Mr. Wyden has been quoted in talking about Willie Sutton, the famous bank criminal who said that he focuses on banks because that's where the money is, the money today is inside the computer. Therefore, the computer has become the vault of a small business because that is where their assets are stored, and that is where the principal data of their physical assets is stored, and therefore, it is an obvious focus.

Computer business crime is also changing because the methods are changing, and again Mr. Wyden has mentioned the whole array of new methods of business crime, including Trojan horses, logic bombs, superzapping, data diddling, asynchronous attacks, and so on.

It is also changing because the timing has changed. Some business crime occurs in 3 milliseconds; in less than three thousandths of a second the crime is perpetrated, all the evidence is electronically erased. It is over with.

Finally, business crime has changed because the geography has changed. If I could find a telephone booth in Outer Mongolia, I could conceivably be conducting some kind of a crime in a city in the United States in a computer that is connected to the dial-up telephone system.

As has been stated here, there are no valid statistics on the subject, and even though almost every article of computer crime quotes numbers, I can assure you that they are not valid, and I know that because most of them come from me in my studies. We know only a very small amount, and our numbers are taken out of context and made representative of the problem, whereas they are not, because there is no mechanism available yet in order to count the cases.

We are currently doing a study for the U.S. Department of Justice to count and record all computer crimes that have been prosecuted under the 20 State computer crime laws. Possibly by the end of this year we will have a reasonable start of some valid data on this subject, but obviously very limited.

In studying the problem on a case-by-case basis, I believe what is happening today is an escalation of business crime. That is, I anticipate that the number of business crimes, and I can refer this to small businesses as well, over the next few years could go down in frequency whereas at the same time the losses per case in business crimes could go up drastically. As I said, this is not based on statistics but is based on looking at over a thousand cases and on a case-by-case study of the problem.

To make this clear, what I am saying is that the total number of business crimes could go down, but at the same time the number of

computer crimes will continue to go up drastically. What that means is that computer crime will be a much higher proportion of business crimes. In fact, most business crimes in the next few years won't even be able to occur without involving computers in some way.

Now consider a typical case of a security situation for a small wholesale distributor. He has three clerks who are handling the orders, invoices, purchasing, controlling inventory, handling the accounting records, and so on. Information that management gets is at least 3 weeks old, and the clerks are low paid, handling all this on typewriters and paper stored in unlocked file drawers and in unlocked offices.

They decide to acquire a computer. They convert to the use of a computer. Now they have three technically trained people who sit at terminals. The reports of the company are stored in the computer and on magnetic tape kept in a locked room. Each of these individuals has his own password and access only to the data that is necessary for that person to do his job. The computer programs that they are using are accounting and other application packages available on the market and developed with very extensive and powerful controls built into them.

This situation also provides management of that small company with performance information of the company on a daily basis; so day by day management knows and can look at any deviations from normal activity.

Looking at this little case study we conclude that the problems that are faced are those of change, and not necessarily of increased or decreased vulnerability, but of changing vulnerability. It is important that management in small business understand the changes that are going on.

I find that there is a significant need for the proposed task force and resource center in H.R. 3075. There is no objective mechanism to get computer vulnerability and security information to small businesses. The computer and computer program manufacturers will provide the security necessary but only the security that the small business is willing to pay for, and they don't know that they need the security. The salesmen of these companies are certainly not going to inform their customers of all the terrible things that could happen to them in the purchase of their products.

Consultants do not have the marketing capabilities to sell their consulting services to aid small businesses. Consultants generally work for very large business and under very large contracts.

On the plus side, the insurance industry is awakening to the huge market for EDP insurance. This is a very strong force that will be coming in the next several years. The insurance companies will play an important role in informing small businesses of their vulnerability, and of course, providing the insurance. Also their loss control services will be made more available to small businesses. Another positive force comes from many small businesses that are now manufacturing security products and have a wide range of very powerful security products available for computer systems.

However, we still lack a source where the motivation for supplying information comes from an objective viewpoint. That source should be something like the resource center that has been proposed in this bill and deriving from a task force that can gain the information and get the resource center started.

In conclusion, my recommendations are: one, that you shorten the period of performance of the task force, as Mr. Wyden has already suggested. In 3 years computer crime will be an entirely different problem than it is today because of the fast and rapid change of technology, so I think it ought to be at least no longer than 18 months, and I would even recommend about 1 year because of the urgent need.

It is probably not going to be possible for this task force to produce a reasonable estimate of annual loss from computer crime in small business, and I do not think that should be made a requirement of the task force. There just aren't any mechanisms in order to do that. There should be more explicit emphasis of private sector representation on the task force. It looks like it is a little overloaded with Federal representation. We need people such as information security experts, auditors who play important roles in small business protection, prosecutors and police investigators who have had some experience with computer crime, an insurance expert since insurance is going to play an important role, and a representative from the computer and computer program manufacturers. These people would all provide the scope necessary and the background and expertise in order to examine the problem.

Finally, one last point, that the massive amount of information that has already been developed be examined as the starting point for such a task force.

Thank you for the opportunity to testify here, and I will be glad to answer questions.

[Mr. Parker's prepared statement follows:]

Prepared Statement of Donn B. Parker, Senior Management Systems Consultant, Information Systems Management Department, SRI International

Introduction

My name is Donn B. Parker. I have extensive qualifications in the computer field, having worked for 30 years in computer programming and computer systems management. For the past 13 years of my career, I have been a researcher and consultant specializing in the computer crime problem and computer security. I have a Master of Arts degree in mathematics from the University of California at Berkeley. I am currently a senior management systems consultant in the Information Systems Management Department at SRI International, Menlo Park, California. The statements included herein are my own and do not necessarily represent those of SRI International or any clients of SRI.

I have published widely. I wrote the definitive book on computer crime, Crime by Computer, in 1976; a new book, Fighting Computer Crime, was recently published. In addition, I have written two books for the professional audience, Computer Security Management and Ethical Conflicts in Computer Science and Technology. My SRI associates, Ms. Susan Nycum, a leading lawyer in computer law, and I produced the definitive manual on computer crime investigation and prosecution, Criminal Justice Resource Manual on Computer Crime, and a new report, Computer Security Techniques, for the Bureau of Justice Statistics of the U.S. Department of Justice.

The Nature of Computer Crime

As noted in HR 3075, a bill to establish a Small Business Computer Crime and Security Task Force, "...there is increased dependency on, and proliferation of, information technology (including computers, data networks and other communication devices) in the small business community." Statistics on small computer sales, packaged computer programs, and increasing numbers of small businesses selling such computer and program products support this statement; however, no valid statistics exist to indicate that such technology has permitted and expanded criminal activity against small businesses because no mechanisms are in place to obtain such information. Nevertheless, I believe that an increasing proportion of crimes perpetrated against small businesses involves computers, primarily because of the increasingly important role of computers in environments where such crime occurs. At the same time, the total number of crimes of all types against small business may be diminishing while the loss per case is growing.

SRI International has the most extensive collection of documented computer crime cases in the world--more than 1,000 cases reported since 1958--yet this collection is neither complete nor representative of the problem. My 13-year, case-by-case study of computer crime and research and consulting in computer security show that small business is probably safer from the incidence of all kinds of crime because of the increasing use of information technology. The likely escalation of small business crime consisting of reduced frequency but larger loss is seen as the result of factors depicted in the typical scenario described below.

A small wholesale distribution business used to have three low-paid clerks receiving and filling orders, purchasing and maintaining an inventory of products, typing and sending invoices, receiving and posting payments, and keeping accounting records. Management studied the piecemeal, limited, summary business records that frequently lagged transaction dates by 3 weeks.

After a small computer was installed, significant changes were made. One clerk now receives and fills orders and enters them into the computer. Invoices, purchase orders, all accounting records, and business record summaries are automatically produced on a daily basis. Another clerk receives and posts the payments in the computer. A third employee operates the computer, develops simple computer programs for specialized purposes, and maintains a set of purchased application program packages used by many other small businesses as well. The computer and data tapes and disks are kept in a locked room.

The small business described in this scenario is probably safer from crime in many ways after installing the computer:

- The continuously functioning controls built into the application packages are far better and more reliable than the limited, error-prone controls employed by the three clerks who were not always well-motivated.
- Managers examine summary business records and exception reports produced by the computer on a timely basis to detect any deviations from normal or expected activity.
- Clerical and technical personnel have been upgraded to a more professional and highly paid level. Staff members are far more productive and disciplined, and their assigned work consists of more narrow tasks; they have only limited knowledge of activities in other areas.
- Most business records are processed and stored in a limited access room by the computer and application programs that are not easily altered.

If a crime were to be committed after the computer was installed and operating well, it would most likely require more skills, knowledge, access, and collusion than before the facility was installed. Because the crime would be more dangerous and complex for the perpetrator, a rational perpetrator's gain would generally have to be larger to make the crime worthwhile.

Other factors are also evident in this scenario. The business was probably more vulnerable to crime during conversion to computer usage. The business would also be far more vulnerable to crime if management failed to use the new controls available or employed people not sufficiently competent to deal with the new technological complexities. Greater vulnerability to crime would also be likely if the computer and application packages were not sufficiently resistant to fraud. Computers, automated processes, and data in computer media are fragile and subject to damage by a destructive individual in different ways than paper records in filing cabinets where all processing work is performed by people. Finally, a sufficiently sophisticated criminal or team of criminals would have the same computer power as the business to engage in crime with greater gains. Therefore, the crime-related factors revealed by this scenario support the likelihood of higher losses per case, but fewer crimes in small businesses.

The Need for HR 3075

The scenario also supports the need to establish the Task Force specified in Section 3 and subsequently the Resource Center described in Section 4 of HR 3075 to alert management to problems and potential solutions; no other effective functions are in place to serve this purpose. The problem to be addressed is not necessarily an increase or decrease in incidence of small business crime but a drastic change in the nature of such crime as use of information technology increases. In fact, for the first time in the history of small business, we have the opportunity to reduce small business crime to unprecedented low levels by urging, instructing, and motivating small business management to use computer-related controls and security procedures already known and available on a cost-effective basis.

As small business owners and managers are given opportunities to modernize their businesses with new information technology, they must also be made aware of the dangers, vulnerabilities, and security associated with use of these powerful tools. The computer manufacturers and computer program suppliers are adequately providing the security that customers demand and are willing to pay for, but their salesmen do not go out of their way to inform their customers of the dangers and vulnerabilities, for obvious, commercial reasons. Therefore, the motivation to create a demand for security must come from other sources; HR 3075 could fill this need.

Most computer security consultants find it difficult to sell their services to small businesses. The cost of selling such services to potential customers who do not recognize that they need help is too high relative to the size of resultant contracts to make a viable consulting market considering current security review methodologies.

Fortunately, two positive forces are emerging to encourage small business owners to protect themselves in the informtion age. The first is the insurance industry, which is now starting to consider the huge potential EDP insurance market. When insurance premium rates become variable dependent on the amount of the insureds' information security, and when insurance companies apply their massive loss control capabilities to the problem, great security advances to reduce risk will be realized.

The second force to reduce the risk of small business crime is a growing computer security products industry. Many new small businesses now offer relatively low-cost devices and computer programs to prevent computer equipment and program theft and unauthorized access into computers. Others are offering computer program packages to provide protection of data using cryptographic techniques.

I believe, however, that these forces alone are not sufficient to solve the problem and take advantage of the potential for crime reduction possible with the increasing use of computers. The Task Force and Resource Center provided for in HR 3075 could be a powerful force to achieve these objectives through awareness and education programs and provide a great service to the small business community and their customers. The Task Force is similar to an idea that I presented in testimony on HR 1092, Congressman Nelson's bill on computer crime, before the House Judiciary Subcommittee on Constitutional and Civil Rights on September 23, 1982. I suggested a national commission to investigate computer crime.

Recommendations

The Task Force should first use information that has already been produced. At SRI, we are engaged in research under a grant from the U.S. Department of Justice, Bureau of Justice Statistics, which should be of assistance to the proposed Task Force. In conjunction with Ms. Susan Nycum, we are compiling all computer crime cases prosecuted under the 20 state computer crime statutes and studying the new crimes of unauthorized access to computers by juveniles (system hacking) and theft of computer programs (software piracy). In previous projects, SRI documented 500 reported computer crimes in the U.S. Department of Justice JURIS data base retrieval system and produced a report identifying 82 computer security safeguards and a new baseline methodology for selection of generally accepted controls.

The Task Force should be composed of more representatives from the private sector and fewer from the Federal government than proposed in HR 3075. Private sector information security experts, police and prosecutors experienced in dealing with computer crime, information processing product manufacturers representatives, auditors for small businesses, and EDP insurance experts should be represented on the Task Force.

The Task Force should complete its work in 18 months rather than in the 3 years specified in the bill. The computer crime problem will change drastically in 3 years, and immediate action is needed.

Although obtaining accurate information about some reported cases of computer crime is possible, so much is not reported or not reported in retrievable ways and so many victims are reluctant to report criminal activity that it is not practical to obtain accurate estimates of the cost per year of computer crimes against small business. This requirement should be stricken from the bill. Otherwise, the bill contains practical methods for aiding small business.

References

1. Donn B. Parker, Fighting Computer Crime (Scribners, 1983).

2. Donn B. Parker, Computer Security Management (Reston, 1982).

3. Tom S. Eason and Douglas A. Webb, Nine Steps to Effective EDP Loss Control (Digital Press, 1983).

4. Computer Security Techniques, Report No. 1982-361-122/1873 (U.S. Government Printing Office, Washington, D.C.).

5. Criminal Justice Resource Manual, Report No. 1979-311-379/1710 (U.S. Government Printing Office, Washington, D.C.).

Mr. Luken. Mr. Faries.

Sgt. Faries. Good morning!

Mr. Luken. Sergeant Faries.

Sgt. Faries. That is correct, sir.

Mr. Luken. Do we have your statement? Apparently we have a statement from you dated July 14, 1983, and without objection, it will be admitted into the record.

You may proceed in any way you see fit.

TESTIMONY OF LARRY FARIES, ASSISTANT COMMANDER, CRIME PREVENTION UNIT, MARYLAND STATE POLICE, ON BEHALF OF THE MARYLAND CRIME PREVENTION ASSOCIATION, AND THE MARYLAND CRIMINAL JUSTICE COORDINATING COUNCIL

Sergeant Faries. Thank you. I am here today representing the Maryland Crime Prevention Association of which I am the current president. In addition, I am representing the Maryland crime watch program which is an arm of the State of Maryland. I am a sergeant in the State police and currently am the assistant commander of the crime prevention unit of the Maryland State Police.

The Maryland Crime Prevention Association is made up of a group of law enforcement officers, private businessmen, businesses, and individuals from throughout Maryland who have a vested interest in crime prevention. The association has worked to foster crime prevention programs in the State of Maryland for the last 5 years.

The association works very closely with Maryland crime watch, which is a steering committee composed of representatives from every major law enforcement agency in the State of Maryland whose task it is to provide instructional programing and materials for the law enforcement agencies throughout the State of Maryland. This allows continuity and consistency with our programs in the State.

We are entrenched in the State of Maryland in crime prevention programing. This can be exemplified because on June 30, Governor Hughes of the State of Maryland accepted an award from the National Crime Prevention Coalition for the practitioners in the State of Maryland as being the finest crime prevention affiliated State in the country. In representing these two organizations, I would like to lend my support to H.R. 3075. It seems that in the State of Maryland as a law enforcement officer I am very well aware that we have a very sophisticated computerized program which interfaces all the major and minor law enforcement agencies throughout the entire State. In addition, with a small plastic card and four digit number I can go to any bank in the State of Maryland where I have an account and get a loan, transfer money, pay my water bill, just about anything else, so computers and the computer industry are very much entrenched in our State and in the law enforcement community.

From what I can gather and from what Mr. Bequai said a little earlier today, computerized crime is dealing the citizens of this country and small business in particular with a $40 billion annual tariff, and from what my research has shown me, only 1 percent of the computer crimes that are detected are normally detected by accident. Only 1 in 22,000 of these particular cases is prosecuted successfully. Computer criminals I think are a unique breed of people. In law enforcement we are use to dealing with street criminals. You don't find that type of individual in computer crimes. You are dealing with highly sophisticated, very well-educated young people. Most of them are affiliated with reputable firms and have received their training at some of the finest colleges and universities in the United States.

Now unlike Mr. Parker, I am not a computer expert. I have a very limited knowledge in the field. I am a law enforcement officer. I know that today's local and State law enforcement agencies do not have the capacity to deal with computer crimes. To do so requires a level of human expertise and support of resources that currently do not exist. In addition, law enforcement must continue its emphasis on reducing crimes against people and crimes against property.

I am also a crime prevention practitioner. I know in fact that crime prevention works. When people in neighborhoods or when a group of business people in a shopping center get together and pool their efforts, they can reduce the opportunity of criminal undertakings to take place in that particular environment. I know, and I have seen that we can reduce burglaries in neighborhoods. I know that Southland Corp. has reduced up to 70 percent armed robberies in their convenience stores. It is a commonsense approach to law enforcement and is one whose time has come.

People throughout the Nation have focused their attention on defeating the criminal before the crime occurs. While we in crime prevention have focused our efforts primarily in these last 15 years or so to crimes such as breaking and entering and rape and armed robbery, auto theft, those types of crimes, I don't see any reason why we couldn't focus our efforts in the field of computer criminalization.

There is no substitute for an initiative taken before crime occurs. I don't care what the crime is. That is just basic commonsense. H.R. 3075 provides a sound initiative upon which a nationwide prevention program, focusing on our information systems, may be built.

If approved, the task force cited in the bill would have access to a myriad of crime prevention programing already underway in all the States. In fact, those of you on this subcommittee represent States that have some of the finest, most productive crime prevention networks in existence worldwide.

We in crime prevention are organized. We have a network of information sharing that is second to none in this country. The challenges posed by the computer criminal are far too vast for the existing criminal justice system. If our primary objective is that of reactive policing, we cannot deal with this crime from a reactive standpoint. We must approach it from a proactive or preventive approach because this gives us the opportunity to attack the potential criminal before the crime occurs, and this law enforcement philosophy today is the bottom line.

I totally support Mr. Wyden and his bill.

[Sergeant Faries' prepared statement follows:]

Prepared Statement of Larry Faries, Assistant Commander, Crime Prevention Unit, Maryland State Police, on Behalf of the Maryland Crime Prevention Association, and the Maryland Criminal Justice Coordinating Council

Good day. Mr. Chairman and Members of the Subcommittee, I am Larry Faries. I am here today representing the Maryland Crime Prevention Association and the Maryland Crime Watch Program of the Maryland Criminal Justice Coordinating Council. I am a Sergeant with the Maryland State Police and serve as Assistant Commander of the agency's Crime Prevention Unit.

The Maryland Crime Prevention Association is made up of law enforcement officers, private businesses, and individuals from throughout Maryland who have a vested interest in crime prevention. The Association has worked to foster crime prevention programs and legislation for over five years.

MCPA has worked closely with the Maryland Crime Watch Program of the Maryland Criminal Justice Coordinating Council. MCW provides a wide range of materials and instructional programs to criminal justice agencies in Maryland in order to ensure consistency and quality in our Statewide efforts.

On June 30, the State of Maryland was presented the first Award for State presented by the National Crime Prevention Coalition. This award was presented following application made by the Crime Prevention Association and Maryland Crime Watch Program.

In representing both the members of the Crime Prevention Association and Maryland Crime Watch, I am asking for your support for H.R. 3075, To Amend The Small Business Act to Establish A Small Business Computer Crime and Security Task Force.

Federal, state, and local businesses, industries, and governmental agencies are turning toward computerized data systems at an amazingly rapid rate. In Maryland, an elaborate computer network has been established by which law enforcement agencies may readily exchange information on criminal offenders. Almost every bank chain has a computerized system that can be accessed by consumers through use of a simple plastic card and a four-digit code.

In 1976, the Task Force on Private Security of the National Advisory Committee on Criminal Justice Standards and Goals estimated that there were 140,000 computer systems in use in the United States. Some estimates show that this number has increased five-fold since the report was published. The Task Force, which was formed by LEAA in 1975, recommended a standard on computer security that stated, "Possessors of computers should have a comprehensive protection plan for both physical site and data, regardless of whether the computer is used solely for their own needs or for providing computer services to others."

It has been estimated that computer crimes in the United States may run as high as $40 billion annually, according to August Bequai.

Sue Reid, of the University of Tulsa School of Law, estimates that only one percent of the computer crime that occurs is detected . . . and most of that is detected by accident. She also estimates that only 1 in 22,000 of the *detected* computer crimes will be successfully prosecuted. This estimate is supported by Robert Campbell, President of Advanced Information Management.

Computer criminals are unique. They do not fit the stereotype of the street burglar or mugger. They pose a new and unusual challenge to the law enforcement and criminal justice community.

Most computer criminals are young, white-collar-type offenders who have received training in a college or university. They are often associated with reputable firms and hold impressive positions. Many learned their criminal art during their college training when breaking into a computer system was an encouraged educational activity.

I am not a computer expert. I am a law enforcement officer. I know that today's local and state law enforcement network is not prepared to deal with computer crimes. To do so requires a level of human expertise and supportive resources that do not currently exist. In addition, law enforcement must continue its emphasis on reducing crimes against persons and crimes that affect people in their homes.

I am also a crime prevention practitioner. I know that crime prevention works.

When people, whether they be citizens in a neighborhood or small business owners, take the initiative to make crime more trouble than it's worth for the potential offender, we win victories. We have evidence to show that private citizens can reduce burglaries in their neighborhoods. We have evidence to show that armed robberies in convenience stores can be significantly reduced through low-cost, prevention techniques. People throughout the nation have focused their attention on defeating the criminal before a crime occurs.

While crime prevention has focused primarily on such crimes as breaking and entering, rape, armed robbery, and auto theft, there is no reason to believe that the concept could not be expanded to the prevention of computer crimes. There is no substitute for initiative taken before a crime occurs, regardless of the nature of the crime.

Bill #3075 provides a sound initiative upon which a nationwide prevention program, focusing on our information systems, may be built. If approved, the Task Force cited in the bill would have access to a myriad of crime prevention programs underway in every state. In fact, those of you on this Subcommittee represent States that have some of the finest, most productive crime prevention networks in existence worldwide.

The challenges posed by computer crimes are too vast for our existing criminal justice system, if our primary focus is one of reaction. A proactive approach . . . a preventive approach . . . gives us the opportunity to attack the potential criminal before he or she attacks our information systems. Proactive approaches to crime cost far less than those involving long investigations, complex prosecutions, and incarceration or follow-up services.

Your support of this bill establishes the foundation for a proactive approach to computer crime. It will positively impact those people who can least afford to be victimized . . . small business owners.

I encourage your full consideration of this bill and your continued support for a proactive approach to computer crime. Thank you for your time and interest.

Mr. Luken. What is the name of the company you mentioned?

Sergeant Faries. Seven Eleven, sir.

Mr. Luken. And they have reduced robberies 70 percent through computer detection?

Sergeant Faries. No, rather through basic crime prevention techniques, whether it be handling the cash flow to employee training and knowing what to do and what to look for.

Mr. Wyden. Mr. Chairman, I would appreciate your yielding for a second. I think that is important testimony. It is my understanding—maybe the witness can tell us more about it—that is primarily because they don't keep cash at night.

Sergeant Faries. That is exactly right.

Mr. Luken. I just wanted a clarification. I didn't know whether you meant there was a computer connection with those efforts.

Sergeant Faries. No, sir.

Mr. Luken. All right. The final witness on this panel is Mr. Bobby Marrs.

Mr. Marrs. Good morning.

Mr. Luken. Mr. Marrs, you have sometimes been described as a victim.

Mr. Marrs. Yes, sir.

Mr. Luken. But I am sure you will be able to tell us about your experiences.

Mr. Marrs. I will be glad to. First of all, I want to thank you for inviting me up here.

Mr. Luken. Where do you live?

Mr. Marrs. Shreveport, La.

Mr. Luken. What is your occupation?

Mr. Marrs. Office manager of our company, National Bonded Money Orders.

Mr. Luken. Were the experiences that you are about to describe connected with your employment?

Mr. Marrs. Yes, sir.

Mr. Luken. National Bonded Money Orders, what is that?

Mr. Marrs. It is a money order company like Travelers or American Express.

Mr. LUKEN. Except it is not on the same scope as the ones you described?

Mr. MARRS. We are much smaller than they are; the same thing, similar company.

Mr. LUKEN. Is it regional?

Mr. MARRS. Yes, sir. We are limited to Louisiana, mostly a sale limitation because we are a small company. There are just three of us that are employed at our office, including myself, at this time.

Mr. LUKEN. Three employees in the whole company?

Mr. MARRS. At this time, yes, sir.

Mr. LUKEN. OK.

Mr. MARRS. Maybe I should clarify. We have agents around the State who sell the money orders for us. We are just the accounting office, and we and our computer do most of the accounting.

Mr. LUKEN. All right. I won't impede you any further. You go ahead and tell us in your own words what the situation is, when it developed.

Mr. MARRS. You just want an account of what happened to me?

Mr. LUKEN. Whatever you think will help us.

Mr. MARRS. OK.

Mr. LUKEN. That certainly is an important part of it.

TESTIMONY OF BOBBY MARRS, NATIONAL BONDED MONEY ORDERS

Mr. MARRS. Well, National Bonded Money Orders is a subsidiary of a larger company, Shreveport Tobacco. We were a wholesale tobacco company which we sold in November 1980, but at the time this all occurred we were still in the wholesale business when we converted to a computer system a year or two before to put our wholesale division on this computer system. At the time we bought the computer, the company we bought it from provided us with a programer who helped us implement the application software. Most of it was packaged application software.

He helped us implement the software and he worked with us closely for probably 2 years. Over that time, he became like an employee. We got to be friends, he and I, because he was there almost every day. He eventually had access to the computer at will and almost anything else, because in the process of implementing applications packages you have to have a pretty detailed understanding of the workings of the business, so he did have access to most everything, our records, and anything he needed to help him in his work.

In the meantime, we had decided to sell our wholesale division, and at about the same time we decided to put our money order division on the computer as well. Well, this involved writing a whole new program from scratch, and he took that job as well. He wrote this software from scratch. Before we had our accounting package developed we had an accounting firm in Shreveport handling our money order system for us. We turned over all our documents and our canceled checks and everything. We had another company handling all the processing for us, so in the switchover process there was a several month period in which our books were not in balance while we were transferring the control from the other company to our computer system. Our books were out of balance, and this is when he perpetrated his crime. He made some very simple modifications to the program that allowed him to steal money orders from us, cashing them as he saw fit. He paid his bills and this and that. He used our money orders, and with these few extra codes and the computer system that he put in there he could run these money orders through our accounting system undetected and it showed up nowhere, and since our books were not in balance at the time, this made it pretty easy for him to do it and hide the evidence.

I might point out had our books been in balance he could not have gotten away with this, but during this period of time when they were not in balance he took advantage of that. Over a several month period he cleared quite a few money orders through our bank undetected.

Mr. LUKEN. What were the dates? Over what period of time? Several months in what year?

Mr. MARRS. Well, we switched control on August 15, 1980, and I believe it was shortly thereafter that he started the program. I understand he was in the horses and he had gotten in debt and, as Mr. Faries pointed out a minute ago, he was not a hardened criminal. He was a bright young man, but he just succumbed to some financial pressures, saw an easy way to obtain the money, and took advantage of it, hoping that he could make amends before it was ever detected.

Well, things didn't work out, and he found it was easier and easier to steal the money. Like so many people, once you start doing it, it just comes.

Mr. LUKEN. Did you say what ultimately happened? Was there a prosecution?

Mr. MARRS. Yes, sir. He was prosecuted under a criminal charge.

Mr. LUKEN. Do you know what that charge was?

Mr. MARRS. It was theft. Well, maybe I should explain a little bit first.

Mr. LUKEN. Sure.

Mr. MARRS. He continued to steal money orders for several months.

Mr. LUKEN. Electronically?

Mr. MARRS. Well, it wasn't that simple. He had to go through a number of steps to pull it off, but he did use the computer and his extra code in there to help hide the crime, but after several months it became apparent.

Mr. LUKEN. Did he take other overt acts by which he could be charged?

Mr. MARRS. He found out that we were getting ready to do an audit to figure out where the money was going. Our bank account continued to diminish and we couldn't account for this so we hired our auditor to come in and figure what was going on. He found out about this and that night he broke into our building and stole some records. I don't really understand why he did it because that just tipped me off immediately, but I guess he thought maybe he could throw us off the track, and that is what he was charged with, simple theft. I forget what the other charge was.

Mr. LUKEN. Is that what he was charged with?

Mr. MARRS. Yes, sir. We found out at that time that what he had been doing was not a criminal charge. It was a civil matter, and that he could not be convicted criminally of embezzling this money.

Mr. LUKEN. So if he hadn't broken in, the substantive crimes that he had committed would not be crimes under the law as you understand it?

Mr. MARRS. As I understood it, yes, sir.

Mr. LUKEN. Where he really got away with cash, that was not a crime?

Mr. MARRS. It was a civil crime.

Mr. LUKEN. The crime was committed only in his attempt to avoid responsibility for that.

Mr. MARRS. That is why he was in jail, not because he stole the money.

Mr. LUKEN. That is the reason he was caught?

Mr. MARRS. Yes, sir.

Mr. LUKEN. Like Al Capone on the income tax. Mr. Wyden.

Mr. WYDEN. Thank you, Mr. Chairman.

I'll start with you, Mr. Marrs, and then go right down the line. First, let me thank you for coming on up today to share your views with us.

Mr. MARRS. My pleasure.

Mr. WYDEN. I think it is only human nature that nobody likes to talk about a problem.

Mr. MARRS. If it will do some good.

Mr. WYDEN. That's exactly the spirit in which we need your testimony, and I want to thank you. That is the reason we asked you to come. I think you understand that this is really what helps to promote change, so it is not just a bunch of Members of Congress talking about some kind of dry, abstract pie in the sky problem, that in the real world of small business, people run into these kinds of things.

Is there anything you think you could have done to avoid the violation of your company's computer, or at least cut your losses? I think it is always easy in hindsight to look back and say what we would have done, but what is your perception? Could you have done some things that might have cut the losses or kept it from happening the first time?

Mr. MARRS. Oh, yes, that is so true. You look back and say I wish I had only known that. First of all, if nothing else, just look over the program. By just looking it over it might be difficult to pick up on something, but if you are looking for a problem with the program, in this case it wouldn't have been hard to detect.

The biggest problem we had that allowed him to do that was our trust in this individual. Like I say, he had become a friend of mine and it never would have occurred to me that he would do so, so that is one of the hardest things to deal with. This is probably one of the biggest sources of this type of crime, embezzlement and that sort of thing, trustworthy employees getting to you. The person that you don't trust rarely has the opportunity to pull this off, whereas the person that you do trust does, and this is what happens.

Another point, as I mentioned before, was that he had to go through several steps. It wasn't just something that he told the computer to take care of. First he had to steal the money order. He would have to issue them on a computer. He would have to generate their presence on the computer. When the checks clear the bank we key them into the computer as being cleared on what day and for what amount, so he had to issue them on the computer so our clerk could put them in. If they had not been issued, the computer would not accept them when they cleared the bank, so he had to issue them first, and then after they cleared the bank he would have to check to make sure they cleared, then he would delete them off the computer, and then he went and actually stole the canceled checks. It was a multistep process.

Mr. WYDEN. He was really working at it?

Mr. MARRS. Yes, and like I say, he never would have pulled this off if he did not have my complete trust. He had stolen a validation plate, too, which is used in the machine to cut the money orders. We use a check writer to validate the money order, and it has a plate that is made up to our specifications. He had stolen one of those, so if we just had a little tighter security, it would have been much harder for him, if not impossible.

Mr. WYDEN. At your firm have you put in some additional security measures since the incident? Have you done anything different?

Mr. MARRS. No, because the employees, with one exception, are limited to our family now, who are the principals of the business. We have one part-time secretary. She is beyond reproach, but I do have a better concept of what can happen to me now. I am a little more aware. There is no need to ever doubt this part-time secretary. Again, he could not have pulled this off if our books had not been unbalanced. Currently I balance them every week. There is just no way to steal money. Someone might pull off another type of crime, but as far as embezzling money out of our account now, it just couldn't be done.

Mr. WYDEN. Do you think that most small businesses think that investing in computer security just isn't worth the money because of the capital crunch? Capital is tight. These are high interest rate times. Do people in small business just think these investments aren't worth the money?

Mr. MARRS. I am sure that is true. I know a lot of them who buy a system to start with and are not real sure that it is worth the money to even buy the computer.

Someone had mentioned earlier about counseling services. That is another expense that I am sure a lot of small businessmen would just do away with because having the system in and getting it on line to start with are pretty expensive. It is easy for the small businessman to say well, we can probably get by without this, and I'm sure a lot of them do.

Mr. WYDEN. Do you think that kind of attitude is a mistake at this point?

Mr. MARRS. Oh, yes. I think if you are going to put your business on a computer system, the principals, the owner or someone who is the management should have more than a general knowledge of computers and computer systems. They should have knowledge of the software that the system should be using so they can check for themselves. It comes down to education. If they are not familiar with the system, they really should think long and hard about putting it in.

Mr. WYDEN. What was the effect down there in Shreveport when the other small businesses heard about your misfortune? Did they go out and make some investments in computer security or did they just say well, it's his mistake and it wouldn't happen to me? Did you hear any discussion?

Mr. MARRS. No. I am not aware that anything happened.

Mr. WYDEN. Nobody even called you and said how did it happen and try to think what might be applicable to their situation?

Mr. MARRS. Most of them were just acquaintances or close business associates. I had one security company call me on it and offer his services.

Mr. WYDEN. Was it in the newspaper and what not?

Mr. MARRS. Yes. It was in the newspaper, but I am not aware of any major effect on the small businessman.

Mr. WYDEN. Thank you very much. Your testimony was very much appreciated.

Mr. Chairman, I had some questions for Mr. Parker and Mr. Faries, but I have taken a long time.

Mr. LUKEN. Proceed.

Mr. WYDEN. Thank you. I very much appreciate the Chair's indulgence. I will keep this brief.

Mr. LUKEN. I might say to the gentleman there is no need to keep it any briefer than the questions allow. We want to devote whatever time is necessary. We have the time, so the gentleman has the time.

Mr. WYDEN. Thank you. Mr. Parker, I've got your book. I hope they will put it on television and all the rest and make some sales. Maybe it will make everybody more aware in this country. This book, right there on the jacket, I think it says you are the best known computer security analyst in the world and I don't think there is any doubt you deserve the title. I got my bachelors degree at Stanford, right across from the Stanford Research Institute, and you are well known throughout California and throughout the country.

We very much appreciate your coming today, and I just have a few questions for you.

Now it is my understanding that in the 97th Congress you were over with the House Committee on the Judiciary and at that time you suggested that we establish a National Computer Crime Study Commission. Could you explain the nature and purpose of the Commission as you saw it? I guess what I am interested in particularly is H.R. 3075 and whether it addresses some of the needs that you saw could be dealt with by your proposal last year.

Mr. PARKER. Yes, Mr. Wyden. I feel that passing a Federal computer crime statute requires more exposure of the problem and more characterization of the problem other than the research studies that are being done. The idea of a task force to bring national attention to the problem and thereby gaining the support for the legislation that can do something about it was my purpose in suggesting this national task force.

Your task force satisfies many of the requirements and the functions that I was hoping and anticipating in the suggesting of that task force.

Mr. WYDEN. In your book—I better not hold it up anymore; I'll be involved in advertising as part of my congressional duties. You state that the reason for great concern is not so much the past incidents of computer crime but rather it is potential harm to society both in terms of incidence and loss. Can you explain some of the threats that you think this country is going to face in the years ahead, particularly as they relate to small business?

Mr. PARKER. Yes. One of the major problems that we face in small business is the conversion stages of changing from a previous system, maybe a manual system to an automated system, or from one state of automated system to the next one.

Mr. Marrs pointed out very dramatically that his problem occurred during his conversion period. This is the most vulnerable time for any company because their business activities are upset. As he said, the books are out of balance, and it is the time at which it is most likely to have these criminal activities occur.

In the future we are going to have a more technically educated criminal community. As you may know, almost every major prison in the United States is now teaching data processing to the prisoners. It is more common and popular than teaching lockmaking. There is an opportunity for career criminals to learn this technology and to use it in their criminal activity as well as for the amateur white collar criminals that we are now faced with mostly in computer crimes. I think that the greatest danger is going to be a more educated criminal community. The criminals can use the same computer power being used in small business today to engage in their crimes, and that is why with this great leverage the business crimes that occur are going to be much larger when they do occur, in fact, so large that it would more likely result in the complete failure of a business rather than just a pinprick or an unfortunate incident because all of the business' functions are now concentrated in that computer and in the minds and talents of a very few number of people. We are putting more trust in fewer people and more of business activities into a computer, and if that one computer fails in a small business, the business fails.

If that one computer is ripped off, if there is a crime involved in the computer, it can have far more disastrous effects than it can if the crime were done in a manual environment where paper must be shuffled and there are more people around to see what is happening and going on.

Mr. WYDEN. That was just a superb answer, and that is my judgment, too, that this mirrors the growing use of computers in society and criminals are being trained. Some of those career offenders aren't going to be able to take their skills out in the street for a while at least until they show that they are not going to commit further offenses, but I think you have given us a good understanding of this, that the problem mirrors increased use of computers generally, and it is going to require new approaches to contain it.

Do you think the SBA task force is structured properly in H.R. 3075, or are there things that you think we ought to do to improve its approach, different organizations say from the private sector?

Do we have the right people on there or do you have any suggestions at this point for us with respect to the legislation?

Mr. PARKER. I thought that it seemed to be explicitly overweighted with Federal representation, although there is a provision for private sector representation as I understand it. I wouldn't include the DOD. I don't really see a purpose in having the Department of Defense involved in this task force. The National Bureau of Standards, however, does play a very important role. While their work is primarily aimed at Federal agencies, their guidelines are used very extensively in the private sector, and it would be useful, but I think it is particularly important to get the people on the task force from the private sector who know the problem. The task force would have far more weight and be looked at with more attention if it did have more private sector representation.

Mr. WYDEN. We intend that it will. It is a little bit hard in Federal legislation to enumerate that kind of thing, but let me state now as I did when I introduced the legislation, that the task force will have a broad-based group of private representatives on it, and I think you make the case for it in a nutshell. If we want credibility with the private sector, if we want credibility with the small business community, we have got to get people who are outside of Washington. You can guess with the Department of Defense we put them on because the whole Federal budget practically involves the Department of Defense these days in some respect or another.

The last question I have is: Are there figures available as to the number of computer crimes committed in relation to the number of computers in the country?

Mr. PARKER. In fact, I have tracked down the source of numbers Sergeant Faries quoted and I know the individuals who stated them. I can assure you that they were essentially pulled out of the air, that they were guessed at, and as I say, any numbers today are simply not valid.

However, we do not have to have these statistics in order to identify this as a serious problem. Even though I understand that the world is number crazy, you give someone a number and you are an instant expert. You have settled an argument and established a fact, whether the number is meaningful or not. I like 85.6, by the way. It's a very nice number; I use it all the time.

Twelve is a good number, too, but the point is that I don't think we should try to get into this numbers game, and I understand that from the legislative point of view if you have got numbers you have got something to hang your hat on, but we are simply not going to get it because in my experience at least most people do not come forward when they are victims of these crimes because it is embarrassing. They will lose more money from the embarrassment and lost business than they will from the crime itself. They look at what has happened to them and they realize that someone else could do the same thing to them, so they keep it secret. They look at the problem and they say that the prosecutors, the justice community won't accept the case, and in fact we have instances where the local prosecutors simply tell people who come to them with computer crimes to go away. They say: "I don't understand computers. I don't understand what has happened to you. Don't bother us. We have many more rapes and murders to deal with." So I

think it is important, as Sergeant Faries pointed out, that education is extremely important to foster, and your bill, and this task force, and the resource center concept is an important way to get that education out there.

Mr. WYDEN. Let me ask you one other brief question I could just listen to you the entire day, frankly, and the Chair has really been too kind in letting me ask all these questions, but one of the things that we heard is that innovation in data processing is occurring much more rapidly than innovation in security technology—that the gap is in effect growing greater. Is that correct?

Mr. PARKER. Well, it is a little bit more complicated than that. The technology is growing as you say exponentially. However, we are also making very great strides in the technical aspects of security. We have a huge array of very powerful controls that we can put into computers, around them, and into the computer programs. The problem is getting people to understand that we have these very low cost, very powerful controls.

The problem is that we are dealing with a people problem here, not a technical problem, and the problem has to do with advancing the administrative and management controls, as Dr. Katzke mentioned, to keep up with this advancing technology. It is the human factors and the human controls that have to be advanced that will go along with the increasing vulnerability that is created by this concentration of assets in a fragile form inside computers and squeezed through telephone lines.

Mr. WYDEN. Thank you, Mr. Parker. Thank you, Mr. Chairman.

Mr. Faries, you were just excellent, and I ought to let the Chair start with some questions for you. We very much appreciate your comments.

Sergeant FARIES. Thank you.

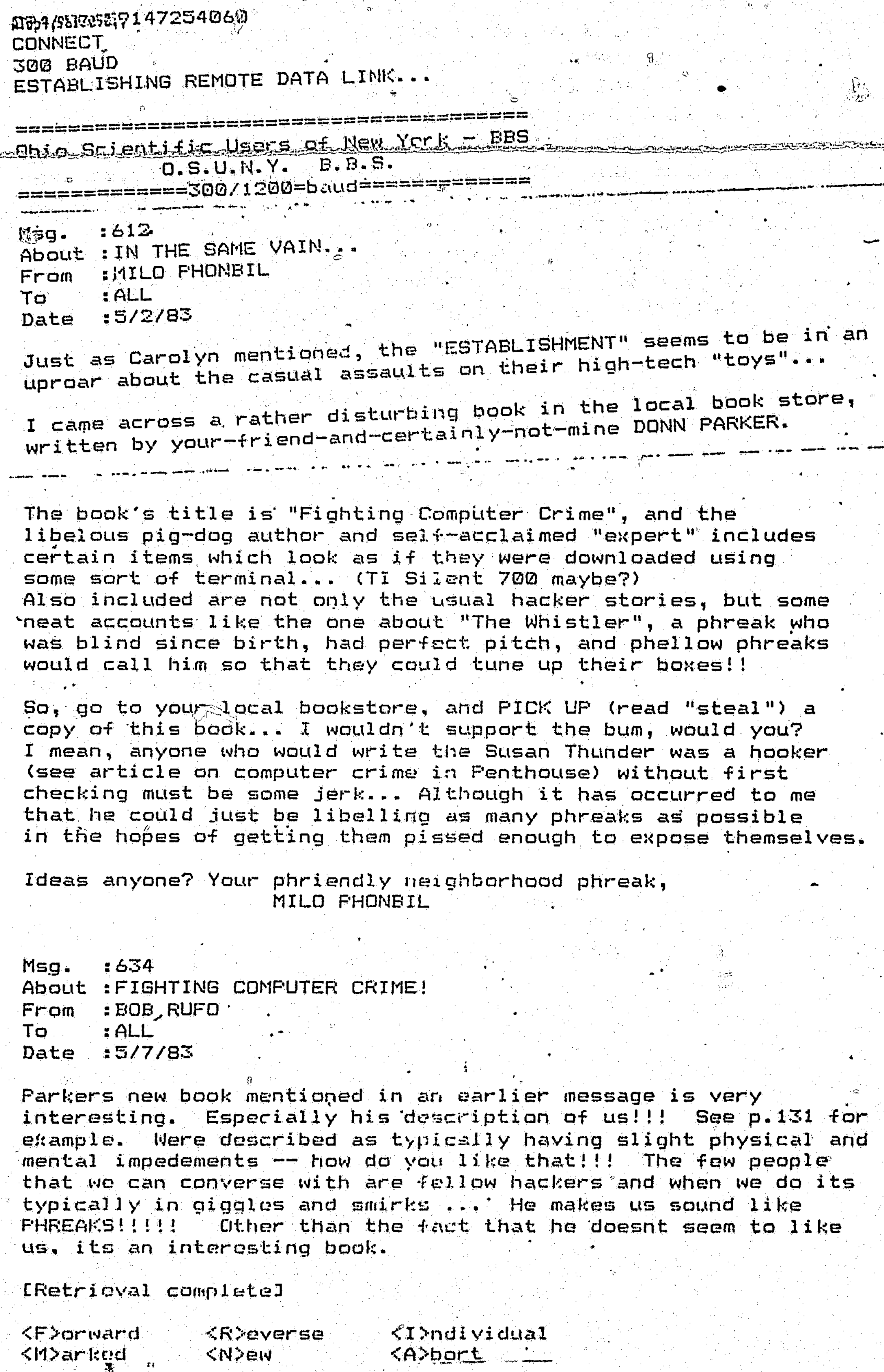
Mr. LUKEN. Mr. Parker, someone just handed me the Ohio Scientific Users of New York. Are you familiar with this?

Mr. PARKER. Yes, I am.

Mr. LUKEN. Was this done maliciously?

Mr. PARKER. Yes, it was.

[The document referred to above follows:]



```
[illegible]9147254060
CONNECT
300 BAUD
ESTABLISHING REMOTE DATA LINK...

=====================================
Ohio Scientific Users of New York - BBS
            O.S.U.N.Y.  B.B.S.
=============300/1200=baud=============

Msg.   :612
About  :IN THE SAME VAIN...
From   :MILO PHONBIL
To     :ALL
Date   :5/2/83

Just as Carolyn mentioned, the "ESTABLISHMENT" seems to be in an
uproar about the casual assaults on their high-tech "toys"...

I came across a rather disturbing book in the local book store,
written by your-friend-and-certainly-not-mine DONN PARKER.


The book's title is "Fighting Computer Crime", and the
libelous pig-dog author and self-acclaimed "expert" includes
certain items which look as if they were downloaded using
some sort of terminal... (TI Silent 700 maybe?)
Also included are not only the usual hacker stories, but some
neat accounts like the one about "The Whistler", a phreak who
was blind since birth, had perfect pitch, and phellow phreaks
would call him so that they could tune up their boxes!!

So, go to your local bookstore, and PICK UP (read "steal") a
copy of this book... I wouldn't support the bum, would you?
I mean, anyone who would write the Susan Thunder was a hooker
(see article on computer crime in Penthouse) without first
checking must be some jerk... Although it has occurred to me
that he could just be libelling as many phreaks as possible
in the hopes of getting them pissed enough to expose themselves.

Ideas anyone? Your phriendly neighborhood phreak,
                    MILO PHONBIL


Msg.   :634
About  :FIGHTING COMPUTER CRIME!
From   :BOB RUFO
To     :ALL
Date   :5/7/83

Parkers new book mentioned in an earlier message is very
interesting.  Especially his description of us!!!  See p.131 for
example.  Were described as typically having slight physical and
mental impedements -- how do you like that!!!  The few people
that we can converse with are fellow hackers and when we do its
typically in giggles and smirks ...  He makes us sound like
PHREAKS!!!!!   Other than the fact that he doesnt seem to like
us, its an interesting book.

[Retrieval complete]

<F>orward      <R>everse      <I>ndividual
<M>arked       <N>ew          <A>bort
```

Mr. LUKEN. Would you describe that to us?

Mr. PARKER. Well, there is an epidemic across the country of what is known as juvenile system hacking. It is otherwise referred to as electronic vandalism. It is characterized in the new movie called "War Games." There are thousands of young people in high school and college gaining very powerful technical capability as they learn about computers and technology.

A few of them are using that technology to engage in unauthorized attacks on computer systems that are attached to telephones, and they are also using electronic bulletin boards as a means of communicating intelligence. When one of these juvenile delinquents obtains telephone numbers and passwords into a computer system, he immediately dumps it into the electronic bulletin board so that all across the country thousands of kids will get the same information and then can attack the same system.

We are currently doing a study on this for the Department of Justice. System hacking mostly stems from the phone freaking of the 1960's. It is trying to be a hero, trying to outdo their associates. As I say, it is vandalism. It is mischief primarily, but it has resulted in some very serious criminal cases, and there are some juveniles who are now in custody as a result of engaging in some of these serious attacks.

The electronic bulletin board is where the review of my book appeared, and those system hackers are quite unhappy with it because I exposed them.

Mr. LUKEN. So this is the electronic bulletin board?

Mr. PARKER. That's right. That is where it came from.

Mr. LUKEN. Well, this disparages you and your book.

Mr. PARKER. I am very happy for that as well.

Mr. LUKEN. I guess it is not criminal in itself, is it? Libelous, perhaps?

Mr. PARKER. Perhaps.

Mr. LUKEN. Maybe you shouldn't say perhaps, but other than being libelous, it is not criminally so?

Mr. PARKER. No, I don't think so.

Mr. LUKEN. It is just that they were able to give it wide circulation by getting into these electronic bulletin boards? Would you describe how they circulated that in greater detail?

Mr. PARKER. Yes. An electronic bulletin board is simply a small computer that has been set up with dial-up telephone access to the computer. I might say there are very legitimate uses for electronic bulletin boards as well. The juvenile system hacker gets on his terminal, dials into the computer using the telephone number and on his terminal he can then type messages into the bulletin board. He can also see all of the messages on the bulletin board and displayed on his terminal including telephone numbers and all of the intelligence necessary for making unauthorized access to computers all over the country and to engage in other kinds of mischief.

Mr. LUKEN. What system is this?

Mr. PARKER. That is one that is available apparently throughout the State of New York. There are hundreds of these bulletin boards. Every large city has at least a dozen or so of them.

Mr. LUKEN. Who operates them?

Mr. Parker. Many of them are operated privately by individuals who just are having fun in providing them. Computer stores offer them and provide assistance through them to their customers. Computer clubs all over the country have established these bulletin boards. Hackers also engage to a certain extent in software piracy through the bulletin boards, that is they provide information about how to steal copies or make unauthorized copies of packaged computer programs.

Mr. Luken. What is the technology? How do they connect?

Mr. Parker. They connect up through a dial-up telephone that is connected to the computer. On the other end a system hacker simply dials on the telephone and when he gets to the computer he hears a computer tone and knows he has arrived at a computer. He puts the telephone handset into a cradle of a modem and he turns on his terminal and immediately he receives the initial information that the computer provides in answering its telephone and it says something like welcome to the x, y, or z bulletin board. What is it that you would like to do? Here is a menu of our functions.

Mr. Luken. This all goes over the telephone wires?

Mr. Parker. That is correct.

Mr. Luken. That is what we are talking about?

Mr. Parker. Yes.

Mr. Luken. All courtesy of Ma Bell.

Mr. Parker. Many of those computers are in small businesses and hooked up to the dial-up telephone system which makes them particularly vulnerable to this kind of attack.

Mr. Luken. Can you see other uses for this, other criminal or nefarious uses besides this vandalism type of thing?

Mr. Parker. Yes.

Mr. Luken. More mischief?

Mr. Parker. Yes. We know of some Fagans, adult leaders of these juveniles who are urging them——

Mr. Luken. You better explain to the gentleman from Oregon. Go ahead.

Mr. Parker. Adults encouraging these juveniles to engage in this kind of thing primarily for the theft of copies of computer programs that are protected as trade secrets or by copyright and so there is a commercial crime aspect.

Mr. Luken. You are still in the area of juveniles, though.

Mr. Parker. But there are adults engaged in this activity as well. It is not just limited to juveniles.

Mr. Luken. This is primarily a prankster kind of thing?

Mr. Parker. It has started that way. The most serious problem is that it is creating the subculture and very unhealthy values among these kids who are going to be programing the computers in our banks in another 5 years. We are concerned that they are gaining a set of values that says it is acceptable to do this kind of thing.

Mr. Luken. But at the moment you cannot perpetrate a white-collar crime on them?

Mr. Parker. Oh, yes, you can.

Mr. Luken. Through this system?

Mr. Parker. Yes.

Mr. Luken. How?

Mr. Parker. For example, we have one case where a 17-year-old got on his terminal and found his way into a leasing company business in San Francisco. He proceeded to spew dirty words throughout the file of inventory of products for lease. He put them out of business for 1½ days. They lost $60,000. It cost another $200,000 for them to gain the attention of the criminal authorities and to find this kid and stop him, so it was a considerable loss to them.

Mr. Luken. Was he charged with a crime?

Mr. Parker. Yes. He was charged with a crime and convicted.

Mr. Luken. What crime?

Mr. Parker. He was charged under the California computer crime law, a new law that was instituted in 1980, and he was successfully convicted of a crime.

Mr. Luken. If he had been in a State that didn't have a new law like that he might not have been charged with a crime?

Mr. Parker. I believe that to be the case, that's right.

Mr. Luken. Well, I think that is very helpful to me because it is illustrative of the situation. Anything else?

Mr. Wyden. Not from me, Mr. Chairman. Thank you.

Mr. Luken. All right. We thank all of you. Your testimony has been excellent, and extremely helpful to us. We thank you for what you have been able to offer to us today.

Finally we have Mr. Donald Devine of Comshare, Inc., the chairman of the software protection committee of ADAPSO.

Mr. Devine, I believe we have your written testimony.

Mr. Devine. Yes, you do.

Mr. Luken. Without objection, it will be received. We will place it in the hearing record at the end of your testimony.

TESTIMONY OF DONALD J. DEVINE, GROUP VICE PRESIDENT, COMSHARE, INC., AND CHAIRMAN, SOFTWARE PROTECTION COMMITTEE, ASSOCIATION OF DATA PROCESSING SERVICE ORGANIZATIONS

Mr. Devine. Thank you. Mr. Luken. When I was young, my grandfather took the time to tell me how hard he had it when he was a kid. He had been born in 1872 and was raised on a prosperous farm in Pennsylvania. They didn't have any electricity and didn't have central heat and they had a pump in the side yard and an outhouse. During his life he saw a lot of changes take place.

He saw his family get indoor plumbing, telephones, and electricity. My father saw his family get an automobile and a radio, and I can tell my kids that I can remember when we didn't have a television set at home.

Well, I have got a computer at home, but I got it just recently, and my children can tell their children that they can remember when we didn't have a computer at home.

My purpose in this digression is to say that we have got a continuum here of technological change. The evolution of computer technology is just one part of this continuum. The computer is becoming much more common in all aspects of our daily lives and all aspects of business. It has finally reached the economic point where it is becoming quite common in small business.

As the computer becomes more common it is itself not creating more crime, but it is getting involved in crime. This is particularly true because a computer has two features that make people more willing to use a computer when committing a crime. Those features are information and control.

First, with respect to information. People put their most valuable information into a computer. Information like how much money they owe other people, how much money other people owe them, how much money they are paying in salary, and all of that is called the accounts payable, the accounts receivable, and the payroll. There are other things as well. That information has great value to anybody who wants to commit a crime against that company. They need access to that information either to commit the crime or to cover up the crime which they have already committed.

The second aspect is control. There has been a lot of discussion in earlier testimony about control. People are tending to put almost their entire control mechanism on the computer. That is the control mechanism which keeps track of who made what changes when, who was authorized to make what changes, and whether or not the books are in balance. But when all those controls are in one place, it is quite possible for someone who is competent and trusted like the person that Mr. Marrs talked about to get access to that computer and to circumvent those controls and either cover up a crime or commit a crime. In that way the computer is becoming a focal point in crimes against small businesses. It has the information and it is the central point of control.

Now that computers have become less expensive, small businesses everywhere are getting them but they don't understand well enough how to use the computers. They also don't understand how to keep the computers from being used improperly either accidentally or on purpose. There is a large need for education.

There are four things that people need to be concerned about with this education. The first one is how to deter computer crime and accidental misuse from taking place.

The second one is how to tell very quickly when computer crime or accidental misuse has taken place in order to minimize the loss.

The third one is how to plan or insure for the recovery from the consequences of having been the victim of computer crime or accidental misuse.

Fourth, a lot of people in small business are themselves perpetrators of computer crime because they don't understand that they are doing something wrong when they improperly copy or use or distribute certain licensed or copyrighted program material. They might have acquired this material from a store or from someone who himself did not acquire it properly.

Basically I would like to make the following suggestions for this legislation.

First, I very much endorse the shorter time period of 18 months because I think changes are taking place so quickly that we must have a sense of urgency. If we are not urgent, we are going to have a report that will be out of date before it is completed.

Second, I very much endorse the participation of the private sector on the task force, in particular people in the software industry who are doing a great deal today to build safeguards and controls into packaged software which is used by small business.

Last, I would see the focus of the task force be aimed at improving for small businesses (a) the methods of detering computer crime, (b) detecting the incidents of computer crime, (c) advice on plans and techniques for recovery for being the victim of computer crime, and finally (d) the information on how to avoid being a perpetrator of a computer crime through the misappropriation or misuse of licensed or copyrighted software.

That is the essence of my testimony which is given in the prepared statement. I will be happy to answer any questions.

Mr. Luken. Well, how about the question of definition of a computer crime? Has that been something that you have considered at any length?

Mr. Devine. I have, and it is not easy to define because essentially the computer is just a tool which can be used in committing many other types of crimes which have been around traditionally.

In addition, there are crimes which relate to the changing or destruction of information which I don't believe are adequately defined in the statutes today and which permit people to do some things which have very serious repercussions to small business. They may be malicious things or they may be covering up a crime or they may actually be assisting in the production of incorrect checks or money orders or something like that.

Mr. Luken. Are you familiar with the California computer crime law or a similar one?

Mr. Devine. I am not personally familiar with that law. I have heard thirdhand some very good comments about it, and I certainly endorse the attention of all of the states to legislation like that.

Mr. Luken. Do you know what it basically does? Is it similar to our Federal statutes that make it a crime to do anything that is usually a crime by reason of larceny or anything? If it is done by wire, if it is done by interstate transportation in an automobile or if it is done by wire or some of the other means is it that kind of a statute that it says theft by use of computer is a crime?

Mr. Devine. I am not familiar with the details of it. It is my understanding, however, that it is relatively bold and includes statements that make certain manipulation and destruction of data a criminal act as well as performing other acts with the computer which would be criminal, that it does include making it illegal to change data which you are not authorized to change. I believe that Mr. Wyden, for example, earlier talked about someone who puts a time bomb in a program so that the accounts receivable would all be forgiven at the end of 6 months.

Mr. Luken. How would you protect against that? Is there any way?

Mr. Devine. Well, there are several things that you should do.

Mr. Luken. I think you described earlier that the more protections you put in, the more trust you need in whomever is in charge of those protections. Also, the more centralized it becomes, the greater the possibility for subversion.

Mr. Devine. There are several things you can do. I believe the most important thing you can do is to invoke management controls very similar to what you do have done ordinarily if these were manually controlled books or manually controlled inventory or manually controlled accounting system. You don't want to allow a single person to be the only one who knows what is going on in your business. You want to have reports produced. You want to balance your books each day. You want to keep audit trails of the transactions that have been made, who made them, when they were made. With that information it is possible if your computer blows up or your computer dies or if someone commits computer crime to go back and reconstruct the steps which got you from where the books were last correct to the point where they were in error or were destroyed.

Mr. LUKEN. That would be rather hollow advice for a small business that just doesn't have enough personnel for more than one person.

Mr. DEVINE. With a very small business, it is not so much a problem because the person operating the computer would have to himself be the criminal and also be the victim, unless it was a crime against a taxing authority or some such thing as that. With a small business my recommendation is very much along the lines of Mr. Marrs' testimony, that the principals need to be involved and understand what is going on inside the computer, and at least one of the principals needs to have a good understanding of the computer technology. He does not have to be a super expert but needs to be more than just casually informed about what is going on with the computer.

You are making an investment when you put a computer in. You are investing your business in a computer and you are relying upon it, and just as you would not rely on some other important piece of machinery in your factory that no one in your company had any knowledge or experience with, you should not rely upon an important piece of machinery in the accounting department of your business that you don't have at least one person who has some knowledge and experience with. It must be a person of trust. If it is a small business, it should be one of the principals. If it is not a small business, you should partition the work to where there are checks and balances and more than one person would have to be in collusion in order for a computer crime to take place. Then you also need to have good controls in the form of backups and audit trails, that is, lists of transactions that took place so that you would be able to do a recovery or a diagnosis of the problem.

Mr. LUKEN. Well, do you think the Small Business Administration would be helpful in providing those kinds of guidelines?

Mr. DEVINE. I believe it is principally a matter of fostering education. It is the most important thing that can be done.

I also believe, by the way, that education is needed not just in small business. We need education of law enforcement people, people in the judiciary, and people in the areas of prosecution. They have to understand this as well so that when computer crime does occur, small businesses are able to turn to the authorities and the agencies of government, both State and Federal, to get things done. The education has to take place both at the level of the small businessman and in the various agencies of government.

In addition to that, there do need to be some changes in legislation, and those changes in legislation I believe are principally State problems as opposed to Federal, although I am not really an expert on that. What we need to do is to see to it that crimes against data, crimes where data has been misappropriated or destroyed or changed either to cover up or cause a crime to take place are in fact themselves criminal acts and that people will be tracked down and prosecuted in those areas.

It is my belief that a lot of this will still be taken care of by education, and by good management procedures, but we need both. We need a balanced approach, both education and legislation.

Mr. LUKEN. Well, you said that you believe it is primarily a State matter. Do you think States can accomplish very much? States are by their very nature different in size and therefore different in amounts of resources.

Mr. DEVINE. I think it is largely because many small businesses are in fact so small that they are involved only in business within a given State and they have tended to look to the State for the kind of assistance they need both legislative and law enforcementwise.

Mr. LUKEN. We are the Small Business Committee.

Mr. DEVINE. I would just like to see the legislation take place. It is my opinion that we would be much, much better off with legislation uniform throughout the United States as opposed to different in each State because those companies which are in more than one State or those of us who are in small businesses that provide software to other small businesses and have the Nation as our marketplace would benefit from uniformity. I much prefer uniformity.

Mr. LUKEN. Mr. Parker described a computer crime that was committed that was able to be prosecuted because California was a progressive enough State. It had a computer crime law of 1980. If this occurred in South Dakota, the perpetrator might go scot-free.

Mr. DEVINE. That would be very unfortunate. We should have a national law.

Mr. LUKEN. For guidelines?

Mr. DEVINE. Yes. That would be quite advantageous.

Mr. LUKEN. The gentleman from Oregon.

Mr. WYDEN. Thank you, Mr. Chairman. Mr. Devine, I know you are an authority in this field, and I apologize for missing some of your testimony, and I am very appreciative that you stressed education because I think that is the key. It is education that includes small business but also includes general use of computers.

Could you give us, specifically, your thoughts how this education should be conducted? Do you think the Government should put on classes? Do you think we should just get out of it and suggest to the private sector they do it? Exactly how can we educate people to these issues and given the fact you and I are in agreement that education is the key, how would you best like to see that done?

Mr. DEVINE. Well, first of all, I would like to see the education appear through every available channel, and I don't mean to restrict any channels.

Mr. WYDEN. No difference of opinion there.

Mr. DEVINE. I believe that the education will be effectively handled a number of ways. First of all, trade associations are paying a great deal of attention to this and they should be encouraged to spend more time paying attention to it because the specific problems that small businesses face vary by industry. Those businesses which are principally in the electronic handling of moneys, those which are in the inventory or manufacturing businesses tend to have somewhat different profiles of risk, and so it would pay for trade associations to do this.

Individual software companies, hardware companies, people who are consultants to small business are already paying much more attention to education of small business. More needs to be done there. The education community itself is making people much more computer aware. I would even go so far as to suggest using the elementary and secondary school districts throughout the United States. We need to have more training in how computers are properly used and how to avoid their improper us, either accidental or intentional. We must have a computer literate society. Computers are going to be everywhere in the future.

I think those are some of the principal methods of doing it. I won't want to cut off any other successful method of training.

Mr. WYDEN. Let me ask you about the clearinghouse in this bill because I see the benefit of that as primarily education. What we want to do is in effect make sure that as the most current, most up-to-date kinds of approaches come on line, we can get those out across the country, that it would be in effect the most current guide to the security remedies at that time. We don't want to duplicate anything else, but we feel that some place in the United States you ought to be able to have this clearinghouse that can be the latest up-to-date information place to turn to, and I see that as educational.

Do you think that is a viable approach? Is that something you can go along with?

Mr. DEVINE. I do. I go along with that. I feel that it will be most effective if it recognizes that there are third party conduits as opposed to attempting to send information directly to individuals in private industry. I don't think that will work very well. It will be very expensive and I don't think it will work very effectively.

Instead I would see the clearinghouse giving information to whatever organizations have the initiative to undertake this necessary education. They may be trade associations and they may be others.

Mr. WYDEN. One other quick one. Again I'm sorry I missed some of your testimony, and I am going to read it carefully.

Do you think that it is important that the small businesses in particular insure themselves against computer crime losses? Is that another area of education that is not really being done at this point and we ought to do it and get the word out that it can be helpful?

Mr. DEVINE. The answer is unequivocally yes. I feel that some existing insurance already overlaps this coverage and that work needs to be done in the insurance industry to more clearly define these risks and to provide packaged coverage for small business. For example, fidelity insurance which is aimed at a trustworthy employee who potentially goes astray, embezzles, would cover this kind of risk. I do believe that small businesses should insure.

Mr. WYDEN. Thank you, Mr. Chairman.

Mr. LUKEN. Can you tell us any more about the subject of insurance? The insurance aspect of it alone is vast, I am sure. When you say fidelity coverage where the employee benefits, that would cover no matter what the method used, wouldn't it?

Mr. DEVINE. That's right, and it is my belief that all businesses should also assess their risk and should determine what their probability of those risks are and aren't and what the impact of those risks would be, and to have a plan for all of their highly likely risks, or high impact risks, those risks that would put them out of business.

Mr. LUKEN. They might not have coverage, for the vandalism aspect of it. That might fall through the cracks.

Mr. DEVINE. There is coverage which is presently offered which is a data processing media insurance which most small businesses do not understand and which is not well aimed at them.

Mr. LUKEN. We understand that they don't understand because we might not understand.

Mr. DEVINE. But there are some pieces of coverage. Essentially the insurance industry has not adequately packaged many of the coverages which it already offers, so that they are aimed at these risks, but instead they just have a number of offerings today which somewhat overlap. There are holes and many businesses are faced with these gaping holes in their insurance coverage.

I think adding a representative from the insurance industry to your task force would be a very worthwhile activity, and I think we should do everything we can to encourage the insurance companies to package their offerings specifically for this need.

[Mr. Devine's prepared statement follows:]

PREPARED STATEMENT OF DONALD J. DEVINE, GROUP VICE PRESIDENT, COMSHARE, INC., AND CHAIRMAN, SOFTWARE PROTECTION COMMITTEE, ASSOCIATION OF DATA PROCESSING SERVICE ORGANIZATIONS

I am Donald J. Devine, Group Vice President of Comshare, Inc., representing ADAPSO, the national industry association of the computer software and services firms. Comshare provides computer software and services to business of all sizes throughout the U.S. and western Europe. At present, I am the president of ADAPSO's Microcomputer Software Association and the Chairman of ADAPSO's Software Protection Committee. I have been working in computer software and services since 1957 at a variety of positions in both large and small business.

THE NATURE AND SCOPE OF COMPUTER CRIME

There is no single good definition of "Computer Crime". It means different things to different people. I consider it simply to mean that the use of a computer is materially involved in a crime. Examples are (a) theft or copyright infringement of information stored on computer tapes or diskettes, (b) authorized destruction or alteration of such information, and (c) modification of computer programs or computerized information either to cover up a crime or cause a crime to be committed. This last category seems to get the most publicity. It includes crimes like adding a fictitious person to the payroll list with the computerized checks being mailed to the criminal's address, or changing the computerized record of the inventory level to cover up for the television sets that have just been hijacked.

Each of these has its analog in non-computer crime—(a) property theft or copyright infringement, (b) property damage, and (c) embezzlement, malfeasance, doctoring the books, covering up for a hijacking, etc. They are the same old crimes we have faced before. The only difference is that a computer is materially involved.

I do not include violent crime as computer crime. The physical destruction of a computer or its peripheral equipment is just another property crime. The special characteristics of a computer are not materially involved. Even though computers can be used to support a violent crime like keeping track of assassination targets or planning a terrorist raid, I don't think of these as materially computer actions. The violence or intended violence itself is the crime. The computer itself, like a pencil and paper or a pocket calculator, is only a tool. To me, computer crime is largely intellectual crime.

Computers are becoming increasingly more involved in all aspects of our lives, including our business. This trend will continue and soon virtually every business, and most homes too, will be using computers as part of their standard equipment. The inevitable result will be that computers will become involved in increasingly larger numbers of crimes. I do not believe that computers are making the incidence of crime go up, only that computers are becoming more involved in everything that happens in the U.S., including crimes.

Computer crime is discouraged relatively well in larger companies through their electronic data processing (EDP) auditing function, security procedures, and other extensive internal and external auditing activities. When computer crime does occur in a larger business, it is usually detected relatively quickly. Quick detection and contingency plans usually keep the damage relatively low. Many larger companies are now well insured against loss from these intellectual crimes which might materially involve a computer.

Computer software "piracy" is a relatively new crime because computer software is a relatively new commodity and it is not well understood by the general public. Many people do not realize that the improper copying, use, or distribution of computer software is a criminal act which greatly damage the computer software industry. Many software authors who are damaged by this "piracy" are in small business. Many of the perpetrators of this crime are in other small businesses. Education and enforcement are both needed on this matter.

HOW IT IS SPECIFICALLY A SMALL BUSINESS PROBLEM

Computer crime is not only a small business problem. Generally, I do not think it is any more a small business problem than it is a large business problem. However, the problem is somewhat different for small businesses and for others, principally because small business have less understanding of computers in general and computer crime in particular, and consequently they are less prepared to deter it, detect it, and recover from it.

Small businesses are rapidly computerizing now. In addition to the order categories of mainframe computers and minicomputers, we now have more than 100,000 powerful yet surprisingly inexpensive microcomputers being sold in the U.S. each month. A large percentage of these are being used in business. For the first time, smaller businesses find that they can readily afford to use computers extensively.

A larger proportion of people in small businesses are novices at using computers. They don't yet understand well enough how to use computers effectively to help them in their business, how to safeguard their valuable information and how computers might be misused either accidentally or intentionally to commit a crime. They also do not understand how they may be committing a computer crime themselves in "pirating" software.

Small business people need to be better educated in all aspects of using a computer, including the risk that they may become victims of computer crime or perpetrators of computer crime. Although this education problem is more serious for small business, there is also an education problem in large businesses related to the controlled and proper use of the new microcomputers and their software.

I have trouble separating the education about computer crime from the education needed about computers and their usage in general. Instead I see it as a broad education need, with most of the general public in the U.S. sharing that need.

Small businesses need to be educated about computer system control procedures. They must recognize the need, and know how to implement and operate good computer system control procedures. Once automated, there are usually fewer people who are knowledgeable about the smaller company's important, and now computerized, business systems—like accounting, inventory, or other recordkeeping. Control procedures are often more lax because people tend to have a strong belief in computer accuracy and reliability. This tends to make it easier for someone in a position of trust, who is knowledgeable about computers, to commit a computer crime against the company.

Computer hardware and software companies as well as business consultants specializing in computer systems are providing private sector help in this area now. More attention needs to be paid to this, but I am confident that the private sector will continue to improve the services it is offering. The private sector vendors will rise to the occasion in this evolving market. They are clearly doing so now in the form of programmed control and audit procedures which are becoming more common in commercially available software packages, for example.

Small businesses rely on local law enforcement agencies. These, too, are largely untrained to deal with computer crime. Prosecutors and the state and local judiciary are also poorly prepared to deal with computer crime. Again, this is an education problem. It affects small business much more heavily than it affects larger businesses. Larger businesses generally have specially trained staff which is competent to detect computer crime, collect evidence, and support law enforcement agencies. In addition, they have the money to hire experts to assist in prosecution. However, they seem to undertake civil actions instead of criminal actions in many cases, or simply discipline or discharge the culprit without involving the judiciary at all.

THE APPROPRIATENESS OF H.R. 3075

This is a passing problem, resulting from a rapid evolutionary change in some business practices in response to changing technology. The trend of computerizing small business is so powerful that we couldn't stop it, even if we tried. And, of course, we don't want to stop it; we want to foster it because it is very good for America.

The private sector of the U.S. economy is resilient and adaptable. On the whole, the trend by small businesses to more highly computerize their operations will be a great success. The problems associated with this evolutionary change will all be handled by the normal mechanisms of the economy in due course. Our free enterprise economy is very good at identifying needs and satisfying them quickly. We can already see that happening with this problem.

The government can help and can avoid hindering this process. One thing we should always do is to keep the private sector involved. H.R. 3075, the Small Business Computer Crime Prevention Act, is very narrowly focused, which is good. It also creates a Temporary Task Force to study and deal with a specific problem. Since the problem is temporary, the temporary nature of this Task Force is important.

HOW H.R. 3075 CAN BE IMPROVED

If passed, H.R. 3075 should be aimed more precisely at computer crime, with an objective of helping the private sector and existing government agencies to deal with this problem more effectively and more quickly, and equally important to be sure the government does not delay or increase the cost of the developing solution to this problem.

The composition of the Task Force should be amended to include representatives from the private sector, specifically people from the computer software industry and the computer hardware industry.

Section 3 of H.R. 3075 should be modified to focus the purpose of the Task Force on how computer crimes against small businesses can be more effectively deterred and detected, and how small businesses can better prepare themselves to recover from the adverse consequences of computer crime when it occurs. The general answer is the improvement of procedures, programs and equipment, and education of small business on how to employ these procedures, programs and equipment effectively. Fostering education is the most important aid the government can provide. Formal standards and more regulation are not needed. They will be counterproductive.

In general, more education on the proper (and dealing with the improper) use of computers is needed throughout the American community. In addition to the general public, legislators, law enforcement offficals, prosecutors, and the judiciary need to be more computer aware. As this happens, it will benefit small businesses generally in their dealings with computer crime, and it will benefit small business microcomputer software companies whose products are often improperly appropriated today.

Mr. WYDEN. I couldn't agree with you more.

Mr. LUKEN. The insurance companies are facing exploding technologies on a number of fronts, aren't they?

Well, in any event, the House is in session and fortuitously we have now been able to complete this glimpse into the problem, and we thank you, Mr. Devine, for your insightful testimony. As to the others, all of whom were extremely helpful today, I hope that we can continue to work with you and to rely upon your good counsel as we have today. Is there anything further?

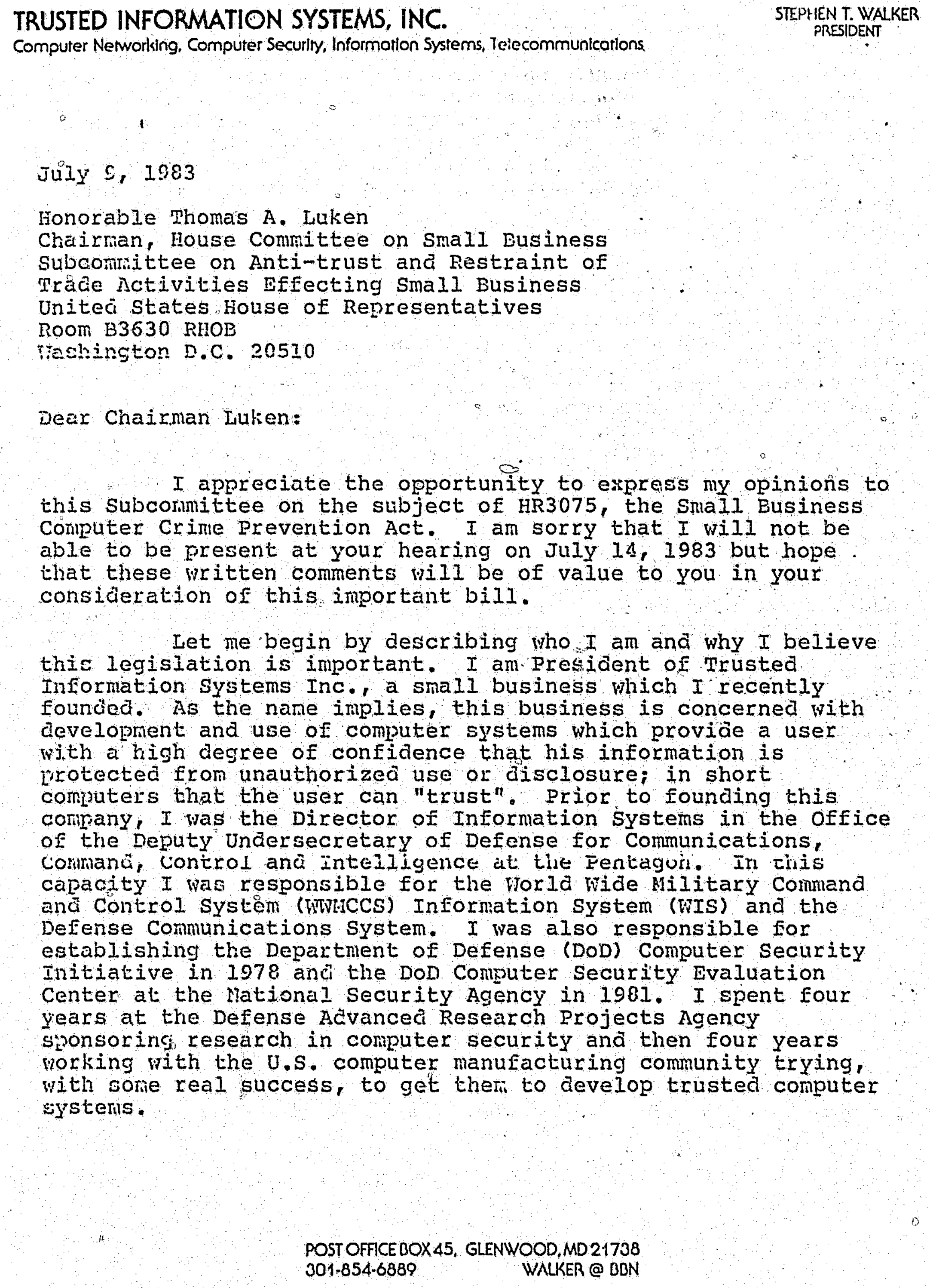
Mr. WYDEN. Not from me, Mr. Chairman; again, Mr. Chairman, I just want to tell you how much I appreciate your making this hearing possible.

Mr. LUKEN. Well, we thank the gentleman for introducing the legislation and getting this very necessary and beneficial activity started, so the subcommittee will be adjourned, subject to the call of the Chair. We will leave the hearing record open for 30 days for additional comments.

[Whereupon, at 12:10 p.m., the subcommittee adjourned, to reconvene subject to call of the Chair.]

APPENDIX

APPENDIX A.—PREPARED STATEMENT OF STEPHEN T. WALKER, PRESIDENT, TRUSTED INFORMATION SYSTEMS, INC.



TRUSTED INFORMATION SYSTEMS, INC.
Computer Networking, Computer Security, Information Systems, Telecommunications

STEPHEN T. WALKER
PRESIDENT

July 9, 1983

Honorable Thomas A. Luken
Chairman, House Committee on Small Business
Subcommittee on Anti-trust and Restraint of
Trade Activities Effecting Small Business
United States House of Representatives
Room B3630 RHOB
Washington D.C. 20510

Dear Chairman Luken:

I appreciate the opportunity to express my opinions to this Subcommittee on the subject of HR3075, the Small Business Computer Crime Prevention Act. I am sorry that I will not be able to be present at your hearing on July 14, 1983 but hope that these written comments will be of value to you in your consideration of this important bill.

Let me begin by describing who I am and why I believe this legislation is important. I am President of Trusted Information Systems Inc., a small business which I recently founded. As the name implies, this business is concerned with development and use of computer systems which provide a user with a high degree of confidence that his information is protected from unauthorized use or disclosure; in short computers that the user can "trust". Prior to founding this company, I was the Director of Information Systems in the Office of the Deputy Undersecretary of Defense for Communications, Command, Control and Intelligence at the Pentagon. In this capacity I was responsible for the World Wide Military Command and Control System (WWMCCS) Information System (WIS) and the Defense Communications System. I was also responsible for establishing the Department of Defense (DoD) Computer Security Initiative in 1978 and the DoD Computer Security Evaluation Center at the National Security Agency in 1981. I spent four years at the Defense Advanced Research Projects Agency sponsoring research in computer security and then four years working with the U.S. computer manufacturing community trying, with some real success, to get them to develop trusted computer systems.

POST OFFICE BOX 45, GLENWOOD, MD 21738
301-854-6889 WALKER @ BBN

All of that involves very high technology, advanced state of the art developments that are important for our national defense and for the protection of sensitive information in large computer centers and networks. But there is another side to computer security which is in a sense more mundane but just as important. Protection of information in a computer is a function of a number of prudent measures acting together, just as protecting the contents of one's home involves locking the doors and windows, putting on a night light, asking the neighbors to watch for strangers, etc. Many of these measures needed to protect information are rather basic common sense steps which, if carried out in reasonable combinations, will afford considerable protection. Unfortunately, many people, especially those in small business situations, do not have sufficient insight into the strengths and weaknesses of computer systems to understand what constitutes a reasonable set of such protective measures. And unlike their large business counterparts, they are unable to afford the estab- lishment of staffs specifically oriented to computer security or the hiring of outside experts to assist them in developing reasonable procedures.

The currently popular movie "War Games" should be required viewing for all who are concerned with protecting sensitive information on computers. Let me state emphatically that the national security related aspects of the movie are nothing more then very interesting fantasy, similar to that portrayed in dozens of similar movies and books in recent years. Military data communications systems are protected with the best communications security mechanisms and procedures available in the world, and computers are always used in advisory roles with humans making all the essential decisions regarding use of military force. However, this movie is much more then just another interesting tale of Armageddon because the measures that the young high school student takes to gain access to his school's computer, the phone number of the airline reser vations service and a bank's computer are all very real and easy to perform using small personal computers. The idea of programming a computer to run through all the phone numbers in a given phone exchange and note the ones that return a "data" tone is neither new nor in the slightest way sophisticated. Once one has a target phone number, the intuitive process for guessing the password of a potential user (assuming the system even bothers with passwords) is very well portrayed in the movie. It is these routine aspects of the movie that are what I recommend all users of computer systems concentrate on because it is these aspects that represent the potential threat they face.

Almost daily one reads in the trade press of yet another case of fraud being perpetrated involving a computer. But much of the so called "computer crime" does not involve sophisticated computer science techniques at all but just extensions of age old "sloppy bookkeeping" as updated to the computer age. The programmer who took the round off error in various accounting operations, consisting of no more then hundreds of a cent per operation, and added it to his account, would never be found in normal audits. The celebrated case in which a former employee retained his password and bluffed his way to the release of several million dollars, only to be foiled by foolish handling of the diamonds he bought with the money is yet another example. A recent edition of the Computerworld trade journal carried a story of a computer operator who embezzled over $84,000 from a state agency in Pennsylvania. She did this over a two year period by pocketing deposited funds from her cash register and misapplying someone else's deposit to cover the computer record. She would eventually get yet another deposit to cover the one she misapplied, and so on. When asked why it took two years to catch her, no one from the Department was available for comment.

These examples are far too prevalent. They are becoming routine as employees who are not very sophisticated are able to get away with "minor" crimes by hiding within the complexity of the computer systems they are using. The approach used in Pennsylvania would not have worked in the manual world of bookkeeping because the delay in posting deposits would have been more obvious. But it is virtually impossible even for a small business to successfully compete without using computers to handle basic transactions. Had the agency supervisors understood that such actions were possible (as they now do), they could have taken steps to detect such activity.

The small business person is very much like the supervisors in this case. They must rely on computers to compete in the marketplace but they are not aware of the vulnerabilities that accompany the use of automated data processing. They frequently must operate in a world of blind faith either assuming that computers "do not make mistakes" or so afraid of the complexity of the computer that they do not attempt to understand even routine protective measures that they should be using. Unfortunately, while large companies can afford insurance against such losses (indeed it is said in the diamond case that the victimized bank actually made money from the later sale of the recovered diamonds), most small businesses have neither such insurance or the resources to recover from what might otherwise be a minor case of embezzling. $84,000 stolen from a small business over two years might be enough to cause it to fail.

Chairman Luken, July 9, 1983

HR3075 will hopefully begin to alleviate this problem for small businesses by making available to anyone simple measures that can be taken to protect a company from potential abuse of its computer systems. I strongly recommend that you give favorable consideration to this bill. If you plan to have further hearings on this subject, I would be pleased to appear in person to express my opinion.

Sincerely,

Steph T. Walk

Stephen T. Walker

cc: Larry Sabbath
Staff Director
House Subcommittee on Anti-trust and Restraint
of Trade Activities Effecting Small Business

Appendix B.—The Bill H.R. 3075

I

98th CONGRESS
1st Session

H. R. 3075

[Report No. 98–423, Part I]

To amend the Small Business Act to establish a Small Business Computer Crime and Security Task Force, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

May 19, 1983

Mr. Wyden introduced the following bill; which was referred jointly to the Committees on Small Business and the Judiciary

October 20, 1983

Additional sponsors: Mr. Mitchell, Mr. McGrath, Mr. Corrada, Mr. Goodling, Mr. Gejdenson, Mr. Won Pat, Mr. Frenzel, Mr. LaFalce, Mr. Levin of Michigan, Mr. Conyers, Mr. Patterson, Mr. Ratchford, Mr. Ackerman, Mr. Tallon, Mr. McDade, Mr. Luken, Mr. Bilirakis, Mr. Williams of Ohio, Mr. Smith of New Jersey, Mr. Conte, Mr. Weber, Mr. Sisisky, and Mr. Broomfield.

October 20, 1983

Reported from the Committee on Small Business with an amendment and ordered to be printed

[For text of introduced bill, see copy of bill as introduced on May 19, 1983]

A BILL

To amend the Small Business Act to establish a Small Business Computer Crime and Security Task Force, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SHORT TITLE

SECTION 1. This Act may be cited as the "Small Business Computer Crime Prevention Act".

FINDINGS AND PURPOSES

SEC. 2. (a) The Congress hereby finds that—

(1) there is an increased dependency on, and proliferation of, information technology (including computers, data networks, and other communication devices) in the small business community;

(2) such technology has permitted and expanded criminal activity against small business concerns; and

(3) small business concerns are not always able to protect their information technology from the computer criminals.

(b) The purposes of this Act are—

(1) to improve the management by small business concerns of their information technology; and

(2) to encourage such business concerns to protect such technology from criminal activity.

COMPUTER CRIME AND SECURITY TASK FORCE

SEC. 3. Section 4(b) of the Small Business Act (15 U.S.C. 633(b)) is amended by adding at the end thereof the following new paragraph:

"(3)(A) The Administrator shall, not later than sixty days after the effective date of this paragraph, establish a task force to be known as the 'Small Business Computer Crime and Security Task Force'.

"(B) The Task Force shall consist of the following members:

"(i) an employee of the Small Business Administration, appointed by the Administrator;

"(ii) an employee of the Institute of Computer Sciences and Technology of the Department of Commerce, appointed by the Secretary of Commerce;

"(iii) an employee of the Department of Justice, appointed by the Attorney General;

"(iv) an employee of the Department of Defense, appointed by the Secretary of Defense;

"(v) one individual, appointed by the Administrator, who is representative of the interests of the providers of computer hardware to small business concerns;

"(vi) one individual, appointed by the Administrator, who is representative of the interests of the providers of computer software to small business concerns;

"(vii) one individual, appointed by the Administrator, who is representative of the interests of the providers of insurance to small business concerns;

"(viii) one individual, appointed by the Administrator, who is representative of the interests of the providers of computer security equipment and services to small business concerns;

"(ix) one individual, appointed by the Administrator, who is representative of the interests of associations of small business concerns, other than small business concerns engaging in any of the activities described in clauses (v) through (viii); and

"(x) such additional qualified individuals, appointed by the Administrator, as the Administrator determines to be appropriate.

"(C) It shall be the function of the Task Force—

"(i) to define the nature and scope of computer crimes committed against small business concerns;

"(ii) to ascertain the effectiveness of State legislation, and available security equipment, in preventing computer crimes against small business concerns;

"(iii) in cooperation with the National Bureau of Standards, to develop guidelines to assists small business concerns in evaluating the security of computer systems; and

"(iv) to make recommendations to the Administrator with respect to the appropriate activities of the resource center established under paragraph (4).

"(D) The Administrator shall designate one of the members of the Task Force as its chairperson. The Task Force shall meet not less than once during each six-month period following the effective date of this paragraph, at the call of its chairperson. A majority of the members of the Task Force shall constitute a quorum.

"(E) Each member of the Task Force shall serve without additional pay, allowances, or benefits by reason of such service. To the extent and in the amounts provided in advance in appropriations Acts, each such member shall be reimbursed for actual expenses, including travel expenses, determined by the Administrator to have been resaonably incurred in the course of performing the functions vested in the Task Force.

"(F) The Administrator shall provide the Task Force with such staff and office facilities as the Administrator, following consultation with the Task Force, considers necessary to permit the Task Force to carry out its functions under this paragraph.

"(G) The Task Force may secure directly from any Federal agency information necessary to enable the Task Force to carry out its functions under this paragraph. Upon request of the chairperson of the Task Force, the head of such agency shall furnish such information to the Task Force.

"(H) Not later than eighteen months after the effective date of this paragraph, the Task Force shall submit to the President, the Administrator, and the Congress a detailed *report setting forth the findings of the Task Force with respect to the matters described in subparagraph (C) and containing such recommendations as the Task Force determines to be appropriate.*

"(I) The Task Force shall terminate not later than thirty days after the submission of its report under subparagraph (H).

"(J) For purposes of this paragraph and paragraph (4)—

"(i) the term 'computer crime' means—

"(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; and

"(ii) the term 'Task Force' means the Small Business Computer Crime and Security Task Force established under subparagraph (A).".

COMPUTER CRIME AND SECURITY INFORMATION

SEC. 4. Section 4(b) of the Small Business Act (15 U.S.C. 633(b)), as amended in section 3 of this Act, is amended by adding at the end thereof the following new paragraph:

"(4)(A) The Administrator shall—

"(i) provide to small business concerns information regarding—

"(I) computer crimes committed against small business concerns; and

"(II) security for computers owned or utilized by small business concerns; and

"(ii) provide for periodic regional forums for small business concerns to improve the exchange of information regarding the matters described in clause (i).

"(B) Not later than sixty days after receipt of the report of the Task Force under paragraph (3)(H), the Administrator shall establish as part of the Small Business Administration a resource center that will carry out the functions of the Administrator under subparagraph (A)(i).".