S. HRG. 98-739

S. 1920, SMALL BUSINESS COMPUTER CRIME PREVENTION ACT

HEARING

BEFORE THE

COMMITTEE ON SMALL BUSINESS
UNITED STATES SENATE

NINETY-EIGHTH CONGRESS

SECOND SESSION

ON

MALL BUSINESS COMPUTER CRIME PREVENTION ACT

MARCH 7, 1984

inted for the use of the Committee on Small Business

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON : 1984

33-723 O

CONTENTS

HEARING DATE

S. 1920, SMALL BUSINESS COMPUTER CRIME PREVENTION ACT

WEDNESDAY, MARCH 7, 1984

U.S. SENATE,
SMALL BUSINESS COMMITTEE,
Washington, D.C.

The committee met, pursuant to notice, at 10 a.m., in room SR 428A, Hon. Paul E. Tsongas (acting chairman of the committee) presiding.

Present: Senator Tsongas.

Staff present: Michael W. Morris, counsel; Alan L. Chvotkin, minority chief counsel; and Dorothy C. Olson, hearing clerk.

STATEMENT OF HON. PAUL E. TSONGAS, A U.S. SENATOR FROM THE STATE OF MASSACHUSETTS, AND ACTING CHAIRMAN, SENATE SMALL BUSINESS COMMITTEE

Senator TSONGAS. Since it is 10 o'clock, we should begin.

Let me begin by thanking Senator Weicker, who is chairman of the committee, for his willingness to allow this schedule to be expedited and allow us to hold the hearings on the bill. I appreciate his willingness to let me chair. If I thought the Democrats would take over and I would do this more regularly, I would stay here. [Laughter.]

We welcome you to the hearing and the issue of computer crime and its prevention as it affects the small business community.

The Congressmen are on their way, and they will be our lead witnesses today. They have recognized the mounting threat of computer crime and have introduced and successfully passed legislation in the House to deal with this problem. Senators Nunn and Boschwitz have joined me in the counterpart bill which we are going to consider here today.

I don't think anybody in the room needs to be told about the problems of computer crime. The question is what we do with it, and in that respect, and to expedite the proceedings, I would ask that my statement appear in the record as if read. I would also ask that a statement by Senator Nunn be included at this point in the record.

[The prepared statements of Senators Tsongas and Nunn follow:]

United States Senate
COMMITTEE ON SMALL BUSINESS
WASHINGTON, D.C. 20510

SENATOR PAUL E. TSONGAS

OPENING STATEMENT FOR HEARINGS ON S. 1920 -- THE SMALL BUSINESS COMPUTER CRIME PREVENTION ACT

MARCH 7, 1984

Good morning. Welcome to this hearing, which is devoted to issues related to computer crime and its prevention, as it affects the small business community.

I would like to start by acknowledging the leadership of Congressmen Ron Wyden and Vin Weber, who are invited to be our lead witnesses today. They have recognized the mounting threat of computer crime, and introduced and successfully passed legislation in the House to deal with this problem.

Senators Nunn, Boschwitz, and myself have recently introduced parallel legislation (S. 1920) in the Senate, in response to widespread concern about the potential impacts of growing computer crime on the most vulnerable, but highest productivity sector, small business.

Today, the Senate Small Business Committee seeks to continue the effort of educating Congress with regard to the existence, nature, and scope of the computer crime problem, which may further jeopardize the survival of small businesses in an inflationary economy. I hope that the Senate will be as responsive as the House was to the needs of the small business community, in moving this legislation speedily out of Committee and onto the floor.

THE PROBLEM:

Computer crime has been on the rise in recent years, and this problem has gained substantial media attention.

Although this new class of white collar crime impacts on the private and public sectors alike, its potential damage to the small business sector is greater, for the following reasons:

- Small businesses are increasing their use of computers, in order to improve productivity and cut costs;

- Small businesses typically have fewer available resources and dedicated trained personnel to prevent, detect and combat computer crime, than either large corporations or the federal government;

- Small businesses appear to opt for greater accessibility and ease of use of features in acquiring computer systems, with obvious security trade-offs;

- There is relatively little awareness in the small business community of the risks involved in adopting new management and accounting technology, and a prevailing lack of information as to the availability and cost-effectiveness of computer security methods available to prevent and control computer crime.

The small business sector is vital to our economy, accounting for more than a third of our GNP, for virtually all of the private sector employment growth, and for at least half of all innovations. Yet, it is more vulnerable to the effects of computer crime and abuse, especially during critical periods of business growth and acute competition, when it is most attractive as a target for computer crime.

THE SOLUTION:

This bill, S. 1920, the Small Business Computer Crime Prevention Act, offers a promising and cost-effective solution to the problems to be addressed in today's testimony.

The bill requires the SBA to define and assess the nature, extent, and impacts of computer crimes committed against small businesses. The SBA is

expected to take advantage of the expertise developed in both federal and the private corporate sector for protection and control of computer crime, and screen for dissemination via the resource center mandated by the Bill, those methods suited to the needs and means of small businesses.

I believe that the SBA has an excellent network already in place, for outreach and education of its constituency. The SBA can play a key role in strengthening computer security, while fostering wider introduction and growth of high technology office automation. Also, the preventive and educational thrust of this bill, insures both lower cost and greater effectiveness in alleviating the computer crime problem, than the punitive approach in existing and proposed legislation.

In conclusion, while it is becoming widely recognized that computer crime is a growing problem, this awareness has come largely through media coverage. Press accounts of 'hackers', who gained unauthorized access to both federal and private sector computers and data banks; and of white collar criminals, who removed private funds or products via computers for profit, have made us all aware that the computer crime threat is real and growing: Numerous TV shows and serials (like The Whiz Kids, The Facts of Life, and Knight Rider) and movies (like War Games, and Tron) have dramatized the variety of computer crimes and their potentially grave outcomes. In fact, the media may have recently lavished more attention on the problem, than Congress has devoted in considering appropriate legislation to alleviate it.

As several witnesses will point out later today, we need a greater awareness of the computer related risks and crime prevention strategies among small businesses, in order to encourage them to introduce computers into the office and help them wisely use their scant resources.

OPENING STATEMENT BY
SENATOR NUNN
March 7, 1984
on S. 1920

Today, the Senate Small Business Committee begins hearings on S. 1920, the legislation Senator Tsongas, Senator Boschwitz and I have introduced to address the critical issue of computer security and its impact on small business. This bill, a number of other legislative proposals on computer crime, and the number of hearings in both the House and Senate are indicative of the impact which computers have on our society, and the potential damage their misuse could have on the total business community in particular and on the economy generally. It has already been estimated that the private sector loses at least $1 billion annually through direct computer crime only.

While there has been valuable and significant attention which the Congress has given to computer-related users, our Committee's hearings are unique among the reviews made. First, our focus in this legislation and in the hearings is on the special problems of computer security which confronts small business. Foremost among these concerns, in my view, is a lack of awareness by the small business community that computer security is an issue in which they have a vested interest. The smaller personal computers, utilized extensively by most small businesses, present such security problems as a lack of access control programs, and the physicial accessibility and mobility of the diskettes

At our hearing on the House side in July, we heard from Donn Parker, one of the truly renowned experts on computer crime, and he said then that he felt this problem as it affected small businesses was going to get worse and worse.

He said, and I quote:

> 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 some computers in some way.

Mr. Parker also made the significant point that, right now, there is no appropriate mechanism to get computer security information to small businesses. He said, and again I quote:

> 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 certainly are not going to inform their customers of all the terrible things that could happen to them in the purchase of their products.

Mr. Chairman, we have also heard from a variety of representatives from the small business community. One witness on the House side was particularly helpful to us at our hearing last July. He had been victimized, and in his words—again I quote:

> 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.

I would just like to make a couple of other points very briefly, Mr. Chairman.

Unfortunately, thousands of small business people are choosing to use computers today—and they have told us this themselves—without adequate knowledge of their vulnerabilities and what steps they can take to protect the integrity of the system.

I would just say that I think that our legislation is a cost-effective way to get this kind of practical information across to the small business community.

The heart of this bill, of course, is the resource center which would be established as soon as possible after the legislation is signed into law by the President. It strikes me that there are a lot of things we can do for very little money to assist small business.

For example, SBA is now running a national toll-free line for small business, and I would like to see us use that national toll-free line as a way to help small businesses get information about computer security, and I would think for very little money, through the resource center, we could do that.

The last point that I would make, Mr. Chairman—and then I want to yield to my colleague who has been so helpful in getting this bill passed on the House side—is that we know we cannot pass a law that says there shall never be another computer crime in this country. We know that cannot be done.

What we can do is reduce the risk, and we can reduce the risk for a segment of society, the small business community, that is particularly vulnerable. That is the kind of approach we have pursued and pursued successfully on the House side.

I want to thank you again for the chance to come here and discuss this with your committee today.

I also want to thank my colleague, Mr. Weber, for coming as well. He has been tremendously helpful. In essence, the three of us have worked together in trying to get the legislation across, and I am grateful to you both.

[The prepared statement of Representative Wyden follows:]

Statement of Hon. Ron Wyden, a Member of Congress from the State of Oregon

Mr. Chairman, I want to thank you for the kind invitation to appear before your committee today. It is a pleasure and an honor to be here.

I also want to commend Senators Tsongas and Nunn for the active leadership they have shown in addressing the critical problem of computer security and its importance to the small business community. As you may know, I share that concern.

I also would like to thank my colleague, Vin Weber, who has been a tremendous booster of this legislation, and who has been just super in helping to forge the bipartisan coalition that helped move this legislation through the House without opposition.

Last year, before "War Games" and before "hacker" became a household word, I began to take a close look at the growing use of computers in this country, and, along with that, their vulnerabilities. I read the stories of the multimillion dollar frauds and the youngsters who took joy rides on their school computer, ordering cases of Pepsi to their doorstep.

But I also began talking to small business people throughout my district and observing their operations, and I began to detect a disturbing trend. The trend was that, in general, the small business community knows very little about computers and even less about their vulnerabilities.

Moreover, it became clear that in addition to this general lack of knowledge, small businesses are particularly vulnerable, yet in general have fewer resources to deal with these problems.

As a result, I introduced HR 3075, the Small Business Computer Crime Act. My legislation is identical to the measure this committee is considering today. HR 3075 unanimously passed out of the Antitrust Subcommittee and the full House Small Business Committee and passed the House by a unanimous voice vote on October 24, 1983. It is the first piece of legislation specifically addressing computer security to pass either body.

Considering the problem of computer security and computer crime reminds me of a certain long distance telephone advertisement that makes the claim "Anywhere, anytime..." Computer fraud and abuse is a pervasive problem that can happen almost anywhere and anytime. And according to testimony we heard on my legislation in the House, is going to get worse before it gets better.

At the hearing we held last July, we heard from Donn B. Parker, a world-renowned computer crime authority, who empahsized this point. He said: "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 some computers in some way."

Mr. Parker also made the significant point that, right now, there is no appropriate mechanism to get computer security information to small businesses. He said, and I quote, "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 they need the security. The salesmen of these companies certainly are not going to inform their customers of all the terrible things that could happen to them in the purchase of their products."

At that hearing, we also heard from a small businessman who was the victim of a computer crime. He emphasized the point that most small business people just don't think investing in computer security equipment is worth it.

This businessman also emphasized one of the keys to prevention. In his words:

> "The principles, the owner or someone who is the managment 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."

Unfortunately, thousands of small business people are choosing to use computers without adequate knowledge of their vulnerabilities and what steps they can take to protect the integrity. They won't protect their computers for the same reason they won't fasten their seatbelts -- they don't believe it can happen to them.

I am hesitant to use figures in discussing the problem of computer crime. As many here know, we have few hard statistics about the number of computer crimes, mainly because businesses that are victims often do not report these trespasses because they fear it could cause a lack of public trust.

But some figures do exist that give us an idea of the increasing scope of our vulnerabilities. For example, Dun and Bradstreet recently reported that nearly 15 percent of firms with fewer than 20 employees use microcomputers, with many companies reporting they had acquired their micro only within a few months of the survey, which was conducted last summer.

In addition, John Borden, senior analyst with the Yankee Group, a Boston-based market research company, says that the potential for security breaches is increasing with the number of people who have technical abilities. The Group estimates that by 1986, the nation's data networks will be able to be accessed by almost 9 million desk-top computers.

Now that more computer systems are being hooked up to dial-up data networks, a whole new range of vulnerability has been added to systems where we were already, in many cases, unable to prove or maintain integrity.

The growth of these data networks has been a boon to productivity in this country. They have, however, made transcontinental trespassing that can happen in the blink of an eye a common occurrence.

One of the reasons is that these data networks make using a computer relatively cheap. For instance, sending computer data for an hour over a regular Bell System telephone line costs about $32, but the same serive through a data network can cost the user as little as $8.

Another computer security expert, Stanley Halper, who is the National Director of Computer Audit Assistance Group at Coopers and Lybrand, says that computer security has become one of the most serious problems facing business today. He maintains that the sophistication of computer theivery has grown as rapidly as the sophistication of the machines themselves, and says that the smaller the firm, the more difficult it is to safeguard the system.

This is true because the limited resources of a small business usually mean fewer and less specialized employees. That handicap reduces the division of duties among departments and employees -- one of the main defenses against losses through crime or mistake.

Another reason is that smaller businesses tend to use smaller computer systems, which, by and large, have fewer or more limited security features designed into the system.

Third, small businesses often have little control over the bulk of the "information system" they are using. They usually lease their phones and communication lines; often they lease or use time-shared computers owned by others and many use packaged software purchased off the shelf. This dependence puts comprehensive knowledge of computer security out of the reach of many small businesses.

Unfortunately, it has become difficult for managers to comprehend all the precautions necessary to protect businesses from fraud and abuse. Yet these precautions have never been more important. As Arthur Gillis, President of Computer Based Solutions, Inc. of Atlanta recently said, "The rip-offs are likely to be more frequent and larger."

Mr. Halper also has made the statement that management needs more education in computer safeguards. That is exactly what this legislation intends to do.

In introducing my bill, I in no way intended for us to re-invent the wheel. I am well aware that there is a wealth of information on the problem of computer crime.

My objective was to take a specific, focused look at the implications for the small business community, which, to the best of my knowledge has never been done, and then find a cost-effective way to get this practical information to the small business community.

I think the SBA resource center provided for in the legislation can achieve that latter goal, and it is my objective that the resource center be put in place just as soon as possible after this bill is signed by the President.

To sum up, I view the legislation I introduced and that Senator Tsongas introduced in the Senate as a practical attempt to fill a very obvious void.

We are living in an automated society, and that is nothing to be afraid of. We must, however, be aware of the inherent vulnerabilities that come with the date chip age.

Computer Crime is preventable. I support tougher, specific laws that will punish those who abuse computers. In fact I recently introduced a bill that makes it a crime to tamper with medical records that are on computers.

I continue to believe, however, that these new laws must go hand in hand with an increased effort to educate those who face these vulnerabilities. Tougher laws alone will not do it.

I believe the Small Business Computer Crime Act is one practical vehicle where the vast resources of the public and private sectors can be combined to attack this problem. I view this approach as being far preferable to one in which we react in a crisis atmosphere and spend our time playing catch-up ball in the crucial game of computer security education.

33-723 O - 84 - 2

STATEMENT OF HON. VIN WEBER, A MEMBER OF CONGRESS FROM THE STATE OF MINNESOTA

Representative WEBER. Good morning, Mr. Chairman.

I want to begin by saying I am here to support my colleague from Oregon, who has really brought this issue to the attention of the House of Representatives and who has developed the approach for dealing with it, and he is the expert on it. Also, I want to explain a little bit of the background of the bill in terms of what action was taken by our committee.

My testimony reflects more the experience that I have had in the committee rather than the substance of the bill on which Congressman Wyden really is the expert in the House of Representatives.

As ranking minority member of the Subcommittee on Antitrust and Restraint of Trade, I want again to present the background of this bill, H.R. 3075, which was introduced by Congressman Wyden and has now become known as the Computer Crime Bill.

I want to explain, from a Republican standpoint, why I believe the Federal Government should play a role in assisting small business in understanding and effectively dealing with computer crime.

Our subcommittee heard testimony on this bill which focused on crimes committed against small businessmen who use computers in their everyday business. It appeared that small businessmen either did not have access to information to help them prevent computer crime or, more importantly in my judgment, the financial resources to invest in protecting themselves from crime.

By unanimous vote, the subcommittee modified the original bill and reported it to the full committee on September 25. The full committee, again by a unanimous vote, sent the bill to the floor. It was placed on the suspension calendar and was passed on October 24 of last year.

The members of the Small Business Committee looked favorably on the bill because it addressed the concerns heard in the hearing—as expressed by experts in the field—while doing the job economically. I think that is something which we have been very sensitive to in the Small Business Committee.

The subcommittee made every effort to keep the costs to a minimum by preventing the establishment of a new bureaucracy within the SBA. This, in my opinion, helped create the solid bipartisan support for the Wyden bill.

That provides you, Mr. Chairman, with a short history of what has happened in the House to date. Now I would like to focus a little bit on why I think the bill should become law.

I think the bill is consistent with the thinking of small businessmen in this country. As a former small businessman and representing a district in southwestern Minnesota which contains a great many small businessmen I think most small businesses want to be relatively free from Government control and regulation. They want a minimum amount of Government intervention necessary to protect the Nation and to promote its general welfare. They are not asking for, nor do they need, large Federal spending programs to protect them from competition. They don't request bail-outs for bad ventures, nor are they particularly enthused with industrial policies calling on the Federal Government to pick the winners and losers.

Small businesses believe that creativity and innovation are the watch words for the marketplace. They understand that, given time, private sector initiatives will fill the gaps in services resulting from technological advances.

These bills, S. 1920 or H.R. 3075, are examples, in my judgment, of the proper functions the Federal Government can provide to small business in this area. The legislation will fill the gap between the present and the future. It will give small businesses a place to turn to answer questions about protecting themselves from computer crime, and it will help shape a potential market for entrepreneurial companies to develop. Economies of scale will allow every small business in America the opportunity to deal with this problem.

The SBA seems to be the logical organization to provide this interim program. It already has the structure for regional conferences and advocacy. It has the personnel to coodinate and continually update the information center. With instruction from Congress, I know SBA can do the job.

In conclusion, let me just say, Mr. Chairman, that I am not particularly wedded to the exact wording of this legislation. I think the concept is very important. But I do think that our colleague from Oregon has done a thorough job in putting the bill together in the House, and I would urge favorable action by this committee and the Senate as soon as possible.

Thank you, Mr. Chairman.

[The prepared statement of Representative Weber follows:]

VIN WEBER
2D DISTRICT, MINNESOTA
318 CANNON BUILDING
WASHINGTON, D.C. 20515
(202) 225-2331
LEONARD SWINEHART
ADMINISTRATIVE ASSISTANT
P.O. BOX 279
NEW ULM, MINNESOTA 56073
(507) 354-8400
919 SOUTH 1ST STREET
WILLMAR, MINNESOTA 56201
P.O. BOX 1214
MARSHALL, MINNESOTA 56258
(507) 532-9811
JACK MEEKS
DISTRICT DIRECTOR

Congress of the United States
House of Representatives
Washington, D.C. 20515

COMMITTEE ON PUBLIC WORKS AND TRANSPORTATION
SUBCOMMITTEES:
WATER RESOURCES
AVIATION
COMMITTEE ON SMALL BUSINESS
SUBCOMMITTEE:
ANTITRUST AND RESTRAINT OF TRADE
ASSISTANT REGIONAL WHIP
REPUBLICAN POLICY COMMITTEE

REP. VIN WEBER
STATEMENT BEFORE THE SENATE SMALL
BUSINESS COMMITTEE
MARCH 7, 1984

I WOULD LIKE TO THANK THE SENATE SMALL BUSINESS COMMITTEE FOR ALLOWING ME TO SPEAK THIS MORNING ON SENATE BILL S.1920, AND MORE GENERALLY ON THE ISSUE OF COMPUTER CRIME AND SMALL BUSINESS.

MY TESTIMONY THIS MORNING WILL REFLECT MY EXPERIENCE AS A MEMBER OF CONGRESS. I UNDERSTAND THAT MANY EXPERTS IN THIS FIELD ARE SCHEDULED TO TESTIFY LATER TODAY. I WOULD LIKE TO LET THEM TALK ABOUT THE SCOPE AND SIGNIFICANCE OF THE PROBLEM OF COMPUTER CRIMES COMMITTED AGAINST SMALL BUSINESS ALL ACROSS THE COUNTRY.

AS RANKING MINORITY MEMBER OF THE SUBCOMMITTEE ON ANTI-TRUST AND RESTRAINT OF TRADE, HOUSE SMALL BUSINESS COMMITTEE, I WANT TO PRESENT THE BACKGROUD OF THE HOUSE BILL INTRODUCED BY MY COLLEAGUE REP. RON WYDEN, H.R. 3075. THIS BILL HAS BECOME KNOWN AS THE COMPUTER CRIME BILL. I WOULD ALSO LIKE TO TELL YOU WHY I BELIEVE THE FEDERAL GOVERNMENT SHOULD PLAY A ROLE IN ASSISTING SMALL BUSINESS IN UNDERSTANDING AND EFFECTIVELY DEALING WITH COMPUTER CRIME.

MY SUBCOMMITTEE HEARD TESTIMONY ON THIS BILL WHICH FOCUSED ON CRIMES COMMITTED AGAINST SMALL BUSINESSMEN WHO USE COMPUTERS IN THEIR EVERYDAY BUSINESS. IT APPREARED THAT SMALL BUSINESSMEN

EITHER DID NOT HAVE ACCESS TO INFORMATION TO HELP THEM PREVENT COMPUTER CRIME OR THE FINANCIAL RESOURCES TO INVEST IN PROTECTING THEMSELVES FROM CRIME.

IN A UNANIMOUS VOTE, THE SUBCOMMITTEE MODIFIED THE ORIGINAL BILL AND REPORTED IT TO THE FULL COMMITTEE ON SEPTEMBER 25TH. THE FULL COMMITTEE, AGAIN BY UNANIMOUS VOTE, SENT THE BILL TO THE FLOOR. IT WAS PLACED ON THE UNANIMOUS CONSENT CALENDAR AND WAS PASSED OCTOBER 24 OF LAST YEAR.

THE MEMBERS OF THE HOUSE SMALL BUSINESS COMMITTEE LOOKED FAVORABLY ON THIS BILL BECAUSE IT ADDRESSED THE CONCERNS HEARD AT THE HEARING--AND EXPRESSED BY EXPERTS IN THE FIELD--WHILE DOING THE JOB ECONOMICALLY. THE SUBCOMMITTEE MADE EVERY EFFORT TO KEEP COSTS TO A MINIMUM BY PREVENTING THE ESTABLISHMENT OF A NEW BUREAUCRACY WITHIN THE SMALL BUSINESS ADMINISTRATION (SBA). THIS, IN MY OPINION, HELPED CREATE THE OVERWHELMING AMOUNT OF SUPPORT ON BOTH SIDES OF THE AISLE.

THAT PROVIDES YOU WITH A SHORT HISTORY OF WHAT HAS HAPPENED IN THE HOUSE TO DATE. NOW, I WOULD LIKE TO FOCUS ON WHY THIS BILL SHOULD BECOME LAW.

I BELIEVE THIS BILL IS CONSISTENT WITH THE THINKING OF SMALL BUSINESSMEN IN THIS COUNTRY. AS A FORMER SMALL BUSINESSMAN, AND REPRESENTING A GREAT DEAL OF SMALL BUSINESSES IN MINNESOTA'S SECOND CONGRESSIONAL DISTRICT, I THINK MOST SMALL BUSINESSES WANT TO BE FREE FROM GOVERNMENT CONTROL AND REGULATION. THEY WANT THE MINIMUM AMOUNT OF GOVERNMENT INTERVENTION NECESSARY TO PROTECT THE NATION AND PROMOTE ITS GENERAL WELFARE. THEY ARE NOT ASKING FOR, NOR NEED, LARGE FEDERAL SPENDING PROGRAMS TO PROTECT THEM FROM COMPETITION. THEY DON'T REQUEST "BAIL-OUTS" FOR BAD VENTURES, OR ARE PARTICULARLY ENTHUSED WITH INDUSTRIAL POLICIES CALLING ON

THE FEDERAL GOVERNMENT TO PICK SO-CALLED "WINNERS AND LOSERS" IN THE MARKETPLACE. SMALL BUSINESSES BELIEVE THAT CREATIVITY AND INNOVATION ARE THE WATCH WORDS FOR THE MARKET. THEY UNDERSTAND, THAT GIVEN TIME, PRIVATE SECTOR INITIATIVES WILL FILL THE GAPS IN SERVICES RESULTING FROM TECHNOLOGICAL ADVANCES.

THESE BILLS, S. 1920 OR H. 3075, ARE EXAMPLES OF THE PROPER FUNCTIONS THE FEDERAL GOVERNMENT CAN PROVIDE TO SMALL BUSINESS. THE LEGISLATION WILL "FILL THE GAP" BETWEEN THE PRESENT AND THE FUTURE. IT WILL GIVE SMALL BUSINESSES A PLACE TO TURN TO ANSWER QUESTIONS ABOUT PROTECTING THEMSELVES FROM COMPUTER CRIME, AND IT WILL HELP SHAPE A POTENTIAL MARKET FOR ENTREPRENEURIAL COMPANIES TO DEVELOP. ECONOMIES OF SCALE WILL ALLOW EVERY SMALL BUSINESS IN AMERICA AN OPPPORTUNITY TO DEAL WITH THIS PROBLEM.

THE SBA SEEMS TO BE THE IDEAL ORGANIZATION TO PROVIDE THIS INTERIM PROGRAM. IT ALREADY HAS THE STRUCTURE FOR REGIONAL CONFERENCES AND ADVOCACY. IT HAS THE PERSONNEL TO COORDINATE AND CONTINUALLY UPDATE THE INFORMATION CENTER. WITH THE INSTRUCTION FROM CONGRESS, I KNOW SBA CAN DO THE JOB.

IN CONCLUSION LET ME SAY THAT I AM NOT WEDDED TO THE PARTICULAR LANGUAGE IN THE HOUSE BILL, THOUGH I THINK REPRESENTATIVE WYDEN HAS DONE A THOROUGH JOB IN PUTTING IT ALL TOGETHER. I STRONGLY SUPPORT THE CONCEPT OF HAVING THE FEDERAL GOVERNMENT PROVIDE SMALL BUSINESS WITH A WAREHOUSE OF INFORMATION SO OUR NATION'S COMMERCE CAN BE EVEN MORE PRODUCTIVE AND EFFICIENT. AND, MOST IMPORTANTLY, THIS WILL WILL HELP PREVENT THEFT AND OTHER TYPES OF COMPUTER CRIME.

THANK YOU VERY MUCH.

Senator TSONGAS. Let me ask you: as I understand it, the original bill had a 3-year provision for the task force, at which time they were to submit their recommendations to the President, SBA, and Congress. Can you explain why that time has been reduced to 18 months?

Representative WYDEN. Mr. Chairman, in consultation with leaders in the small business community and experts in the computer security field, we felt that was warranted. This is an area of such growing concern—virtually every time you open a newspaper, you hear about additional dimensions to the problem—that we thought we really ought to focus for a shorter period of time, quickly establishing the Resource Center to start assisting small business.

So we found that there was a general consensus among small business groups, small business leaders themselves, people in the computer security community that we ought to go ahead with that kind of approach.

Mr. Chairman, I want to make one other point. I just summarized my remarks, and with the consent of the Chair, I would very much like to have my full prepared statement be made a part of the record.

Senator TSONGAS. I see where you took the bill through on unanimous consent rather than suspension. Is that right?

Representative WEBER. No, it was under suspension.

Representative WYDEN. It was on suspension——

Representative WEBER. On the suspension calendar. That may be an error in my statement.

Senator TSONGAS. So it was under suspension?

Representative WYDEN. Yes, it was on suspension of the rules.

Representative WEBER. It was on the suspension calendar.

Senator TSONGAS. Did you have a rollcall vote?

Representative WYDEN. We did not.

Representative WEBER. No.

Senator TSONGAS. I didn't realize the House had become so efficient in my absence. [Laughter.]

We hope that we can do as well.

There is some hesitation about whether you need a task force at all, whether the issue is well enough defined that we can just go on to the second phase of providing services. How would you both address that concern?

Representative WEBER. I will again defer to the expert, but my feeling—I think Ron touched on it—is that the central reality of this problem is that it is a problem for which we really do not have the answer because it is tied up in the rapid evolution of technology.

In answer to the earlier question you asked, a genuinely long-term approach in this case is specifically not called for because we don't have the long-term answer to it.

I think the steps that we have taken are more appropriate toward getting a handle on a problem that really is growing daily than to go, as you put it, to the next step.

Representative WYDEN. I concur, Mr. Chairman.

There are a lot of different ways to do this. We have talked about a task force. We have talked about an ongoing advisory group. I think, as Vin has said and said very well, we don't know a lot

about the problem. I think we need to figure out how to really take two steps. One is to have the Resource Center, to start assisting small business in a low-budget kind of way, using primarily existing kinds of resources like that tollfree line; then we need a mechanism so that, on an ongoing basis, we can really understand what the state of the art is.

I like very much the idea that has been discussed over here on the Senate side of an ongoing body. I think that makes sense as well. We are not wedded to one specific kind of approach or another, but we think we are going to have to do some work really discussing what the dimensions of the problem are.

Senator TSONGAS. Just for the record, why don't you just give us one minute on how you got into this issue? I can understand someone from the Silicon Valley or Minnesota or Massachusetts getting involved with this, but you are from Oregon.

Representative WYDEN. My district center is very much like Vin's: it is just chock full of small businesses, and like all Members we make tours, we make plant visits and the like.

I would go through front offices and I would see all these computer systems essentially unattended, and I would say to people, I would say, "it really looks like it would be fairly easy for somebody who was unhappy about something or for a disgruntled employee to get into one of these things and virtually wipe you out."

People would kind of look at me kind of sheepishly, and they would say, "You know, Ron, that's really right. We don't know much about it."

As I made plant visits and I saw all these small businesses with small systems that were unsecured and I asked them what they were doing to secure their systems, they would say, "We really don't know much about it. We probably are fairly vulnerable. What do you suggest?" And I didn't have all that many good answers for them. That is what got me interested in this initially.

Representative WEBER. I would like to respond, also. I think that although it is no doubt a problem for Silicon Valley firms or for Control Data and Honeywell in Minnesota, the point I would make is that those firms are specifically better able to deal with the problems than the businesses in Ron's district and my district and those in the State of Massachusetts, which are now utilizing technology developed by the Control Data's, IBM's, and Honeywell's of the world but really don't know how to deal with any of the problems.

Since virtually every businessman today is moving into the computer age at a speed that he never probably anticipated he would, I really think that it is more important for people who represent districts like mine that don't have these high-powered high technology firms to be concerned about it.

Senator TSONGAS. As a Republican, have you had a chance to speak to the administration about their hesitance about all this?

Representative WEBER. We have had some conversations with them in the course of the small business meetings, but we really haven't pushed them, no. We do have the support, of course, of all the Republicans on the Small Business Committee including Joe McDade, the ranking member.

I think we have dealt with the problems in terms of the economies of the bill and in terms of establishing new bureaucracies within the SBA so that I feel relatively comfortable about going to the administration at the appropriate time and pushing them for support. But no, we have not specifically done that.

Senator TSONGAS. Well, we will assign that task to you when the time comes.

Thank you very much.

Representative WEBER. Thank you.

Representative WYDEN. Thank you very much, Mr. Chairman.

Senator TSONGAS. Professor Ball.

STATEMENT OF DR. LESLIE D. BALL, PROFESSOR OF INFORMATION SYSTEMS, BABSON COLLEGE

Dr. BALL. Good morning.

My name is Leslie D. Ball. I am professor of information systems at Babson College, where I am responsible for teaching and developing computer graduate and undergraduate courses for students who are primarily business majors.

In addition, I have done extensive research in the area of computer crime and security and am active in several professional organizations.

For the past 20 years I have worked in the computer industry, and during the last 10 years I have authored several articles and books about computer crime and its prevention. One book, Information Systems Audit Review Manual, is used as a study guide by persons who take the Certified Information Systems Auditor exam. It is this certified group of individuals who are primarily responsible for ensuring that our Nation's largest corporations have adequate security protection.

In 1980, I became the founding chairperson of the Association of Computing Machinery's Special Interest Group on Security, Auditing, and Control, which is commonly referred to as SIGSAC. ACM is the world's oldest organization of computer professionals, and SIGSAC is one of the 36 special interest groups that ACM members can belong to.

SIGSAC publishes a quarterly newsletter, sponsors presentations at national meetings, and conducts conferences and workshops all addressing computer crime and computer crime prevention issues. The organization currently has nearly 1,100 members.

Let me start by saying that computer crime is growing as computers are becoming more commonplace. Prior to 1950, banks were not very concerned about check forgery because personal checks were not very popular. Yet today 40 billion checks are processed in the American banking system each year.

I use this example to demonstrate that something such as checks, which was once so rare, is now commonplace only 35 years later, and we will find very quickly that computers are as commonplace as checks.

Very soon every office worker, whether they are a clerk or an executive or whether they work in a large or a small organization, will have a computer terminal on his desk. That is when computer

crime will be the major problem for American businesses, and it will take forms that we cannot anticipate at this time.

Computer crime can be thought of as theft, destruction, or disclosure of data, programs, or equipment. For example, someone might destroy a company's accounts receivables records, which would make it difficult or impossible to determine who owes the company funds. But damage could also occur to a person as a result of a computer crime. For example, someone might alter computerized voter registration lists in a county to disenfranchise a minority group—this event, by the way, has already occurred— and someone else could alter an individual's credit record at a small credit agency to make it impossible for them to buy goods on credit or to secure a loan.

Victims, too, come in all sizes and shapes. They are small companies and large companies. They are nonprofit organizations and highly profitable, well managed companies. They are poorly managed companies and some that we think as of being the best managed. Some are even computer companies.

About the only characteristic that they have in common is that they have some system within their organization which has a missing control that the penetrator has found.

I would like to say that computer crime is declining, but I cannot. We are now in an era in which computers are being used in ways never thought possible. Computers are used by individual executives to develop financial models so that they can ask what if questions. The results of these models will enable them to make decisions about managing their departments or companies.

We now move billions of dollars daily between banks and businesses. We can now create electronic offices that allow us to send electronic mail messages from individual to individual.

Because of advances in telecommunications, we can now have one company's computer access another's to order goods and services. Data within most companies' computers can now be made available to everybody in the company as they move to an access free world.

Finally, the fastest growing segment of our working population is something known as the knowledge worker who must have access to computer resident information to complete his assigned tasks.

I relate all of these changes to you because, although they alter the way in which businesses are run in a positive way, they create more opportunities for the computer criminal.

When new technology is introduced, it is always marketed with its advantages somewhat overstated and its disadvantages rarely mentioned. To the vendors' defense, the disadvantages are seldom totally known.

For example, I do not believe that anybody can predict how the growth in electronic mail will create new computer crime. But I do believe that crimes that we have never seen before will begin to be committed as electronic mail increases in popularity.

I do not mean to suggest that all new technologies be held from the marketplace until their crime potential be analyzed, but only that new technologies are watched carefully because they represent an entirely new ballgame for computer thefts.

How does all of this relate to the small businesses? Well, first, the problems are complex even for large businesses, and they are becoming even more complex. Large businesses are committing more of management's time to the problem and are hiring specialists to solve the problems.

Small businesses are really no less complex than large businesses. A computer can solve their problems just as it can for a large business. The costs of computer hardware and software have declined so rapidly that nearly all businesses can afford computers.

The problem that a small business has is the lack of management time and expertise. Virtually ever small businessman has more tasks than he can complete in most business days.

For example, if he has the following options—one, spend 20 hours of work on developing security controls and you may save $20,000 someday; or, two, spend 20 hours in the development of new production procedures and you will save $40,000 in production costs over the next year—it is clear which option he would choose to take.

Computer crime, therefore, is a low priority item for the small businessperson, and they do not have the expertise in-house to deal with the problem.

Another issue is cost. To develop fairly secure systems requires a lot of money be spent. Excess cash for this type of investment is often not available to small businesses. For small businesses, every spare dollar must be invested to yield a positive return.

Finally, there are no information resources that are readily available to small businesses. For example, our organization, SIGSAC, has members coming from primarily academic and large businesses. All of the trade journal articles about computer crime prevention assume that the audience is a large organization. Software and hardware prevention products are also primarily aimed at this audience.

I am in support of the task force proposed by the bill. In spite of the fact that the small businessperson might not realize that computer crime is a problem for him, it is. This task force should develop vehicles to combat that crime.

My main concern is that the task force recommend adequate information resource centers and educational programs for the small business. Both of these could be conducted through SBI's at universities where academics, in conjunction with information systems and computer science professionals, could work with the SBI and its clients.

These resources should enable the small businessperson to learn about the problem and to become properly educated about how to protect himself against what is in reality a very severe problem.

I would urge your support of the bill.

Thank you.

[The prepared statement of Dr. Ball follows:]

Statement by:

Leslie D. Ball, Ph.D.
Babson College
Wellesley, Massachusetts

Before Subcommittee on Small Business Crime Prevention Act

March 7, 1984

Introduction

My name is Leslie D. Ball. I am Professor of Information Systems at Babson College where I am responsible for teaching and developing computer graduate and undergraduate courses for students who are business majors. In addition, I have done extensive research in the area of computer crime and security and am active in various professional organizations.

For the past twenty years I have worked in the computer industry and during the last ten years I have authored several articles and books about computer crime and its prevention. One book, Information Systems Audit Review Manual, is used as a study guide by persons who take the Certified Information Systems Auditor examination. It is this certified group of individuals who are primarily responsible for insuring that our nation's largest corporation have adequate security protection.

In 1980 I became the Founding Chairperson of the Association of Computing Machinery's Special Interest Group on Security, Auditing, and Control which is commonly referred to as SIGSAC. ACM is the world's oldest organization of computer professionals and SIGSAC is one of thrity-six special interest groups that ACM

members can belong to. SIGSAC publishes a quarterly newsletter, sponsors presentations at national meetings and conducts conferences and workshops all addressing computer crime and computer crime prevention issues. The organization currently has nearly 1,100 members.

Scope of Computer Crime Problem

Let me start by saying that computer crime is growing as computers are becoming more commonplace. Prior to 1950 banks were not very concerned about check forgery because personal checks were not very popular. Today, however, nearly every adult has a checking account and approximately 40 billion checks are processed by the American banking system each year. I use the example of checks to demonstrate how commonplace something that was once rare is now commonplace less than thirty-five years later because computers are also becoming so available. Very soon every office worker, whether they are a clerk or an executive or whether they work in a large organization or a small one, will have a computer terminal on their desks. That is when computer crime will be a major problem for American businesses and it will take forms that we cannot even anticipate at this time.

Computer crime can be thought of as the theft, destruction, or disclosure of data, programs, or equipment. For example, someone might destroy a company's accounts reveivable files which would make it difficult or impossible to determine who owes the company funds. But damage could also occur to a person as a result of a computer crime. For example, someone might alter

computerized voter registration lists in a county to disenfranchise a minority group or someone could alter an individual's credit record at a small credit agency to make it impossible for them to buy goods on credit or to secure a loan.

Victims come in all sizes and shapes. They are small companies and large companies. They are non-profit organizations and highly profitable companies. They are poorly managed companies and some that we think of as being the best managed. Some are even computer companies. About the only characteristic that they have in common is that some system within the organization has a missing control that the penetrator has found.

I would like to say that the computer crime problem is declining but I cannot. We are now in an era in which computers are being used in ways never thought possible. Computers are used by individual executives to develop financial models so that they can ask "what if" questions. The results of these models will enable them to make decisions about managing their department or companies.

We can now move billions of dollars daily between banks and businesses. We can now create electronic offices that allow us to send electronic mail messages from individual to individual. Because of advances in telecommunications, we can now have one company's computer access another's to order goods and services. Data within most companys' computers can now be made available to everyone in the company as the computer moves to an "access free world." Finally, the fastest growing segment of our working

population is the "knowledge worker" who must have access to computer resident information to complete their assigned tasks.

I relate all of these changes to you because, although they alter the way in which businesses are run in a positive way, they create more opportunities for the computer criminal. When new technology is introduced it is always marketed with its advantages somewhat over-stated and its disadvantages rarely mentioned. To the vendors defense, the disadvantages are seldom totally known. For example, I do not believe that anyone can predict how the growth of electronic mail will create new computer crimes, but I do believe that crimes that we have never seen before will begin to be committed as electronic mail increases in popularity. I do not mean to suggest that all new technologies be held from the marketplace until their crime potential be analyzed, but only that new technologies are watched carefully because they represent an entirely new ballgame for computer thieves.

Special Problems of Small Businesses

How does all of this relate to small businesses? First, the problems are complex even for large businesses and they are becoming more complex. Large businesses are committing more of management's time to the problem and are hiring specialists to solve the problems.

Small businesses are really no less complex than a large business. A computer can solve their problems just as it can for a large business. The costs of computer hardware and software has declined so rapidly that nearly all businesses can now afford

computers to complete the tasks that I mentioned earlier.

The problem that a small business has is the lack of manageament time and expertise. Virtually every small businessperson has more tasks than he can complete in most business days. If he is given the following options:

1. spend twenty hours on developing security controls and you may save $20,000 someday, or
2. spend twenty hours in the development of a new production procedure and you will save $40,000 in production costs over the next year, it is clear what option he will take.

Computer crime, therefore, is a low priority item for the small businessperson. Also, they do not have the expertise in-house to deal with the problem.

Another issue is cost. To develop fairly secure systems requires that a lot of money be spent. Excess cash for this type of investment is often not available to small businesses. For small businesses every spare dollar must be invested to yield a positive return.

Finally, there are no information resources that are readily available to small businesses. For example, SIGSAC members all come from academia or large businesses. All of the trade journal articles about computer crime prevention assume that the audience is a large organization. Software and hardware prevention products are also primarily developed for larger organizations.

I am in support of the task force proposed by this bill. In spite of the fact that the small businessperson might not realize

that computer crime is a problem for him, it is. This task force should develop vehicles to combat that problem. My chief concern is that the task force recommend an information resource center and educational programs for the small businessperson. These resources should enable the small businessperson to learn about the problem and to become properly educated about how to protect himself against what is in reality a severe problem.

I would urge you to support the bill as it will have a positive impact on the management of small businesses.

Thank you.

Senator TSONGAS. I find it hard to imagine that you could have a user friendly computer that gives people full access to the system and have it remain secure. Take the example of someone who wants to wipe out the accounts receivable. Can you really protect a company from a disgruntled employee who would engage in something like that?

Dr. BALL. There will always have to be a trusted group of employees, but we can offer certain levels of protection at certain levels in the organization. We can provide almost a pyramid-shaped protection level, so someone has access to just the top of the pyramid or someone has access to everything in the pyramid, and we can do that, from a technological standpoint, in many large systems. But in most smaller systems, you don't have that capability.

Senator TSONGAS. Give me an example.

Dr. BALL. In a business environment, there are many, many different types of systems. Let me take an airline reservation system that we are all familiar with.

Senator TSONGAS. Let's take a small business. Let's say there are 50 people involved with the business.

Dr. BALL. In that type of environment, we do not have many of the technological safeguards that we have in a larger environment. Two or three people would probably be involved in the day-to-day accounting functions. They would have to have total access to the entire system, and that is where you have the concept of the trusted employee, and you really have to put a degree of trust in those people.

What you also would like to do is to protect the organization from the other employees who should not have access to that system, and you do that by institution management controls such as turning off terminals and locking doors and some very, very simple concepts that, unfortunately, small business people are not aware of and they need to be made aware of through educational facilities.

Senator TSONGAS. Stepping up for a moment, let's take a 1,000-person organization where, clearly, you have a large number of people involved with the computer. What do you do in that case?

Dr. BALL. In those cases, you have division of responsibilities, just as you do in an organization that uses strictly paper for the same control. One person is allowed to do one type of task only. You control access to that task. The computer can actually control when the person started to work on a job, when they ended working on the job, what records they accessed, and so forth. We can keep records of that. So in a larger organization, it is much easier to do that. We do that through password control. The computers all have clocks on them, and it is very easy to control access in a much larger organization.

Senator TSONGAS. I would assume that is effective against your average disgruntled employee, but I would assume at certain levels of sophistication of computer software, et cetera, the controls you would have to build in would be so expensive relative to the danger that most people would not do that. Is that correct?

Dr. BALL. Unfortunately, that is true, and I would even suggest that there are some very large institutions in this country that have not installed controls that they should have because of the costs involved.

Senator TSONGAS. So the kind of person that you would have to be worried about would be somebody like yourself? [Laughter.]

Dr. BALL. That is quite true; in fact there are several cases of computer security consultants who have stolen from the companies they have worked for.

But you have to be concerned about the insider more than the outsider. The person who is working as an accounts receivable clerk, who identifies that there is a problem with the system, can then steal from the system without you knowing about it. That is the person that you really have to be concerned with, not the person who is in your operation to make delivery and happens to pick up a data tape or some other media. That very infrequently occurs.

Senator TSONGAS. My understanding is that they have done profiles on the average hacker, et cetera, and you are talking about insiders more than outsiders.

Dr. BALL. Yes; the big problem is the insiders. The profile of a computer criminal is one who is probably very bright, very eager, hardworking, highly motivated, technically competent, young, 18 to 30 years old, typically male—we tend not to see females, as a matter of fact—involved in every part of the business.

Senator TSONGAS. When we pass the ERA, we will take care of that.

Dr. BALL. That is right. The issue, however, is that the hacker, which is the 15-year-old kid who has an Apple computer at home, grows out of that stage before too long. He goes to college and he gets into some interesting courses, and he just doesn't have the time to do the hacking that he once did. He recognizes that there are more important, more interesting things to do, and so hackers are very young. They might do a lot of damage to a large business, but they will not be the problem to the small businessperson.

STATEMENT OF A. JASON MIRABITO, ESQ., PROFESSOR OF LAW, SUFFOLK UNIVERSITY LAW SCHOOL

Mr. MIRABITO. Good morning, Mr. Chairman.

I am Jason Mirabito. I am an attorney and a professor of law at Suffolk University Law School in Boston, Mass., where I teach a course entitled, somewhat whimsically, "Computers and High Technology Law."

I appear before you today on behalf of SBANE, which is the Smaller Business Association of New England, an association of more than 2,000 member companies, some of whom are computer product and service companies and many of whom have computers in their various businesses.

Mr. Chairman, there has recently been much activity, both on the Federal and the State level, concerning these issues of computer crime. I would like to very briefly now focus my attention on two points, that of legislative activities on the Federal level and the State level to control computer crime and, second, SBANE's view of the role of the Federal Government, and particularly the Small Business Administration, in dealing with computer crime issues.

A more extensive discussion is contained in my written submission.

On the Federal side, crimes against the United States are codified in some 40 sections in title 18 of the United States Code. Most of the debate in recent times surrounding the need for specific Federal legislation regarding computer crime has focused on the adequacy of these various provisions to effectively cover the ambit of crimes associated with computer systems.

Evidently, a need for such legislation has been felt by some Senators and some Congressmen. Back in 1977, Senators Ribicoff and Percy sponsored Senate bill 1766, the Federal Computer Systems Protection Act of 1977. That has been followed by Senate bill 240 later on and, most recently, Representative Nelson's bill.

Testimony which has been given on some of these bills has indicated that some people have questioned the necessity of the proposed legislation in light of the already-existing Federal legislation, which could be interpreted to cover virtually all presently existing types of computer crime.

Further, some people have questioned the wisdom of enacting Federal legislation which might expand Federal jurisdiction into areas presently already within State or local control.

I mentioned that Senator Nelson's bill, which is H.R. 1092, was reintroduced in January 1983. This bill has not yet been passed and merited an editorial in Computerworld fairly recently—Computerworld is a leading DP industry magazine—to the effect that, quote: "Perhaps the time has come for DP professionals to let their representatives know that a computer crime bill deserves serious attention before 6 years pass and more hackers grow up to try their hands at computer and information abuse."

On the State level, depending on whose statistics one reads, and depending on what one's definition of computer crime is, some 18 to 20 to 22 States have enacted computer-related crime legislation. These pieces of legislation vary from very simple modifications and

amendments to State larceny statutes to very broad computer crime legislation such as that which was enacted in 1978 by Florida.

In my home State of Massachusetts, for example, legislation was enacted in 1983 relating to computer crime. What Massachusetts did, quite simply, I think, is amend the State larceny statute to define the term "property" which is subject to the larceny statute to include electronically processed or stored data, either tangible or intangible.

Further, Massachusetts amended its State trade secret theft statute to include in the term "trade secret" anything tangible or electronically kept or stored. The Massachusetts legislation is typical of the approach that has been taken by some States, though I think it is quite effective. I should note, however, that our Lieutenant Governor is contemplating introducing legislation in Massachusetts which would in fact broaden the definition and scope of the computer crime legislation to that somewhat similar to proposed Federal legislation.

Senator TSONGAS. How were those bills passed? Who was the prime mover of the legislation?

Mr. MIRABITO. In Massachusetts?

Senator TSONGAS. Yes.

Mr. MIRABITO. The industry. Well, actually it was not the industry directly, but through industry trade associations, accounting firms, and attorneys; it was also in large part due, on the House side, to work by the Criminal Justice Committee.

If one looks at the hearings that were held on that, there was not an overabundant amount of divert industry support for it. I think the reason for that is not because the industry was not in favor; it was because, I think, in some cases, companies did not want to come forward themselves and say computer crime is a problem that we legislate against.

Senator TSONGAS. So the legislation was developed not by a trade association but by the State legislature itself?

Mr. MIRABITO. Yes, largely that is correct.

A question is, with the State enactments and with the pending Federal legislation, if the latter is to be enacted, why is this bill necessary? The point has been argued by some that Federal legislation is unnecessary, although I do not personally support that position. Yet some 20 States have decided, for one reason or another, that their own State legislation was or may have been inadequate to deal with the problem of computer crime.

The argument has also been made by some parties in favor of further study of the matter before enacting Federal legislation. To the extent that such study is needed, certainly then S. 1920 will go far to address those concerns.

If one accepts the argument that many computer crimes are either not discovered, not discovered until too late, or not reported at all, then S. 1920 is an important bill, because the various State and Federal laws look to punishment and, to some extent, deterrence, of the crimes once committed. They therefore look at and attempt to treat the problem after the fact; that is, regulate how the governments treat computer crimes after they have been committed.

The existing Federal and State laws do not, and obviously cannot, establish the precautions necessary to prevent the computer crime from being committed in the first place. It is here that S. 1920 can be of immense assistance, particularly to small companies who cannot afford to hire the consultants to fashion their security measures to deter computer crimes directed against them.

What should be the role of the Small Business Administration? We note that S. 1920 places upon the U.S. Small Business Administration the primary responsibility in establishing and directing the task force under the bill and, most importantly, later disseminating to small businesses information on computer crime and security techniques.

The SBA is, we believe, the proper authority to perform the tasks assigned under S. 1920. The SBA is the primary Federal agency small businesses realistically look to for advice and guidance in many other areas which affect small businesses, such as in financing, management assistance, and most recently in exporting.

Since the mission of the SBA under the Small Business Act is to aid, counsel, assist, and protect the interests of small businesses, it is believed proper for the SBA to assume the responsibility in the area of dissemination of computer crime detection and prevention information. The close relationship that SBA has with small business makes it uniquely qualified to be the primary support agency for the task force.

The subsequent dissemination of information to small businesses nationwide can best be accomplished through the large number of regional and district SBA offices already in operation throughout the country.

Mr. Chairman, we in small business believe that the cost of the task force and subsequent SBA activities are well worth the potential benefit to small business which may be gained by the work of the task force and the very valuable work to be performed by the SBA in disseminating information on this very important concern of small business in this country.

Thank you very much.

[The prepared statement of Mr. Mirabito follows:]

STATEMENT OF A. JASON MIRABITO, ESQ., PROFESSOR OF LAW, SUFFOLK UNIVERSITY LAW SCHOOL: REPRESENTING THE SMALLER BUSINESS ASSOCIATION OF NEW ENGLAND, INC.

Introduction

Mr. Chairman, Members of the Committee and Audience:

I am A. Jason Mirabito, an attorney and professor of law at Suffolk University Law School in Boston, Massachusetts. I teach a course entitled "Computers and High Technology Law" in which one of the topic deals with the issues of computer crime.

I appear before you today on behalf of SBANE, the Smaller Business Association of New England, an association of more that 2,000 member companies, some of whom are themselves computer product or service companies, and many of whom possess data processing systems in their business. SBANE is sensitive to the concerns of its membership, and to those of small business in general, regarding the problem of computer crime committed against their businesses.

Mr. Chairman, there has been a great deal of legislative interest both on the federal level and the state level on this issue of computer crime. I would like to focus my attentions on two matters, first legislative activities on the federal and state level regarding computer crime and more particularly the effect or expected effect of those activities, and, second, SBANE's view of the proper role of the Federal Government, particularly the Small Business Administration, in dealing with computer crime issues.

Federal Legislative Activity

Crimes against the United States are codified in Title 18 of the United States Code. Title 18 contains some 40 sections that potentially may be used in the prosecution of computer crimes.

Those most commonly applied are section 641 (embezzlement or theft of public money, property or records), section 2314 (interstate transportation of stolen property), section 1341 (mail fraud), and section 1343 (wire fraud). Most of the debate surrounding the need for specific federal legislation regarding computer crime has focused on the adequacy of these provisions to effectively cover the ambit of crimes associated with computer systems. Evidently, there is a need for such legislation which has been perceived by some members of the Congress, albeit without success up to the present time. Senators Ribicoff and Percy sponsored S.1766, the Federal Computer Systems Protection Act of 1977. Hearings were held in the Senate but no further action was taken. Senator Ribicoff reintroduced a very similar bill in 1979 as S.240. S.240 met with an equal lack of success and testimony by some persons questioned the necessity of the law in the light of already existing legislation which could be interpreted to cover all presently-existing types of computer crime. Further, some questioned the wisdom of enacting federal legislation which might expand federal jurisdiction into areas presently within state or local jurisdiction. In brief, S.240 attempted to make criminal, in interstate commerce, activities including access to a computer, computer system or network for the purpose of committing a fraud or in order to obtain money, property or services by means of false or fraudulent pretenses. Also, the bill would have made criminal the unauthorized access, alteration, damage or destruction of any computer, computer system or network, any computer software program, or data

contained in a computer system. The bill would have, therefore, presumably covered unauthorized use of computer systems, the alteration or destruction of information and files in a computer system, the introduction of fraudulent data into a computer, and, importantly I believe, the theft, on-line or off-line, of money, property (including programs or valuable data), or services.

During the 97th Congress, Representative Nelson introduced H.R. 3790, The Federal Computer Systems Protection Act of 1981, but no action was taken on the bill. This bill was very similar to S.240, except that it contained provisions tempering Federal jurisdiction in light of concurrent state jurisdiction and the magnitude of state interest in the matter. Representative Nelson re-introduced his bill in the 98th Congress as H.R. 1092 in January 1983. This bill has not yet been enacted, and merited an editorial in Computerworld, a leading DP industry magazine as follows: "Congress moves very slowly on bills in which a public mandate is not putting pressure on representatives to speed the bills along. Perhaps the time has come for DP professionals to let their representatives know that a computer crime bill deserves serious consideration before six years pass and more hackers grow up to try their hands at computer and information abuse" (Computerworld, Dec. 5, 1983, at 54).

Problems in enacting legislation may include not only the opinion by some federal law enforcement that presently existing legislation is sufficient, but also the view that the issue is more effectively tackled on the state level. We will look at this latter matter presently. Finally, and importantly in light

of S.1920, it is reported that some persons, including those in the DP industry, prefer additional study before legislation (Computerworld, Nov. 28, 1983, at 1, 8).

State Activity

Depending on whose statistics one reads, and depending on what one's definition of computer crime is, some 18-20 states have enacted computer-related crime legislation. These vary widely, from simple amendments to state larceny statutes to comprehensive legislation such as that enacted in Florida.

In my home state of Massachusetts, legislation was enacted in 1983 relating to computer crime. Massachusetts (quite simply) amended the state larceny statutes to define the term property subject to the larceny statute to include "electronically processed or stored data, either tangible or intangible." Massachusetts also amended its state trade secret theft statute to add the following: "The term 'trade secret' as used in this paragraph means and includes anything tangible or electronically kept or stored. . . ." The amendments arose out of a 1981 Massachusetts Supreme Judicial Court decision (Commonwealth v. Yourawaki, (425 N.E.2d 298 (Mass. 1981)), in which the Court found that the data contained on a video tape cassette did not come within the "property" definition under the then-existing statute.

With the State Enactments And Pending Federal Legislation, Why is this Bill Necessary?

As discussed above, the point has been argued that federal legislation is unnecessary. Yet some 20 states have decided, for

one reason or another, that their legislation was or may have been inadequate to deal with the problem of computer crime. The argument has also been made that some parties favor further study of the matter before enacting federal legislation. To the extent that this is true (if it is), certainly then S.1920 will go far to address those concerns.

However, notwithstanding these "necessity" arguments, I believe the provisions of S.1920 are, in fact, necessary to be enacted. If one accepts the argument that many computer crimes are either not discovered, not discovered until too late, or not reported at all, then S.1920 is important.

The various state and federal laws look to punishment (and to some extent deterrence) of the crimes once committed. They, therefore, look at and attempt to treat the problem after the fact, that is, regulate how the governments treat computer crimes after they have been committed. The existing federal and state laws do not establish the precautions necessary to prevent the computer crime from being committed in the first place. It is here that S.1920 can be of immense assistance particularly to small companies who cannot afford to hire the consultants to fashion their security measures to eliminate or at least deter computer crimes directed against them.

My only suggestion for addition to the present bill, or perhaps other legislation, is that medium and large businesses are, as well, interested in an assessment of the issues to be addressed by the Task Force to be established under S.1920 for those computer crimes committed against them. The benefit of

such an undertaking may be, at least, a crystallization of the computer crime issues across the board which might move the Congress to enact federal legislation.

The Role of the Small Business Administration

We note that S.1290 places upon the U.S. Small Business Administration the primary responsibility in establishing and in directing the Task Force to be established under the bill and, most importantly, disseminating to small businesses information on computer crimes, security techniques for computer systems used by small businesses, providing regional forums to assist in information exchange, and establishing a resource center within the SBA.

The SBA is, I believe, the proper authority to perform the tasks assigned under S.1920. The SBA is the primary federal agency small businesses look to for advice and guidance in many other areas which affect small businesses (in the areas of management assistance, financing assistance, and recently exporting). Since the mission of the SBA is to help people get into business and to stay in business and to aid, counsel, assist and protect the interest of small business concerns under the Small Business Act, it is believed proper for SBA to assume the responsibility in the area of dissemination of computer crime detection and prevention information. The close relationship between small business and the SBA makes the SBA uniquely qualified to be the primary support for the Task Force. The subsequent dissemination of information to small businesses nationwide can be best accomplished through the large number of

regional and district SBA offices already in operation throughout the country. One suggestion we would make is that Section 4 of S.1920 be amended to require that information contained in the resource center established under the bill be disseminated throughout SBA offices nationwide through handbooks, pamphlets, etc. to reach small businesses across the country. Another suggestion is, in Section (3)(B)(x) of S.1920, that the "additional qualified individuals" should perhaps be limited to small business people. Finally, in Section (3)(E) of S.1920, the phrase "without additional pay" is presumed to mean government employees, since private members do not receive any "basic" pay.

On a cost/benefit analysis, we note that the House Report on the House version of S.1920 estimates the cost of the Task Force plus the cost of information dissemination will be approximately $500,000 for the years through 1989.

We in small business believe that this cost is well worth the potential benefit to small business which may be gained by the work of the Task Force and the very valuable work to be performed by the SBA in disseminating information on this very important concern of small business in this country.

SBANE views and will follow this legislation with great interest. SBANE stands ready to provide you with any additional support, comments, or feedback you may desire on the above subject. Thank you.

Senator TSONGAS. I wonder whether each of you could address the counterargument which is, look, there are these organizations—yours is one—that deal with this issue, and rather than have the Government come in and try to sort of "uncle" their way through the problem, why not allow the marketplace to work its will, and they will eventually come to you when there is a real problem, and it will be dealt with?

Mr. MIRABITO. Of course, we don't want to deal with the issue after the problem. We want to do it beforehand, to prevent the so-called crime from happening in the first place.

I think that most small businesses, realistically, may not even think about the issue of computer crime. If they think about it, they probably don't spend the time to do anything about it and will certainly not spend, I think in most cases because of the current level of knowledge, the money to do something about it.

I think this bill is important because it puts the responsibility on the SBA—and small businesses have regular contacts with the Small Business Administration. It is also an educational process—I think they can be made aware of the security issues that they face and may be encouraged to take action based on this legislation, based on effective dissemination of the information developed by the task force.

I should note that the information that will be contained in the resource center contemplated, I presume, will be in Washington. It would seem to me a better course to have drafted in the legislation, or in any regulations which are promulgated pursuant to it, provisions to make sure that this information is actually disseminated down to the district level of the Small Business Administration offices and to have an education program which SBA offices will, in their management assistance programs and other programs, use to make small businesses aware and concerned about this issue.

Dr. BALL. I think that the problem clearly is different in a small business than it is in a large business. As a matter of fact, earlier you asked me a question about characterizing some computer crimes, and I think it is very easy for us to talk about larger businesses, but we don't know what the parameters are in the smaller businesses. We need to look at those issues in the smaller businesses and try to identify what the potential problems are for those individuals.

No study has been done for that. No educational vehicles are available for those people. No consulting personnel are available for those people at an affordable cost. For the most part, as I think we have both testified, small businesspeople don't recognize the need and somebody has to educate them to the fact that they are a potential victim of a computer crime.

Senator TSONGAS. I agree with you, but I am sure you can anticipate the rebuttal to that, which would be that—I remember once that Hubert Humphrey gave his last speech to the Congress, and Morris Udall got up and, in his typical style, said that Hubert had solutions for which there were not even problems yet.

That, I think, is going to be the criticism leveled against this bill, like seat belts or smoking or whatever. In fact, if people do not recognize the problem, is it the proper role of government to inter-

vene, in essence, and say that even though you don't recognize the problem, here it is and we are going to help you?

I am not saying there is an answer to that, but I think that will be the charge that we will have to try to deal with.

Dr. BALL. I would say that there is a problem. The problem is well recognized in larger businesses, and just because computers are moving into smaller businesses implies that the issue will go down to their level. I think that that is the defense that one would have to take.

Senator TSONGAS. Well, I think it would be important if some of the small business organizations which have been active in this also begin to get their membership to contact their particular Senators, so it is a felt concern as opposed to a theoretical concern.

I have some other questions here which I will submit to you for you to respond to them in writing for the record. But I would like to try to get this hearing resolved this morning. We are looking to a May markup and would like to by that point have resolved the questions of task force membership: should there be a task force?; what kind of timeframe?; and that kind of thing. We will be working with you as the next 2 months proceed.

Thank you very much for coming.

[Subsequent information was received and follows:]

United States Senate

COMMITTEE ON SMALL BUSINESS
WASHINGTON, D.C. 20510

March 12, 1984

Jason Mirabito, Esquire
Professor of Law
Suffolk University Law School
Beacon Hill
Boston, Massachusetts 02114

Dear Professor Mirabito:

We would like to extend to you our thanks for testifying at the March 7, 1984 hearing on S. 1920, the Small Business Computer Crime Prevention Act. Your testimony will be very helpful to the Members of the Senate Small Business Committee.

Due to the time constraints of the hearing, there were some questions we did not get a chance to ask you. In order to make the testimony complete, the Committee would greatly appreciate it if you would consider these issues now and provide written responses for inclusion in the permanent hearing record.

1). There is general agreement about the need to educate the small business community about computer security controls. The SBA is ready to proceed immediately to provide information to small businesses on computer security. Do you support the SBA approach to proceed without the task force and 18-month study period?

2). Is it your opinion that the SBA working together with ICST of the Commerce Department, and for profit and not for profit groups can provide the most cost effective help to the small business community concerning computer security?

Please send your responses to Mike Morris, Counsel of the Small Business Committee staff at 428A Russell Senate Office Building, Washington, D.C. 20510. Should you have any questions

about the hearing or this request, please feel free to call Mr. Morris at 224-2016, or Alan Chvotkin, Minority Chief Counsel, at 224-8497.

Thank you in advance for your cooperation and prompt attention to this matter. Again, your participation in this hearing was greatly appreciated.

Sincerely,

PAUL TSONGAS
United States Senator

LOWELL WEICKER, Jr.
Chairman
Senate Committee on
Small Business

SUFFOLK UNIVERSITY LAW SCHOOL — BEACON HILL — BOSTON, MASSACHUSETTS 02114
OFFICE OF FACULTY
(617) 723-4700

March 27, 1984

Michael Morris, Esq.
Counsel
Senate Small Business Committee
428 A Russell Senate Office Bldg.
Washington, D.C. 20510

Re: S.1920 the Small Business Computer Crime Prevention Act - Additional Comments

Dear Mike:

This letter is in reply to the March 12 letter from Senators Tsongas and Weicker. The letter posed two questions which I would like to address.

The first question relates to whether it is advisable to allow the SBA to proceed presently in a process to educate small businesses on computer crime and computer security controls. I recall from the testimony of the SBA officials on the day of the hearing on S.1920 that they stated that the SBA was ready to roll out a new program on the issue. Although I am not specifically aware of the "metes and bounds" of the new SBA program, it seems to me preferable to have a legislative mandate to the SBA to provide the services, particularly the establishment of the resource center and the dissemination of information to the regional and district SBA offices. The legislation would also provide the SBA, by way of the Task Force, with necessary or at least useful information it may not presently possess. Finally, it may be useful to have the SBA embark on its intended procedure simultaneously with the activities of the Task Force and to provide a contact relationship between the two to perhaps produce some synergistic effect. In summary, I believe that the SBA intended procedure would be useful, but not sufficient without the legislative mandate.

The second and last question asks whether the SBA, Commerce and other groups can provide the most cost effective advice to small business in this matter. I believe this is the case, as pointed out briefly in my written submission on S.1920. The main reasons for this are: (1) that the SBA deals with small business on a continuing basis and is therefore best able to

ask the right questions which would be useful in formulating a policy and a program, and (2) the SBA is (importantly) best able to disseminate computer security information through its many regional and district offices. No other federal agency has such a large number of offices which on a continuing basis counsel small businesses.

If would like me to elaborate on any the above points, or if you require any further information, please do not hesitate to call upon me.

Sincerely,

A. Jason Mirabito, Esq.
Associate Professor of Law
Suffolk University Law School

United States Senate
COMMITTEE ON SMALL BUSINESS
WASHINGTON, D.C. 20510

March 12, 1984

Dr. Leslie Ball
Associate Professor of
Information Systems
Babson College
Babson Park
Wellesley, Massachusetts 02157

Dear Dr. Ball:

We would like to extend to you our thanks for testifying at the March 7, 1984 hearing on S. 1920, the Small Business Computer Crime Prevention Act. Your testimony will be very helpful to the Members of the Senate Small Business Committee.

Due to the time constraints of the hearing, there were some questions we did not get a chance to ask you. In order to make the testimony complete, the Committee would greatly appreciate it if you would consider these issues now and provide written responses for inclusion in the permanent hearing record.

1). There is general agreement about the need to educate the small business community about computer security controls. The SBA is ready to proceed immediately to provide information to small businesses on computer security. Do you support the SBA approach to proceed without the task force and 18-month study period?

2). Is it your opinion that the SBA working together with ICST of the Commerce Department, and for profit and not for profit groups can provide the most cost effective help to the small business community concerning computer security?

3). Do you know what percentage of the small business community is being reached and educated in computer security by private sector organizations - like SIGSAC?

4). Can we expect the private sector to meet the educational needs of small business in the matter of computer security?

Please send your responses to Mike Morris, Counsel of the Small Business Committee staff at 428A Russell Senate Office Building, Washington, D.C. 20510. Should you have any questions about the hearing or this request, please feel free to call Mr. Morris at 224-2016, or Alan Chvotkin, Minority Chief Counsel, at 224-8497.

Thank you in advance for your cooperation and prompt attention to this matter. Again, your participation in this hearing was greatly appreciated.

Sincerely,

PAUL TSONGAS
United States Senator

LOWELL WEICKER, Jr.
Chairman
Senate Committee on
Small Business

Babson College

Babson Park
(Wellesley)
Massachusetts
02157-0901
(617) 235-1200
Cable: Babcol

April 4, 1984

Mr. Mike Morris
Counsel of the Small Business Committee Staff
428A Russell Senate Office Building
Washington, DC 20510

Dear Mr. Morris:

In reply to the March 12,1984, letter from Senators Tsongas and Weicker, I should like to respond to their questions.

Question #1

While I believe that the task force and 18-month study period are well conceived, I see nothing wrong with the SBA commencing to provide information to small businesses on computer security. They have the mechanisms in place to provide such information at a reasonable cost and should do so while the study period is ongoing. Any information that they might provide is solely needed by small businesses.

Question #2

In the absence of knowing about any other organizations that might provide information, SBA and ICST with non-government groups should be effective in helping the small business group. It is my opinion that one function of the task force should be to determine the best vehicles to supply these services. However, in response to this question and question #1, I would hope that this does not become a territorial issue. There is an enormous amount of work to be done. Several organizations, public and private, should participate.

Question #3

There is litte data about how well the small business community is being reached by private sector organizations. However, after reviewing the membership list of SIGSAC and looking at the rosters of previously conducted seminars, I would have to conclude that the percentage is very low and is approaching 0%.

Question #4

At the present time we cannot expect the private sector to meet the educational needs of small business. This is because the costs of such services are much to expensive for them to pay. I would suggest that a function of the task force should be to recommend more vehicles to supply these services at costs which are palatable to small business people.

I trust that these comments will assist the committee in their work. Should you wish additional comments or information, please contact me.

Sincerely,

Leslie D Ball

Leslie D. Ball, Ph.D.
Professor
of Information Systems

Senator TSONGAS. Dr. Sherizen and Mr. Schuldenfrei? Mr. O'Mara and Mr. Kaiser?

Did I pronounce your name correctly, Dr. Sherizen?

Dr. SHERIZEN. Yes, thank you, Senator.

Senator TSONGAS. I tend to be sensitive on that issue myself, so I apologize to Mr. Schuldenfrei.

How did we allow someone from Minnesota to get into this panel? [Laughter.]

I understand that you all have statements. Why don't we proceed? Dr. Sherizen, you are first on the schedule.

STATEMENT OF DR. SANFORD SHERIZEN, PRESIDENT, DATA SECURITY SYSTEMS, INC., NATICK, MASS.

Dr. SHERIZEN. Thank you, Senator.

I would like to have my written testimony entered into the record and give you some additional oral comments.

My name is Sanford Sherizen, and I am very honored to appear before the committee and particularly you, Senator, a Senator for whom I have great respect.

For background purposes, I am one of the few trained criminologists in the United States actively working as a computer security consultant. In addition to founding my own computer security consulting firm, Data Security Systems, Inc., in Natick, Mass., I teach courses in computer security, white collar crime, and private security in the College of Criminal Justice at Northeastern University.

Senator TSONGAS. What is your background?

Dr. SHERIZEN. As a criminologist and sociologist.

Senator TSONGAS. What educational background do you have?

Dr. SHERIZEN. A Ph. D. from Northwestern University.

Senator TSONGAS. In?

Dr. SHERIZEN. Sociology, with concentration in criminology.

Utilizing my background of over a decade of university teaching and research on the sociological and criminological problems of crime control strategies and crime prevention techniques, I provide

consulting services to businesses, government agencies, and institutions.

My consulting is oriented toward computer crime prevention, providing executives with sophisticated evaluations, organizational assessments, implementation strategies, and management seminars on cost-effective security options. At present, I am completing a book under contract with the American Management Associations with a tentative title, "Computer Security Management for the Non-Technical Executive."

This book, as well as the emphasis of my consulting, stresses four major points which are applicable to large or small businesses as well as government. I would like to state on these because I think they summarize some of the most important issues in computer security management.

First, computer security is no longer an optional decision but may be fundamental to the survival of a business. It is no longer cost effective for a business to treat computer crime as just another type of business risk which is controllable by such traditional approaches as detection after the fact, insurance coverage, or absorption of losses.

Second, the core issues of computer security can and must be understood by nontechnical managers, since they will be given the control responsibility, particularly because today's technical solution is tomorrow's social problem.

Third, the essence of computer security lies with management controls, reviews, and policies developed with the active support and involvement of top management.

Fourth, there are a variety of management questions that managers can learn which they can raise with technical staffs in order to evaluate the adequacy of computer protections in their business.

These are what I call part of the new security rules for the computer age.

Today's topic is the protection of small businesses from computer crime. It is an extremely important topic because, from my perspective, I think we are heading toward two basic classes of businesses in our society—large corporations which have or will have sufficient, or at least a number of, security protections; and a majority of small businesses that will find themselves virtually unprotected. Given, Mr. Chairman, that the Senate today is talking about prayer in public schools, possibly we should also be talking about prayer for small businesses.

Smaller businesses will become the easier target for computer criminals, and since they have less ability to absorb losses, they will most likely be the larger victims of computer crime.

There is a parallel here to street crime, when police protection in one area often leads to a spillover or a displacement of crime to other areas. What I suspect will be happening is that computer crime will increasingly be displaced onto small businesses.

With an unknown but significant percentage of business failures already attributable to crime—one estimate is 10 percent of all failures every year—one can conclude that the rate of small business bankruptcies may indeed be increased by computer crime problems.

Senator TSONGAS. The 10 percent is of all businesses?

Dr. SHERIZEN. That is right.

Senator TSONGAS. You are not talking about computer businesses?

Dr. SHERIZEN. No, it is crime affecting all businesses, and that was the Chamber of Commerce estimate as I remember the citation.

My own small business, Data Security Systems, Inc., was established out of an awareness that there are a number of areas in our society requiring crime control and prevention measures. While certain types of crimes are much more difficult to prevent, I have felt that computer crimes are, to a degree, preventable.

Prevention, however, is restricted by many sociological and organizational reasons and factors which limit the ability of a business to accept preventive measures. My firm was founded in order to provide an interdisciplinary approach to the problem of computer crime by combining the insights into human behavior that can only come from the social sciences with technical knowledge of computers and technological development.

There are a number of computer security protections that have been developed over the years. These are physical security, procedural or managerial controls, and technical security, which covers hardware, software, and communications protections over systems and data.

Too few of these are known by large businesses or small businesses. In fact, it has been my experience that computer security has become an issue that no one owns. This often critical responsibility is left without full ownership in large corporations as well as small businesses, with the result that it becomes a management problem only after detection, which may indeed be too late.

I should note here, Mr. Chairman, that small businesses have become a major market for computer vendors. In a recent issue of "Computerworld," a "Time" magazine study was cited indicating that computer usage by small businesses is projected to jump by almost 50 percent in the year between mid-1983 and mid-1984, with the majority of sales being made to companies with less than 20 employees. In the vast majority of those businesses, I would predict there is virtually no protection in place.

Small business owners tend to purchase computers by word-of-mouth advertising, to rely upon their own technical staff, if there is such, or by computer sales representatives. In purchasing computers today, one is led to believe it is possible to buy a complete computer for a certain price. The user-friendly emphasis, the a-la-carte mode of purchase, and the lack of security knowledge effectively work against the purchase of computer security provisions.

If a business was going to purchase a business car, it could correctly assume that the car would come with brakes, windshield wipers, and door locks. There would be no need to ask if these were included at extra cost. Yet this assumption about the automatic inclusion of computer protections would indeed be incorrect.

With this information as background, I applaud this committee for what it seeks to accomplish. Computer security consultants will not be able to solve the computer crime problem for small businesses, first, because there are too few of us, but, second, the realities are that larger corporations are a more natural market. They are

more able to afford and support our efforts, while smaller businesses have more difficulty in deciding that security is a cost-effective decision.

Government has an extremely important role to play in assisting these small businesses. In that regard and in support of the proposed legislation, I would like to make several recommendations for the task force and the resource center.

The first recommendation would be the establishment of a hotline for handling inquiries from small businesses concerning computer security products, approaches, materials, or even consultants. This could obviously be part of that resource center concept.

Second, businesses generally require assistance with the criminal justice system. I envision a small businessperson who wishes to know what to do when he or she finds out that they have been victimized, if found out before bankruptcy.

It is difficult enough to detect computer crime, but there are even more difficulties when one does not know where to go for advice as to appropriate legal action, what the legal options entail, how to gather evidence, or even whether it is advisable to press charges.

What I am suggesting is that the victim assistance programs found within the criminal justice system be adopted, or at least facilitated, by the SBA. This does not require a major revision of the criminal code. Rather, SBA could work with criminal justice personnel to smooth the way for small businesses and, at a minimum, provide these businesses with information about their legal options.

Third, in my consulting work, I sometimes recommend that management require a computer security impact statement whenever there is a major computer purchase or enhancement. Similar to an environmental impact statement, these serve as required reviews of the security implications of computer changes.

Consideration might be given to having SBA or other Government agencies form evaluations of security implications of generic types of computer systems, and that these could be made available to small businesses.

Last, I have some comments concerning research needs. It is ironic to end my testimony by indicating that many of the most basic facts about computer crime are not known, and while the enormity of the problem for small businesses can clearly be estimated by experts, the necessary statistics are just not available.

If there is one study that should be undertaken by the SBA or other agencies, it should be a victimization study. There is a wealth of information on how to best mount such a study. Criminologists have developed sophisticated surveys which have provided information on the extent of such victimization, the reasons why or how crimes occur, who the offenders were, and possibly even more highly important information on what some individuals or businesses have done to avoid becoming a victim.

The Census Bureau has undertaken victimization studies on a national basis for a number of years using face-to-face as well as telephone survey methods. Unfortunately, they do not gather the type of information that you are seeking.

The type of survey which SBA might most readily consider—a mail survey sent to a sample of small business owners or manag-

ers—just will not be sufficient to determine the information being sought.

I would suggest that coordination might be sought with the Census Bureau, the Bureau of Justice Statistics, or with experts to establish a survey approach that is cost effective and sophisticated enough in design to lead to the required results.

[The prepared statement of Dr. Sherizen follows:]

DATA SECURITY SYSTEMS, INC.
COMPUTER SECURITY CONSULTANTS 5 Keane Terrace, Natick, MA 01760 (617) 653-7101

PREPARED STATEMENT OF DR. SANFORD SHERIZEN, PRESIDENT, DATA SECURITY SYSTEMS, INC., 5 KEANE TERRACE, NATICK, MASSACHUSETTS AND COLLEGE OF CRIMINAL JUSTICE, NORTHEASTERN UNIVERSITY, BOSTON, MASSACHUSETTS

PRESENTED TO THE SMALL BUSINESS COMMITTEE OF THE U.S. SENATE REGARDING HEARINGS ON S. 1920, THE SMALL BUSINESS COMPUTER CRIME PREVENTION ACT

MARCH 7, 1984

Mr. Chairman and Members of the Committee:

My name is Sanford Sherizen and I am honored to appear before this Committee to discuss computer crime prevention for small businesses. For background purposes, I am one of the few trained criminologists in the U.S. actively working as a computer security consultant. In addition to founding my own computer security consulting firm in Natick, Massachusetts, I teach courses in computer security, white collar crime, and private security in the College of Criminal Justic of Northeastern University. Utilizing my background of over a decade of university teaching and research on the sociological and criminological problems of crime control strategies and crime prevention techniques, I provide consulting services to businesses, government agencies, and institutions.

My consulting is oriented toward computer crime prevention, providing executives with sophisticated evaluations, organizational assessments, implementation strategies, and management seminars on cost-effective security options. At

present, I am completing a book under contract with the American Management Associations with a tentative title, Computer Security Management for the Non-Technical Executive. This book, as well as the emphasis of my consulting, stresses the following four major points, which are applicable to large or small businesses as well as government:

1. Computer security is no longer an optional decision but may be fundamental to the survival of a business.
2. The core issues of computer security can and must be understood by non-technical managers.
3. The essence of computer security lies with management controls, reviews, and policies developed with the active support and involvement of top management.
4. There are a variety of management questions that can be raised with technical staffs in order to evaluate the adequacy of computer protections in a business.

These are what I call the fundamental aspects of the new security rules for the computer age.

Today's topic is the protection of small businesses from computer crime. This is an important topic, for I suspect that computer crime is leading to two basic classes of business in our society--large corporations that have, or will have, a number of security protections and a majority of small businesses that will find themselves virtually unprotected. Larger businesses will find the money and staff necessary to protect their resources

while small businesses will not even be in position to know where to obtain such protections. Large corporations may well continue to be the major targets for much of computer crime since that is where the money is to be found. Smaller businesses, however, will become the easier targets and, since they have less ability to absorb losses, they will likely be the larger victims of computer crime. There is a parallel to street crime where greater police protection in one area often leads to a spillover or displacement of crime to other areas. Since today's computer criminal has traded in the tommy gun for the terminal, it is predictable that computer crime will increasingly be displaced onto small businesses. With an unknown but significant percentage of business failures already attributable to crime, one can conclude that the rate of small business bankruptcies may be increased by computer crime problems.

My own small business, Data Security Systems, Inc., was established out of an awareness that there are a number of areas of our society requiring crime control and prevention measures. While certain types of crimes are more difficult to prevent, I have felt that computer crimes are, to a large degree, preventable. Prevention, however, is restricted by many sociological and organizational factors which limit the ability of a business to accept preventive measures. My firm was formed in order to provide an interdisciplinary approach to the problem of computer crime by combining the insights into human behavior that can only come from the social sciences with technical knowledge of computers and technological developments. As

computers have taken on more of an end user driven emphasis and as various computer and communications technologies have merged, computer security has become an issue that nobody "owns". This often critical responsibility has not received sufficient attention in the average business and non-technical managers are increasingly being forced to face the problem, even if they do not have sufficient knowledge or experience.

Since other witnesses have provided testimony about aspects of computer crime, I would like to just make some summary comments as an introduction to discussing the unique problems of small businesses. Computer crimes can be committed in fractions of a second with readily available equipment, sometimes including the equipment that is provided to employees for their authorized work functions. If done with skill, these manipulations can occur with minimal risk for the perpetrator, since audit trails may not be produced or may be deleted, leaving little for auditors or investigators to follow. To compound these computer problems, there is relatively little law directly applicable to computer crime and little interest on the part of law enforcement officials to take on these cases, even in the rare event that a business decides to press charges. Computer crimes require minimal risk for major gain. They are often found out solely by accident and information on how to commit these acts is easily found. Those who commit these acts may even rationalize their acts as non-crimes, since there is no bloodletting and all that they are doing is punching some computer keys or changing some code. Talk about incentives for crime!!

There are a number of computer security protections that have been developed over the years. These are physical security, procedural or managerial controls, and technical security, which is composed of hardware, software, and communication protections over systems and data. Too few of these are known to large corporations and probably are even lesser known to small businesses. Many business persons feel virtually unprotected but don't know where to turn for advice or security products.

Small businesses have become a major market for computer vendors. Due to limits on available markets for mainframes and mini computers and the dramatic developments of micro computers, small businesses are being inundated with computer advertisements and offers. In a recent issue of Computerworld, a Time study was reported, indicating that computer usage by small businesses is projected to jump by 47% in the year between mid-1983 and mid-1984, with the majority of sales made to companies with less than 20 employees. Slightly over 16% or one half million small businesses are using computers today and this is a 25% increase over a three year period.

In many, if not the majority of these small businesses with computers, there are next to no protections in place. Small business owners tend to purchase computers by word of mouth advertising or to rely upon technical staff or computer sales representatives. In purchasing computers today, one is led to believe that it is possible to buy a complete computer for a certain price. The user friendly emphasis, the a la carte mode

of purchase, and the lack of security knowledge effectively work against the purchase of computer security provisions. Most security requires additional costs in terms of equipment, processing time, managerial overviews, and/or technical decisions--all of which tend to be in short supply in these businesses. If a business was going to purchase a business car, they could correctly assume that the car would come with brakes, windshield wipers, and door locks. There would be no need to ask if these were included at no extra charge. Yet, this assumption about the automatic inclusion of computer protections would be incorrect.

Microcomputers tend to lead to less segregation of duties and reduced controls over processing, violating some very basic management controls over fraud and other crimes. The micro user gains enormous abilities to process data and, under certain circumstances, to manipulate data in unauthorized ways. The most sensitive information of a business may be put into computers in an attempt to maximize computer capabilities. By centralizing their sensitive resources, these businesses run the chance of concentrating their risks and maximizing the dangers to their financial health, unless adequate security is put into place. The microcomputer revolution has struck and few business executives are aware of how significant it has challenged many of their traditional managerial controls and operating procedures.

Even those small businesses that have not adopted their own computers but rely upon service bureaus to process their work may

have security difficulties. Given the lack of comprehension I have discussed, owners and managers of small businesses may not be able to ask the appropriate questions concerning security or to make appropriate requests for protections. Often, service bureaus have protections in use and are quite willing to provide extra services, at times for a minimal fee. Yet, in one case I was involved with, a service bureau stated that some of their users demanded and received security services such as access controls mechanisms while other users seldom were interested in these packages or services, even when the bureau notified them of low cost availability.

With this information as background, I applaud this Committee for what it seeks to accomplish. Rather than simply wait for the crisis to hit small businesses, you have provided a means to offer assistance. In general, I support the Act and the Task Force approach. I do, however, have several suggestions and comments that I will pass on for your consideration.

Computer security consultants will not be able to solve the computer crime problem for small businesses since the realities are that larger corporations are our more natural market. They are more able to afford and support our efforts, while smaller businesses have more difficulty in deciding that security is a cost-effective decision. Government has an important role to play in assisting small businesses, particularly through the established roles and services of the Small Business Administration. The nature of the computer security problem for

small businesses, however, requires quite active assistance on the part of SBA to inform businesses about the availability of computer security approaches and products. More specifically, I have the following recommendations:

1. A very beneficial action would be the establishment of a hotline for handling inquiries from small businesses concerning computer security products, approaches, materials, and consultants. This could be part of the resource center concept being discussed. Among the resources that could be made available would be computer security information from other federal and state agencies such as the Evaluated Security Products List of DOD, risk analysis manuals written for various agencies, informational materials about computer crime from the National Criminal Justice Reference Service, and policy statements from lead agencies, and materials from the private sector.

2. Businesses generally require assistance with the criminal justice system. I envision a small business that wants to know what to do when it finds out that it has been victimized. It is difficult enough to detect computer crime but there are even more difficulties when one does not know where to go for advice as to appropriate legal actions, what the legal options entail, how to gather evidence, or even whether it is advisable to press charge. I sympathize with a business that is fearful of publicity and worried that the end result of pressing charges may be great time and effort, possibly worse treatment than that afforded the offender, and even the possibility of the loss of

proprietary information during hearings. That does not even take into consideration the growing movement of prosecutors to use cost-effectiveness determination in deciding on what cases to accept. Few small business cases would fit the priorities which emphasize large amount of loss, deterrence objectives, and seriousness of the crime. What I am suggesting is that the victim assistance programs found within the criminal justice system be adopted by the SBA. This does not require a major revision of the criminal code. Rather, SBA could work with criminal justice personnel to smooth the way for small businesses and, at a minimum, to provide these businesses with information about their legal options.

3. I would also suggest that small businesses could use insurance protection. By providing incentives to insurers to cover small businesses, or by providing coverage similar to the crime insurance program developed by the federal government several years ago, basic computer security protection would be supplemented. Possibly, incentives could be provided to the insurance companies so that they could pass on information to small businesses about computer security approaches which, if installed, would result in lowered premiums.

4. In my consulting work, I sometimes recommend that management require a computer security impact statement whenever there is a major computer purchase or enhancement. Similar to an environmental impact statement, these serve as required reviews of the security implications of computer changes. Consideration might be given to having evaluations be performed of the security

implications of generic types of computer systems be performed and baseline measures be developed and made available to small businesses.

9. Lastly, I have some comments regarding research needs. It is ironic to end my testimony by indicating that many of the most basic facts about computer crime are not known and, while the enormity of the problem for small businesses can clearly be estimated by experts, the necessary statistics are not available. If there is one study that should be undertaken by the SBA, it should be a victimization study. There is a wealth of information on how to best mount such a study. Criminologists have developed sophisticated surveys which have provided information on the extent of such victimization, the reasons why or how the crime occurred, who the offenders were, and even highly important information on what some individuals or organizations have done to avoid becoming a victim. The Census Bureau has undertaken victimization studies on a national basis for a number of years, using face-to-face as well as telephone survey methods. Unfortunately, they do not gather the information we seek. The type of survey which SBA might most easily consider, a mail survey sent to a sample of small business owners or managers, just will not be sufficient to determine the information being sought. I would suggest that coordination might be sought with the Census Bureau, the Bureau of Justice Statistics, or with experts to establish a survey approach that is cost-effective and sophisticated enough in design to lead to required results. In that regard, I have attached an article which contains some of my thoughts on the contributions of victimization studies.

Once again, I would like to thank you for this opportunity to express my ideas to this Committee. I stand ready to answer any questions you may have or to provide any assistance which you may need.

Senator TSONGAS. Let me ask you one question. I would assume there are instances where a business that has been victimized would choose not to let that be known.

Dr. SHERIZEN. Indeed.

Senator TSONGAS. What would the reasons be, other than those that are obvious, and what percentage do you think we are talking about?

Dr. SHERIZEN. Well, the obvious ones I will not cover. Let me talk about some unobvious ones. There have been instances where businesses have gone and pressed charges. As a result of hearings, proprietary information has been revealed, to their chagrin. Therefore, a number of businesses are very gunshy about that.

In addition, the issue of not knowing where to turn and what to do is a major factor. The justice system has a reputation as being more concerned with offenders or perpetrators than victims or witnesses and that is sometimes correct. In many cases, persons do not know whom to turn to for advice.

I should also point out that the criminal justice system does not know how to respond very well to the problem. I have heard a law enforcement person in the Route 495 high technology area of Boston say: "I hope if there is ever a computer crime in any of the high-tech firms here, please, let somebody steal a computer, because I will know what to do. If they steal software, I'm in trouble."

It is that kind of, shall we say, lack of training and information that causes businesses to try to absorb their loss rather than to move to press charges.

Senator TSONGAS. I find that to be a very sophisticated observation. I concede that people would not have known the difference between the software and the computers.

Dr. SHERIZEN. So they may have some training and some insight, yes. But the deeper problem is how to respond to the complex types of crimes that have been surfacing.

Finally, I have no percentages on how many cases are reported by businesses. I would expect this to be much less than reporting figures for all other types of crimes which, in some instances, maybe as low as 10-20 percent of all crimes which occur.

[Subsequent information was received and follows:]

United States Senate
COMMITTEE ON SMALL BUSINESS
WASHINGTON, D.C. 20510

March 12, 1984

Dr. Sanford Sherizen, Ph.D.
President
Data Security Systems, Inc.
5 Keane Terrace
Natick, Massachusetts 01760

Dear Dr. Sherizen:

We would like to extend to you our thanks for testifying at the March 7, 1984 hearing on S. 1920, the Small Business Computer Crime Prevention Act. Your testimony will be very helpful to the Members of the Senate Small Business Committee.

Due to the time constraints of the hearing, there were some questions we did not get a chance to ask you. In order to make the testimony complete, the Committee would greatly appreciate it if you would consider these issues now and provide written responses for inclusion in the permanent hearing record.

1). Would you agree that the most effective role the Federal Government can play in assisting small businesses with computer security controls is to support and sponsor educational efforts in cooperation with the private sector?

2). S. 1920 states that it will be the function of the Task Force to "define the nature and scope of computer crimes committed against small business concerns." Can the scope of computer crimes committed against small businesses be defined with any certainty? Even if it can be, is such a definition of scope necessary to facilitate management assistance by the SBA to small businesses concerning computer security?

3). Is there any way of empirically determining the effectiveness of state legislation as opposed to security equipment in preventing computer crimes against small business concerns?

4). Is it necessary for the SBA to create a resource center as called for by S. 1920 in order to meet the information and assistance needs of small businesses concerning computer security?

5). There is general agreement about the need to educate the small business community about computer security controls. The SBA is ready to proceed immediately to provide information to small businesses on computer security. Do you support the SBA approach to proceed without the task force and 18-month study period?

6). Can you give us any specific instances, based upon your experience as consultants, where a lack of computer security proved damaging to small businesses?

Please send your responses to Mike Morris, Counsel of the Small Business Committee staff at 428A Russell Senate Office Building, Washington, D.C. 20510. Should you have any questions about the hearing or this request, please feel free to call Mr. Morris at 224-2016, or Alan Chvotkin, Minority Chief Counsel, at 224-8497.

Thank you in advance for your cooperation and prompt attention to this matter. Again, your participation in this hearing was greatly appreciated.

Sincerely,

PAUL TSONGAS
United States Senator

LOWELL WEICKER, Jr.
Chairman
Senate Committee on
Small Business

DATA SECURITY SYSTEMS, INC.
COMPUTER SECURITY CONSULTANTS 5 Keane Terrace, Natick, MA 01760 (617) 653-7101

April 16, 1984

Mike Morris
Counsel
Small Business Committee
428A Russell Office Building
Washington, D.C. 20510

Dear Mike,

Once again, my apologies for the delay in responding to the letter. Six specific questions were raised and I will respond to them in their original order.

1) I would see this educational effort as just one of the roles that the Federal Government can play. For reasons stated in the hearings, the private sector may not be able or willing to work with government agencies in providing assistance to small businesses. The Federal Government need not be limited to cooperative ventures with the private sector. It can play unique roles in formulating security approaches, such as those existing in the Institute for Computer Sciences and Technology of the National Bureau of Standards.

2) I doubt that anyone could establish a count of computer crimes against small businesses with any total accuracy. Other than a sophisticated victimization survey of the type discussed in my testimony, the collection of actual statistics would be difficult and filled with methodological difficulties. However, there are generic computer crime problems and conditions which are possible to ascertain, based upon the types of computers small businesses adopt, general threats and vulnerabilities in computer systems, and the management patterns in small businesses. Such a generic approach would provide a top-down view of the nature and scope of computer crimes committed against small business concerns.

My concern with establishing programs without establishing a basic definition of the computer security problem is that the wrong problem may be defined. The SBA, for example, may define the computer security problem within its own set of problem understandings and fit computer security management assistance for small businesses within current program models. From my perspective, this will be inadequate to meet the serious needs of small businesses. The question then is not so much whether the scope of the problem can be fully defined but whether there can be some assurance that the SBA will meet the challenge which computer security experts have indicated are the major aspects of the problem.

3) I recently provided testimony before the Governor's Anti-Crime Council on some proposed computer crime legislation in Massachusetts. I was asked to review state legislation around the country. I reported that there seems to be a mixture of legislative approaches, with little consistency in terms of definitions of computer crime, appropriate punishments, or types of offenders. The trend does seem to be to use as a model some of the proposed federal legislation. From initial reports, there does not seem to be any rush of cases. The Bureau of Justice Statistics has funded a study of state efforts and a report should be forthcoming by Donn Parker during the summer.

The question you raise could be done empirically, examining how potential computer criminals would perceive the deterrence of law versus security equipment. My criminological sense is that we are talking about different types of effectiveness, one specific to legislation and another to equipment. The literature on deterrence suggests that the swiftness of punishment is more relevant to whether someone will commit a crime than is the possible harshness of a future punishment. The visibility of a preventive measure is also more important to a criminal than would be some symbol such as a law. I would suspect that legislation may serve to move the government into the technological age by providing new definitions and responses to the problem of computer crime. Security measures, on the other hand, may have a more direct impact on criminals and provide small business owners with a means of responding directly to their problem of crime. Ideally, the best possible mix of preventions would be legislation (both on the state and federal level), the application of security techniques, and management supported detection and control strategies.

4) The resource center may be one of the strongest features of S. 1920. While there are private computer security resource options presently available, small businesses continue to find it difficult to locate those resources, to pay sufficient funds for the services, and to know how to use computer security protections. The SBA, with its unique relationship with small businesses, can use their communication lines to inform these businesses of the resource center material, particularly if the resources include many of the excellent material from the government, such as NBS and other federal agencies.

5) I am pleased that the SBA is now willing to act but I would need to know what its plans were before I would be able to project how successful it might be without the task force and the 18-month study period. The important issue is how will SBA efforts be reviewed. SBA has appeared to be unwilling to move forthrightly on the computer security effort. While this may be an erroneous impression, the task force composition stated in S. 1920 may not provide enough incentive for an SBA effort, even with the task force and the 18-month study. Therefore, I am more inclined to suggest a review or oversight panel to analyze and direct SBA efforts.

6) I am presently involved with a project in cooperation with the National Center for Computer Crime Data in Los Angeles and International Networks of MIT. We are reviewing the best measures of computer crime protections, penetrations, and opportunities for crime. While the information has not all been collected, my impression is that we will uncover some cases directed against small businesses. We will be interviewing district attorneys from around the country and this might provide some information as well. Other than that, I do suggest that some brief examples can be found in a recent book by Harold Highland, Protecting Your Micrcomputer System (Wiley, 1984).

Once again, I thank you for the opportunity to provide the Committee with my views of the serious problem of computer crime. If I can be of further assistance, feel free to contact me.

Sincerely,

Sanford Sherizen, Ph. D.
President

Senator TSONGAS. Mr. Schuldenfrei.

STATEMENT OF ROBERT SCHULDENFREI, PRESIDENT, S.I., INC., ON BEHALF OF THE SMALLER BUSINESS ASSOCIATION OF NEW ENGLAND, INC.

Mr. SCHULDENFREI. Thank you very much, Mr. Chairman, for the opportunity to address you today.

My name is Robert Schuldenfrei, and I am president of S.I., Inc., a small management consulting company. Our interests are the processing of information from data that small organizations typically have on hand.

I work day in and day out with modest-size organizations on the order of sales of, let's say, $1 million to $5 million in sales.

Senator TSONGAS. Can you give me your background?

Mr. SCHULDENFREI. Yes; I have a master's of business administration from the Amos Tuck School at Dartmouth College and an economics degree from Syracuse University. I have worked in small consulting companies for the last 15 years. I started S.I., Inc., 2½ years ago.

I would like to begin my testimony today by saying that I am not going to attempt to read in all of the material that is in my statement, just highlight it for you.

Senator TSONGAS. That statement, of course, will appear in the record as if you had read it.

Mr. SCHULDENFREI. Yes, thank you very much.

The definition of computer crime is not dependent on the scale of enterprise, whether small business or large business. You can break computer crime down into maybe three categories—arbitrary on my part—crimes against property, theft of intellectual value, and the use of the computer as a criminal tool.

I cannot really say that computer crime hurts small business more than big business. Some years ago, I was involved in a case for the Chemical Bank of New York, which is a large organization, and I think that they were probably more vulnerable than all the small businesses that I have dealt with over the last couple of years. They had all of their computers, super computers of the

1976–77 vintage, two IBM 3033's, an IBM 168 and 158, all interconnected to 176 disk drives on one floor in a Manhattan office tower. All the bank's information was in one place. In a very real sense the computer is the bank. Chemical Bank was very vulnerable to sabotage or to a disgruntled employee. If that computer system went down for any length of time, there was some question of whether the bank would have survived, even though that had a lot of backup. Just to assemble that kind of computer equipment is difficult.

The key characteristic of whether an organization is vulnerable is how dependent is it on its information base. I would like to talk to you about a typical small business that I consult with in Massachusetts, because it is very, very similar to thousands of organizations across the country.

They have a small Wang computer, a Wang 2200, with four display stations, two 20-million-byte disk files, some printers, that they use in the day-to-day business of billing their customers.

They have a billing system that was written by a third party software house, but no one in the firm has any idea about how it works; they have no knowledge of computers other than how to turn it on and answer questions.

No reports are generated for management. I mean, the bills go out, and there is an aging report that gets checked in when the cash comes in, and nobody knows what the current status is. There is no written policy or oral policy on who can use the system, and when a key employee is sick, they try to hustle somebody else on the machine so that they can continue to bill their customers.

Workers are paid minimum wage or just barely above it. There are no statistics, audit trails, or operators' journals, and probably the worst problem is that all of the computer files, the backups, and even the paper records of the firm, are kept in one room. They are extremely vulnerable.

Now, they have not been hit. They have not had any problems. My involvement with that company was not for computer security. In fact, they wouldn't pay for that. They wouldn't buy your services, Mr. Sherizan, for instance. I am in there to get more information out of the billing system and to make some changes in the billing system.

They do not recognize the need for any more security, and I doubt very seriously whether they would pay for it.

What technology is available to firms like this to protect them against the problems that we have heard about this morning?

First and foremost is probably education. It is cheap, and I think it is a very necessary first step. The easiest way to get that kind of education is to have anybody who works for you, like programmers or outside software houses, explain all the elements of the computer system to you. The management, in this case the president of the company should go through each operational job and become familiar with its function; learn how computers work; learn what kinds of disasters can plague a computer installation and what you can do about it.

Next up from education is probably some simple security measures, protecting the system from those things that are most vulnerable to loss—passwords. Most computer programs and operating

systems allow for these things, and they should be changed regularly. Keep cross training of employees to the minimum necessary for a smooth operation, so that you fragment the job and no one person becomes a key employee.

Remember in all of this that the only security, really, is physical security. Lock up the files. Don't send data home, like they do, with employees to get it off the premises, and don't keep communications lines open when it is not necessary; restrict their usage.

Encryption is a technique that may offer some of the bigger companies an answer, but my feeling is that the protection there is overstated. While programs can be scrambled—and I have some experience with some scrambled programs—they can be unscrambled by experts. Data can be coded, yes, but it can be broken by experts.

Often it is only coded in the middle of transmissions. On both ends, the computer end and on the user end, it is encoded again so it can be used, and therefore you get a false feeling of security with an encryption system.

Keep personnel management high in your mind. Hire with care. Supervise all operations, become involved. Set up a policy, a written policy, on what employees can do and who can do it.

Finally, insure with insurance that which you cannot afford to lose.

The last thing that a small business can and ought to do is formalize the audit process. If possible, make this an external audit by teams who are trained in this area. Have that reported to management, and make it widely known within your organization that this audit is going on and that it is being reported to management.

Establish controls over your operations to include daily logs, prenumbered forms, control totals, validation of users, and sample these frequently. These are all things that small businesses can do if they are told to do it, and none of them costs a lot of money.

What can I say about the bill that you are considering today? It is an excellent first step. I think it will be difficult to track down the scope of computer crime, although I think it is possible. There are data bases around that you probably can tap into. The Government probably is the only appropriate entity to use these data bases.

I would expect, however, that when your team is finished, you would have widespread dissemination of its results. The resource center is probably a good idea, but only if it can get this out to the people who need it, because they are not going to come to you. They are not going to come to Washington, D.C. They are not even going to come to Boston. So you have got to get this in their hands, and therefore if you can publish inexpensive media like pamphlets and books and get out to the small businessmen to make them aware of the problem, I think they can then make intelligent decisions on the area of computer crime.

Thank you very much for your time.

[The prepared statement of Mr. Schuldenfrei follows:]

STATEMENT BY:
Robert Schuldenfrei, President
S. I. Inc.
235 Bear Hill Road
Waltham, MA 02154
BEFORE SENATE SMALL BUSINESS COMMITTEE
March 7, 1984

Introduction:

Thank you for this opportunity to testify on behalf of small business in the field of computer crime. My name is Robert Schuldenfrei. For the past 15 years I have worked as a consultant to managements, much of that work with small business. The area of my professional competence is in the application of computer technology to management. Over this time I have been employed by small organizations, two of which I helped found. For a period of five years I taught data processing to business students at the University of Rhode Island.

Computer crime as it relates to small business:

There is very little difference in the nature of computer crime with respect to the size of an organization. As a question of definition, computer crime is the same whether it is committed against a one million dollar firm or a five billion dollar company.

For the purposes of definition computer crime can be broken down into three categories. The first is property crime against the machine. This definition is like any crime against a valuable asset of the firm. Examples of this are sabotage, arson, vandalism, and theft. The computer is no more vulnerable than a truck, a warehouse, or a show room full of inventory.

The second category of computer crime is the theft of the intellectual value of the computer. In this sense the computer is different from most assets of the firm. Here we can find theft of service and theft of information. Theft of service is the unauthorized use of the machine. It can range from the trivial, like playing computer games on the firm's machine to the selling of computer time for personal gain. Much of the publicized unauthorized entry of remote computer services falls under this category. Theft of information is the illegal use of data. Much of computer espionage falls into this area. Software piracy is also in this category.

The final category of computer crime is the use of the machine as a criminal tool. Here the machine is used by

the criminal as a means to an illegal end. The fraud and embezzlement areas are in this category. The computer is not really the target of the crime in this category, but like a cancer, the firm's own mechanism is subverted for the criminal's use. This category can be most damaging, and has been the most popular route for computer crime. The common use here is to create financial instruments to defraud the firm. Bad checks, credit memos, merchandise shipments, and bogus accounts are the methods by which the crime can be accomplished.

Given the above definitions of computer crime, it can not be stated that these activities hurt a small firm greater than a large one. Scale of enterprise is not the relevant factor, dependence on information technology is. Some years ago I was consulting for Chemical Bank of New York, a major organization. At the time they had four super-computers in one room in a Manhatten office building. Since information processing is the work of a bank, it could be said in a real sense that the computer was the bank. One act of sabotage could have ruined the bank. The back up plan could not have possibly been put into action in time to save that institution. In fact, it never was tested. Unfortunately, there are many small firms in the same position as the bank. They are information processors. The threat of complete ruin is as real to them as it was to the bank. On the other hand, other firms are not very dependent on their business systems. For that class of company there is little risk from computer crime.

A small Massachusetts firm, for example, is very typical of the thousands of small businesses. They are a distributor of durable medical equipment with sales of about one million dollars per year. While they have not had any computer crime, the potential exists there. Over the last four years they have been growing due, in part, to a computer billing system. The paper work necessary to run a business which depends heavily on Medicare payments is difficult to perform manually. In order to overcome this problem, the firm bought a Wang 2200 computer system. This mini-computer system is made up of a processor, 4 terminals, 2 twenty million character disk drives, and a high speed printer. The custom software was written by a software house, that has since gone bankrupt.

No one in the firm knows anything about computers, either hardware or programming. When I came in to make some changes in the programs I found that the software house had scrambled the programs, which were the legal property of my client. No one in the company had any idea

how the programs worked. Fortunately, Wang was able to unscramble the programs. Keep this in mind when you consider encryption as a means of security. I was able to do my work, but once again an outsider was performing the sensitive work with no understanding on the part of the client.

The situation in this firm is as follows. While operational documents are prepared, no status reports are generated for management, the president. There is no policy, written or oral, stating who can use the computer system. The workers, who are all earning about minimum wage, are the only operators of the system. There are very few audit trails through the system. I wrote a daily activity report so that I could track activity by operator, management could not be bothered. There are no passwords, operator journals, or system statistics kept. The instructions on running the machine are pinned to the wall for all to see. All computer files, backup files, and paper records of the firm are kept in the same room.

I can not say that there will be trouble for this firm, but if there ever was a proto-typical case, this is it. It is a disaster waiting to happen.

Technology is available to the small business:

Although it may seem strange in a highly technical field like computers, the single most important thing available to firms both large and small is a low tech solution, education. It is reasonably low cost, and most effective. For the large firm this probable means the retention of experts on their staff. For the small firm, this means the training of employees to become intelligent consumers of computing power.

Because business owners do not recognize the threat of computer crime, this education often is overlooked. The demands on the time of the managers means that this area is not given the attention that it should have. There are four things which should be done. First, have the programmers or the authors of software explain all of the elements of the programs, files, and procedures. This should be done in formal sessions with management. The managers, or owners, should look at this material, even if they don't totally understand it. It is important for a number of reasons, none the least of which is it sends a message that management is concerned. In addition, this material is not so hard that managers can not understand

it. If they do, it will be a good check on the accuracy of the material.

The second task is the familiarization with every operation of the system. The manager must know each job and its function. If this means sitting down and processing a few transactions, so be it. It is truly amazing what can be learned about how the work is done, by doing the work.

The third element of this management education is to learn how computers work. One should first learn the proper function of a computer system. Then he should learn how these systems can be used for fraud. I would submit that the way to learn how a computer works is to learn how to program one. A cheap way to do that is to buy a home computer, and teach yourself to program.

The last part of this section is to learn what natural disasters can plague a computer installation. Once this has been mastered, a plan to recover from both natural and criminal disaster can be formulated.

From the above discussion it can been noted that the smaller business can reap many benefits from just education. In the next section you should note that many of the technical approaches to computer security make use of existing features of most computer systems. The following concepts are all simple approaches that make good common sense for business of all sizes. The first is the evaluation of the costs and benefits of protection. The rule is to protect those parts of the system in proportion to their loss value. Thus, the disk pack which has the accounts receivable file on it should receive more attention from management than a pack containing test data. Further, programs which don't change from day to day, need only be backed up when actually changed. Working files need daily backup.

Most programs which deal with sensitive data have password protection. You would be well advised to issue passwords which are random collection of numbers and letters than letting an operator use the phone number. The passwords should be changed often. This is particularly true if the system allows remote access. You would be amazed how many people use their birthday, children's names, or their phone number for a password. If you found a bank automated teller card, you might well be able to use it successfully if you merely looked up the phone number of the owner in the local phone book.

Keep cross training of employees to a minimum. Each person should know only what is necessary to do his job, with reasonable backup of key operators. This is particularly true with programmers. Let them develop and maintain the system with test data. You do not need to give them operational data to test. In the event of a problem, it is valuable to let them try to reconstruct the problem with the test data. It is the computer expert who represents the greatest threat to the firm, because he has the knowledge to create the biggest loss.

It can not be stressed enough that the only security is physical security. Codes and passwords can be broken. Therefore, keep all removable media locked up when not in use. Don't send data home with employees. Have an off premises site for backup. Test your recovery plan periodically. Keep your communications lines open only when necessary and restrict their usage. Use a call back system where practical.

Encryption can be an expensive answer to security. This is available to large firms. It probable causes a false sense of security, as fraudulent information gets encoded with the valid data. Remember the source code I had reconstructed. This was harmless, as my client owned the program, but it shows just how little trust you can place in codes. In addition to programs, data can be coded and communications line scrambled end to end. These are tools that may not be with in the means of a small business, and are not as effective as vendors would have you believe.

Personnel management is as important to small business as education. On a per person basis, this will cost a small firm no more than a large one. Hire with care. Do not expect poorly paid, unmotivated people to have the firm's interest at heart. Supervise all operations and development with attention to detail. Take the time to understand what each employee does. Have a written policy on the physical and intellectual property of the firm. Make sure that each employee understands that policy. Review that policy often.

There is insurance available to protect the firm against the kind of loss described above. It is a good final step to insure against what you can not afford to loose. If you think about why you would insure a building or a person, you will understand why you should consider insuring the important information of the firm.

33-723 O - 84 - 6

Once all of the measures have been taken it will be time to set up an audit and reporting system to make sure that your plans are being followed. While it is easier for a large firm to do this, it is not beyond the capability of a small one to set up a format audit system. You should design this in from the beginning of the system's life. When selecting packaged software, the audit should be one of the considerations.

An external team should perform the audit if possible. The results must be reported to management in terms it understands. Design specifications should be established and reviewed. Operational activities should likewise be controlled. This is include things like daily activity logs, pre-numbered forms, control totals, operations sampled at random, and a validation program for all users.

Comment on Bill S. 1920:

The bill before you is an excellent first step. It makes smaller business persons aware of a problem of which I am sure they are not cognizant. If the task force is given the appropriate tools, I am sure that they can accomplish the objectives set out by the bill. This leads to three comments.

First, section (C)(i) will be difficult to track down. To do a good job here, the task force would need access to legal databases. Some sampling of business at random will be necessary to validate the reported instances of computer crime. This means funds and a method of doing computer searches.

Second, once the work was done I would expect that the widest means of publishing the work would be desirable. It is folly to think that owners of small business would come to the SBA resource center. Low cost documents, distributed through the mail and/or in GSA bookstores, is one approach.

Third, it would be appropriate for SBA to sponsor seminars on computer security. They would be performed by small business for small business. In that way the costs could kept low, while at the same time they could have the widest reach.

RESUME

Robert Schuldenfrei
32 Ridley Road
Dedham, MA 02026
(617) 329-5807

AREAS OF PROFESSIONAL COMPETENCE

Is a general manager with proven accomplishments in administration, marketing, production, and finance. Has analytical skills in logistics, data processing, mathematical modelling, strategic planning, and materials management. Possesses the knowledge to analyze business conditions, forge creative solutions, and organize people to obtain the desired result.

INDUSTRIAL EXPERIENCE

1981-Present. President, and founder of S. I. Inc., a management consulting firm. Performed marketing research for a major producer of industrial chemicals from agricultural raw materials. Developed a logistical simulation for a restaurant chain. Directed the development of a corporate distribution strategy for a manufacturer of a consumer durable product. Developed and implemented a generalized intracompany reporting system for a large industrial client.

1976-1981. Vice President, and co-founder of Shycon Associates Inc. Directed the consulting operations. Was responsible for the design, staffing, and execution of most of the work in the company including the construction of simulation models for the evaluation of corporate distribution strategies. Lead teams of consultants developing and implementing a production/inventory control system.

1972-1976. Lecturer, University of Rhode Island. Developed management science curriculum at both the graduate and undergraduate level. Courses taught were: introduction to business data processing, advanced data processing, database management, quantitative methods, and production. During this period there were numerous consulting relationships with both large and small firms. Typical of this work were material flow studies for New England manufacturers.

1970-1972. Senior consultant, Applied Decision Systems Inc. Produced an econometric model of a region of the United States for the Department of Commerce. The computer model was used in the industrial attraction process. Built simulation models of plant operations. Managed a project to automate the estate planning process for an insurance professional.

1968-1970. Officer, United States Army. Lectured in data processing at the U S Transportation School. Led a five man team in the development of an instructional simulation of theater logistics. Analyzed the data processing and instructional needs of the school. Prepared and delivered speeches on the education of officer students in data processing.

1967-1968. Teaching assistant, Dartmouth College. Taught data processing at the graduate level. Designed and programmed one of the earliest management information languages. That system and the company which owns it was recently sold to A C Nielsen Co. for a reported four million dollars. Solved flow of material problems for a major furniture manufacturer.

ARTICLES:

Modeling for the Non-Modeling Distribution Executive. Proceedings of the annual meeting of the National Council of Physical Distribution Management, October, 1981.

Inbound Collection of Goods: The Reverse Distribution Problem. Interfaces Vol. 10 Number 4, August, 1980.

Fill in the Blanks. 80 Microcomputing Number 25, January, 1982.

Cost-effective Planning keeps Signode Competitive. (contributed to the article) Traffic Management Vol. 19 Number 5, May, 1980.

Interactive Model Building. Interfaces, August, 1975.

Management Science in a Period of Uncertainty. Interfaces, February, 1975.

User-oriented Computer Modeling Environments, a Precis in Management Science Vol. 17, Number 5, January, 1971.

EDUCATION

M.B.A. Dartmouth College, Amos Tuck School of Business Administration, June 1967. Major: Production

A.B. Syracuse University, June 1965. Major: Economics

Senator TSONGAS. You talked about that company that you were consulting with. If that company receives in the mail a pamphlet from SBA on computer crime, what happens to the pamphlet?

Mr. SCHULDENFREI. I think if it has impact, like "You, too, can be held up by a computer" or "Some people rob you with a six gun; others use a computer" it will get read.

I think there is a good chance, when the mail is read, if it relates to their problems. They are prone to spend money only if they see a good chance at results. For instance, the same company tried some communications between two of their stores. I won't say it is a lark, but they tried it for a period of time—they were willing to experiment with communications—and, interestingly, found that the communications did not meet their needs as effectively as centralizing the billing process. They took out the communications and brought it all in centrally.

So I think it is not unreasonable to expect that small business will try things, particularly if they see the benefits, and I think the problem, as was stated so eloquently earlier, is one of lack of knowledge of the problem.

Senator TSONGAS. Do you ever worry about the fact that you could provide all this knowledge to the disgruntled employee at the same time?

Mr. SCHULDENFREI. Yes, I do. But it is interesting, because very often I try to present some of my ideas to senior management of these smaller companies, and basically, they turn the question around and they point their finger and they say, "Bob, I hired you because you have the answers," which means, in a sense, I am giving up, abdicating my role as management. But the realism is that they feel very inadequate to do these kinds of things, and so therefore I feel that any education, even running the risk of telling people how to commit the crime, is probably better than none at all, because I think in telling people maybe how to commit the crime, you are also saying that this management is concerned, so if you are going to commit a crime, you had better be super slick about it and not try some of the easy ways like having the computer print you a payroll check. You are sending a message, if you will, that management is concerned.

[Subsequent information was received and follows:]

United States Senate
COMMITTEE ON SMALL BUSINESS
WASHINGTON, D.C. 20510

March 12, 1984

Mr. Robert Schuldenfrei
President
S. I., Inc.
235 Bear Hill Road
Waltham, Massachusetts 02154

Dear Mr. Schuldenfrei:

We would like to extend to you our thanks for testifying at the March 7, 1984 hearing on S. 1920, the Small Business Computer Crime Prevention Act. Your testimony will be very helpful to the Members of the Senate Small Business Committee.

Due to the time constraints of the hearing, there were some questions we did not get a chance to ask you. In order to make the testimony complete, the Committee would greatly appreciate it if you would consider these issues now and provide written responses for inclusion in the permanent hearing record.

1). Would you agree that the most effective role the Federal Government can play in assisting small businesses with computer security controls is to support and sponsor educational efforts in cooperation with the private sector?

2). S. 1920 states that it will be the function of the Task Force to "define the nature and scope of computer crimes committed against small business concerns." Can the scope of computer crimes committed against small businesses be defined with any certainty? Even if it can be, is such a definition of scope necessary to facilitate management assistance by the SBA to small businesses concerning computer security?

3). Is there any way of empirically determining the effectiveness of state legislation as opposed to security equipment in preventing computer crimes against small business concerns?

4). Is it necessary for the SBA to create a resource center as called for by S. 1920 in order to meet the information and assistance needs of small businesses concerning computer security?

5). There is general agreement about the need to educate the small business community about computer security controls. The SBA is ready to proceed immediately to provide information to small businesses on computer security. Do you support the SBA approach to proceed without the task force and 18-month study period?

6). Can you give us any specific instances, based upon your experience as consultants, where a lack of computer security proved damaging to small businesses?

Please send your responses to Mike Morris, Counsel of the Small Business Committee staff at 428A Russell Senate Office Building, Washington, D.C. 20510. Should you have any questions about the hearing or this request, please feel free to call Mr. Morris at 224-2016, or Alan Chvotkin, Minority Chief Counsel, at 224-8497.

Thank you in advance for your cooperation and prompt attention to this matter. Again, your participation in this hearing was greatly appreciated.

Sincerely,

PAUL TSONGAS
United States Senator

LOWELL WEICKER, Jr.
Chairman
Senate Committee on
Small Business

S.I. Inc.

235 Bear Hill Road Waltham, Massachusetts 02154 (617) 890-4230

April 13, 1984

Mr. Mike Morris
Counsel
Small Business Committee
428A Russell Senate Office Building
Washington, DC 20510

Dear Mr. Morris:

Thank you for the opportunity to respond to your questions concerning S. 1920, the Small Business Computer Crime Prevention Act. Most of my beliefs are contained in my written statement to the committee. Please find below the direct answers to the six questions which you posed to me in your letter of March 12, 1984.

I would, without reservation, agree that most effective role that the government could play is in the area of education. While there is technology to aid in the prevention of computer crime, the best line of defense is an educated managerial community. The private sector is probably better equipped to provide the educational material. This does not mean that there is no role for the public sector. The publication and distribution of that material might be a proper role for the SBA.

The scope of computer crime could be estimated. One would expect that two techniques could be used. The first method is to use the legal databases now being developed for the study of law. This provides a fast method of probing case histories to find examples of crime, small business, and computers. The second method draws of the techniques of marketing research. Just as a firm might test the public to learn if there is a market for its product, so might the task force probe small business for computer related crime.

As to whether knowing the scope of the problem is necessary to facilitate management assistance I would state that it certainly would help. While it is not necessary, I

would think that you would have a difficult time measuring the effectiveness of the result of any action if you did not know how wide spread the phenomenon is before the action. Therefore it is my opinion that a study of the scope of the problem be launched, before any remedy be prescribed.

The third question is hard to answer. Empirical measures in the social sciences are rare. The laws are new. Even if a good background study could be done in each state using the above stated techniques, it is doubtful whether the statutes have been on the books long enough to measure results. Still, in states having computer crime legislation could be studied against the background of those states that do not have such legislation.

There probably is a cause and effect relationship between states that have strong computer crime legislation and those states where the business community is so aware of the problem that they have been moved to purchase security equipment. Because of this it will be very hard to measure the true benefits of legislation as opposed to equipment. Further, if you goal is awareness, it probably does not matter which is better, only that the managing public learns about the problem.

I have strong personal doubts about the utility of an SBA resource center. This may stem from the fact that I have no idea where this will be, or what it will do. The small business community is so spread out across the country that centers of any kind tend to loose their effectiveness. That community would be better served through publication, or the availability of low cost consulting help.

From the testimony given on March 7, 1984, I have reservations about the SBA's ability to proceed immediately to provide information. It seems that all of their sources are geared to large enterprise. One needs to understand the problems of small business. Except for myself, none of the others testifying that day had much small business experience. If this is where the SBA is going for its resources, it would be making a grave error. I support the current wording of the bill, and back the 18-month study.

I have not had any personal experience with a firm that had computer crime. I did relate to the committee an event where a firm had programs written for it that were so scrambled so that they had not hope of ever supporting or changing the programs. In most of the work I do with small companies, I see a large potential for computer based crime. Currently, there is little interest on the part of management to change this. It is my hope that action like S. 1920 will go a long way toward correcting this situation.

Thank you for your interest in this matter.

Sincerely,

Robert Schuldenfrei

Senator TSONGAS. Mr. O'Mara.

STATEMENT OF JOHN C. O'MARA, EXECUTIVE DIRECTOR, COMPUTER SECURITY INSTITUTE

Mr. O'MARA. Thank you, Mr. Chairman.

I appreciate the opportunity to be here this morning.

My name is John O'Mara. I am executive director of Computer Security Institute.

I have been asked to discuss, as a for-profit membership organization, the services we offer to the general public, along with my views as to the role that SBA should play with regard to computer crime prevention.

Computer Security Institute was established in 1974 as a membership organization dedicated to helping computer users recognize the risks of computer use and to offering practical, cost-effective ideas on how to protect themselves.

Senator TSONGAS. Could I ask you to give us some idea of your own personal background?

Mr. O'MARA. Surely. I was a founder of Computer Security Institute. Educationally, I graduated as a mathematics major from Southern Illinois University. I received my master's in business administration at the University of Connecticut.

Senator TSONGAS. Thank you.

Mr. O'MARA. We are currently serving about 3,000 members nationwide. We are an educational organization as opposed to a consulting organization. We provide information on all aspects of computer security via publications, training, and our hotline service.

When a person joins Computer Security Institute, he receives a 500-page manual, which is an instant library on various aspects of computer security. They also receive a bimonthly newsletter, and they also have access to our hotline.

The annual fee for these services is $85. We are also introducing a new service for our members beginning in September of this year, a computer security quarterly. This is a magazine that will be focusing on computer security products and services, which is different than what we are doing at the moment in that most of our services do not concentrate on products and services.

Our other publications include the Computer Security Journal. I provided a sample to the committee previously. We also publish Computer Security Handbook, Computer Security Compliance Test, a small 12-page booklet, Computer Security Manager's Guide [Pure and Simple], which is available to the public free upon request.

We also have a postcard service which is mailed to the approximately 50,000 people who have corresponded with us asking for information about computer security or have participated in our various services. We send to these people twice a year a packet of cards which briefly describes various products and services that are currently available.

Our training includes an annual conference. In New York City this past year, we had 1,000 people participating from around the United States and Canada and overseas.

We have an annual IBM/Amdahl computer users workshop each summer. This is more highly focused. Obviously, it is a manufacturer-specific workshop.

We also have regional seminars that are conducted around the country. In 1984, we are offering 19 programs, 2- and 3-day security seminars, that focus on very specific areas within security—disaster recovery planning, security in the electronic office, establishing a computer security program.

We will train approximately 1,500 to 2,000 people this year.

Senator TSONGAS. Who are these people?

Mr. O'MARA. These are users of computer systems. Unfortunately, most of them are large-scale users. We have had a problem communicating the idea of vulnerability to the smaller users. They are Fortune 500 type companies, for the most part and medium-size companies to a lesser degree.

We also act as a clearinghouse for our members. If they call us with a problem, we try to put them in touch with people in their local area, people that we know have coped with similar problems.

I have provided to the committee brochures which describe these various services.

Senator TSONGAS. Would you give me an example? If someone calls you up and says, I'm concerned about computer crime in my company, and I am from——

Mr. O'MARA. But they don't, Senator, on that topic. Excuse me. I was just making the point that that has not been a historical problem with computer crime.

Senator TSONGAS. Well, you say that you act as a clearinghouse. You put members in touch with each other.

Mr. O'MARA. That is correct.

Senator TSONGAS. Now, the person calls you on what basis?

Mr. O'MARA. On a hotline basis. They will call in and——

Senator TSONGAS. Say what?

Mr. O'MARA. They say, I would like to talk with somebody; I have a problem. For example, we are looking at backing up our facility, our records, and we are starting from ground zero. We would really like to have some help in this area.

We then will put them in touch with people—hopefully, right next door or in the same area—who have been through that process.

Senator TSONGAS. But to make the phone call in the first place, there has to be concern.

Mr. O'MARA. That is correct.

Senator TSONGAS. Is it concern about crime, or is it a concern about——

Mr. O'MARA. That's the point I was trying to make before, that computer crime has not been the issue they have been most concerned with. I will later describe the data we have gathered which will give you a better feel for that.

Before I get to the recommendations for what we view the role of SBA to be, I would like to make a few comments about computer crime, computer security, and the bill in general.

Although I commend the intention of S. 1920 to assist the small business community, I submit that the bill's focus is misdirected. Although computer crime represents a risk to small business, it

should not be our No. 1 concern. If a comprehensive study is conducted to determine the current extent of small business computer crime, I guarantee that the findings will show that it is not a significant problem.

Again, it does represent a risk, but we should not tackle it as our first priority. I say that based on our experience. We are gathering information from our membership and nonmembers alike on a continuing basis. When a member joins, he or she provides us with information via the membership application. We ask them to identify their job function and their experience in security, and so forth, but we also ask them specifically what they are interested in, what kinds of services, what topics do they want us to provide information on.

On the membership application, we have approximately 30 topics that they can simply check off and then circle the one that is of most concern. Computer crime historically has not been high on their list. It is well down the list, at the lower half.

We also have an annual conference each year, as I mentioned before, where we offer 60 workshops. We also have general sessions. We have an exhibition. Out of the 60 workshops, they can only pick 6 to participate in. So that means they have to be highly selective. Again, our experience shows that computer crime is not important to them.

Senator TSONGAS. Wait a minute. You are losing me. You have a seminar on computer security, and you are saying that computer crime is not an issue of concern to them. What kinds of things are they coming to hear about?

Mr. O'MARA. As we just heard, there are areas that are more mundane. They are concerned about identifying their critical applications. If we lost our system, what would put us out of business; the disaster recovery implications; how do I audit my systems; how do I make sure that the people I am working with are the kinds of people that I really want?

That leads us to the question, what should be the top priority, and I submit that helping the small business manager recognize that they might have significant computer security risks is the top priority.

This is an educational problem, and it is a difficult one to manage. We have been trying to cope with this problem for over 10 years, trying to educate both the small- and large-scale users. But we have not been that successful as far as the small business community is concerned.

However, if we do that—that is, have the small businessmen take a look at their operation—they usually find areas for improvement and they will take corrective action.

By taking a more macro approach to the problem—that is, addressing the broader scope of computer security—we will receive the side benefit of reducing our risk of computer crime in the process.

In short, we encourage our members and nonmembers alike to recognize that information is a critical asset which deserves protection just as any other valuable resource; that we can protect ourselves cost-effectively, as evidenced by the comments we have

heard this morning; and we don't have to spend thousands of dollars to do so.

If we are not intimidated by the black box and we install commonsense, good business procedures, we can dramatically reduce our risk exposure.

I propose that we refocus S. 1920 to concentrate on raising small business management awareness of the need to control information resources. Protecting America's small businesses from the threat of computer crime would be a natural byproduct.

With that in mind, I recommend that the SBA's role be as follows: One, the Small Business Administration should take the lead in administering the program and should bypass the proposed task force.

Appoint SBA personnel with computer security expertise to assemble an information resource tailored to the needs of the small business, and that is the key, that it be tailored to the small business user.

Resources should be eminently practical, providing simple diagnostic tools for management to evaluate its own risks. For example, a manager's guide to asking the right questions. Also, the SBA should be making available information on current security products.

Two, distribute information through the existing nationwide network of SBA offices and install a feedback channel.

Three, for small businesses requiring more indepth assistance, provide the regional forums that have been proposed.

Four, establish mechanisms to evaluate the success or failure of the program. Does the experience warrant taking more ambitious steps in the future?

If I could make reference to the task force itself, one of the reasons I am suggesting that we bypass it relates to the functions of the task force. No. 1, the gathering of computer crime information, trying to get our hands around the problem, would be a wasted effort, based on our experience. Knowing that a potential exists is sufficient to get cracking, and I would hate to see us lose 18 months studying the problem.

I am also concerned with the second part of the task force's function, which will attempt to take a reading on what security products are out there. That information is readily available, and we would be more than happy to provide it to the Small Business Administration. Many of the security vendors are already participating in our programs. We have a fairly comprehensive listing of these firms.

I certainly welcome the idea of an information resource center. I believe that it would be an excellent way to go.

[The prepared statement and supplemental information of Mr. O'Mara follows:]

STATEMENT OF JOHN C. O'MARA

EXECUTIVE DIRECTOR, COMPUTER SECURITY INSTITUTE

to the SMALL BUSINESS COMMITTEE of the UNITED STATES SENATE

Mr. Chairman and Members of the Committee:

Thank you for the invitation to comment on S.1920, which would amend the Small Business Act to establish a Small Business Computer Crime and Security Task Force, recently introduced by Senator Tsongas.

I have been asked to discuss, as a for-profit membership organization, the services offered by Computer Security Institute, along with my views as to the role of the SBA in computer crime prevention.

DESCRIPTION OF COMPUTER SECURITY INSTITUTE

The Institute was established in 1974 as a membership organization dedicated to helping computer users recognize the risks of computer use and to offering practical, cost-effective ideas on how to protect themselves. We currently serve approximately 3,000 members nationwide. As an educational organization (we're not consultants), we provide information on all aspects of computer security via publications, training, and our Hot Line service.

A person or organization joining the Institute receives a 500-page Computer Security Manual, a newsletter every other month, and access to our Hot Line services. The annual membership fee is $85 and includes all of the above. Beginning in September of this year, members will receive at no additional cost the new magazine Computer Security Quarterly. Other Institute services include:

Publications

- Computer Security Newsletter *
- Computer Security Journal *
- Computer Security Handbook **
- Computer Security Compliance Test
- Computer Security: A Manager's Guide (Pure and Simple) *

[available to the public free upon request]

Training

- Computer Security Conference & Exhibition **

  Last year's 10th Annual conference was attended by 1,000 people from the U.S., Canada, and overseas.
- Annual IBM/Amdahl Users Computer Security Workshop **
- Regional Seminar program ** -- In 1984 we are conducting 19 two- and three-day computer security seminars around the country.
- We will train between 1,500 and 2,000 persons in 1984.

Networking

The Institute acts as a clearinghouse for people seeking solutions to common problems. We put members in touch with one another--ideally, those located near each other.

---

* A sample of the publication is provided to Committee members.

** A descriptive brochure is provided to Committee members.

CONTINUED

1 OF 2

COMMENTS ON COMPUTER CRIME, COMPUTER SECURITY, AND S.1920

Although I commend the intention of S.1920 to assist the small business community, I submit that the bill's focus is misdirected. Although computer crime represents a risk to small businesses, it should not be our number one concern. If a comprehensive study is conducted to determine the current extent of small business computer crime, I guarantee that the findings will show that it is not a significant problem. Again, it does represent a risk, but we should not tackle it as our first priority.

What should be the top priority? Helping small business management to become aware that they might be exposed to a wide variety of computer risks. This is an educational problem, and a difficult one to pull off. For ten years, we've been trying to educate large- and small-scale computer users to simply take a look at their vulnerabilities. If done conscientiously, they usually find room for improvement and take some type of corrective action. But even if they find their important applications are under control, fine ... they will sleep better. But there's another benefit to be derived from taking a more macro, "systems" approach to the problem -- installing effective controls will simultaneously reduce the risk of computer crime.

In short, we encourage members and non-members alike to recognize that information is a critical asset and deserves protection just as any other valuable resource. And we can protect ourselves cost-effectively--we don't have to spend thousands and thousands of dollars. By using sound judgment and not being intimidated by the

"black box," we can install common-sense, good-business procedures which will dramatically reduce our risk exposures.

I propose that we refocus S.1920 to concentrate on raising small business management's level of awareness of the need to control its information resources. Protecting America's small businesses from the threat of computer crime would be a natural by-product. With that in mind, I recommend that SBA's role be as follows:

RECOMMENDATIONS ON THE ROLE OF THE SBA

1. The Small Business Administration should take the lead in administering the program. Appoint SBA personnel with computer security expertise to assemble an information resource tailored to the needs of small businesses. Resources should be eminently practical, providing simple diagnostic tools for management to evaluate its computer risks (e.g., "A Manager's Guide to Asking the Right Questions") ... plus information on security products.

2. Distribute information through the existing nationwide network of SBA offices and install a feedback channel.

3. For small business requiring more in-depth assistance, provide (as originally proposed) periodic regional forums.

4. Establish mechanisms to evaluate the success or failure of the program. Does the experience warrant taking more ambitious steps in the future?

33-723 O - 84 - 7

United States Senate
COMMITTEE ON SMALL BUSINESS
WASHINGTON, D.C. 20510

March 12, 1984

Mr. John O'Mara
Executive Director
Computer Security Institute
43 Boston Post Road
Northborough, Massachusetts 01532

Dear Mr. O'Mara:

We would like to extend to you our thanks for testifying at the March 7, 1984 hearing on S. 1920, the Small Business Computer Crime Prevention Act. Your testimony will be very helpful to the Members of the Senate Small Business Committee.

Due to the time constraints of the hearing, there were some questions we did not get a chance to ask you. In order to make the testimony complete, the Committee would greatly appreciate it if you would consider these issues now and provide written responses for inclusion in the permanent hearing record.

1). Would you agree that the most effective role the Federal Government can play in assisting small businesses with computer security controls is to support and sponsor educational efforts in cooperation with the private sector?

2). S. 1920 states that it will be the function of the Task Force to "define the nature and scope of computer crimes committed against small business concerns." Can the scope of computer crimes committed against small businesses be defined with any certainty? Even if it can be, is such a definition of scope necessary to facilitate management assistance by the SBA to small businesses concerning computer security?

3). Is there any way of empirically determining the effectiveness of state legislation as opposed to security equipment in preventing computer crimes against small business concerns?

4). Is it necessary for the SBA to create a resource center as called for by S. 1920 in order to meet the information and assistance needs of small businesses concerning computer security?

5). There is general agreement about the need to educate the small business community about computer security controls. The SBA is ready to proceed immediately to provide information to small businesses on computer security. Do you support the SBA approach to proceed without the task force and 18-month study period?

Please send your responses to Mike Morris, Counsel of the Small Business Committee staff at 428A Russell Senate Office Building, Washington, D.C. 20510. Should you have any questions about the hearing or this request, please feel free to call Mr. Morris at 224-2016, or Alan Chvotkin, Minority Chief Counsel, at 224-8497.

Thank you in advance for your cooperation and prompt attention to this matter. Again, your participation in this hearing was greatly appreciated.

Sincerely,

PAUL TSONGAS
United States Senator

LOWELL WEICKER, Jr.
Chairman
Senate Committee on
Small Business

Computer Security Institute

43 Boston Post Road • Northborough, Massachusetts 01532

(617) 845-5050

March 26, 1984

Senator Lowell Weicker, Jr.
c/o Michael Morris
U.S. Senate Committee on Small Business
428A Russell Senate Office Building
Washington, DC 20510

Dear Senator Weicker:

Thank you for your March 12th letter (received 3/21). My responses to your five questions are as follows:

1. I agree that one of the ways the Federal Government can help small businesses protect themselves is to support and sponsor educational programs focused on computer security controls. I support a cooperative effort with the private sector only if it delivers highly practical, tailored information on a cost-effective basis.

2. I believe computer crime in the small business community is not a significant problem (although the potential certainly exists). Even if it were a serious problem, however, our experience indicates that attempting to quantify it would prove fruitless.

   The SBA can be of great help to the small business community without the definition/quantification of computer crime. In fact, we might well do a disservice by concentrating on that area. It would be far better to encourage small businesses to evaluate their computer systems in terms of their total risk. By taking a macro view and installing appropriate, comprehensive controls, we will greatly reduce all our DP-related risks ... including our crime risks.

3. To reply to your question, "Is there any way of empirically determining the effectiveness of state legislation as opposed to security equipment in preventing computer crimes against small business concerns?" -- I do not know of any.

4. Since the computer security needs of small businesses are not being serviced, it makes good sense for the SBA to take the lead and create a resource center as proposed by S.1920.

5. I emphatically support the SBA approach to proceed without the task force and 18-month study period. I believe the establishment of a task force "to study the problem" would be an egregious waste of our resources. (I would be happy to elaborate if you feel it is necessary.)

An additional comment. After participating in the March 7th hearing, it occurred to me that we generated a great deal of negativism. I think it is important to recognize that, in addition to all the problems (real and imaginary) discussed, we failed to identify a tremendous opportunity.

Certainly small business, as a group, is at serious risk with regard to computer security. The key reason is lack of management awareness of their computer vulnerabilities (and not their lack of resources, as we've been hearing). However, with proper education and the availability of effective tools, small businesses can dramatically reduce their risk, and they can do it without spending an inordinate amount of time and money.

And the opportunity? If we are successful in getting businesses to think and act with a security mind-set now, when they (and their EDP systems) are small, we can expect security to become embedded in their growth process. And, as we all know, the most effective, most economical controls are those which are incorporated at the design stages. This opportunity is particularly apparent to data security officers responsible for large-scale systems where security was an afterthought (currently the norm, not the exception). As a result, they must now deal with horrendous security problems on a patchwork, piecemeal basis. Their attempts to secure distributed networks with hundreds of users and dissimilar equipment converts to a difficult if not impossible task.

In summary, we enthusiastically support a modified version of S.1920 in which the Task Force is eliminated and the SBA immediately establishes an information resource center and regional training programs.

Sincerely,

COMPUTER SECURITY INSTITUTE

John C. O'Mara
Executive Director

jco/rkw
cc: Senator Paul Tsongas

Senator TSONGAS. Those comments have been suggested by others privately, so we are looking at that.

STATEMENT OF DAVID P. KAISER, UNDERWRITING OFFICER, ST. PAUL FIRE AND MARINE INSURANCE CO.

Mr. KAISER. Mr. Chairman, it is a pleasure to be here this morning.

Senator TSONGAS. Do you still have snow out there in Minnesota?

Mr. KAISER. Well, you inquired why there were so many people from Minnesota here. I think it has to do with the weather.

I am David Kaiser, underwriting officer from St. Paul Fire and Marine Insurance Co. I am responsible for the insurance products that we have for computer-related risks.

We have submitted a written statement which I will summarize.

Senator TSONGAS. What is your background, if I may?

Mr. KAISER. A graduate of the University of Minnesota with a B.A. degree in political science and sociology, and I have been with St. Paul Fire and Marine in the underwriting division for the last 11 years.

Senator TSONGAS. It is rather interesting that most people who have been here have backgrounds in criminology or business or political science as opposed to the technology-related engineering. I suppose those are the people that commit the crimes? Is that it? [Laughter.]

Mr. KAISER. That could be.

We at St. Paul introduced the first insurance policy specifically designed for computer operations in 1961. Since that time, we have remained——

Senator TSONGAS. 1961?

Mr. KAISER. 1961, correct. Since that time, we have remained in a position of leadership in providing insurance products for computer users and data processing service organizations.

My remarks reflect the view of St. Paul, and I also believe they reflect the views of most of the insurers that provide this type of insurance.

You have invited our comments concerning the role of the SBA in the prevention of computer crime and our involvement in improving computer security.

We believe the SBA must provide the major stakeholders in the prevention of computer crime a forum for the exchange of ideas and information, a structure for the formulation of solutions to this problem, and help in educating all of those involved.

Who are the major stakeholders in the prevention of computer crime? Obviously, small business. Second, vendors of computer security systems and devices as well as computer manufacturers and software developers. Insurance companies have a large stake in computer security, and, of course, law enforcement.

These are the people who must get together to discuss their mutual problems, agree to solutions and methods to prevent computer crime based on the resources and the abilities that each of the individual groups possesses.

We do not feel that any one of those stakeholders has a significant grasp of the entire problem, and only by bringing them together can they share the abilities that they have individually.

As one of the stakeholders in the prevention of computer crime, what have we in the insurance industry done to promote computer security? We have offered policies to provide financial protection against computer crime losses. In the small business area, we have offered limited loss prevention advice to go along with those policies.

Senator TSONGAS. Can you give me an example? Let's take that company in Massachusetts that was referred to. They call you up. What happens?

Mr. KAISER. They would call an agent of our company and inquire about a policy to protect them from computer crime. We get a simple application basically describing what their system is, what types of systems they have in place to protect themselves.

An underwriter at the insurance company will look at that and determine if the basic protection is there. If not, we will suggest that the person applying for insurance do some basic things.

In small businesses, we don't collect enough premium for insurance to individually tailor a loss prevention program for them, so what we do is say, Lock up your room, change your passwords, the commonsense type approaches. It is surprising the number of businesses who don't use the commonsense approaches. Beyond that, there is very little that we provide for the small business.

Senator TSONGAS. If you have a larger client, a Fortune 500, for example, what happens?

Mr. KAISER. With a Fortune 500 company, we will get into the close scrunity of their current security systems and their disaster recovery plans substantially more. We want to know the ins and outs, and we will get experts either that are on our own staff or we will hire consultants to help us in evaluating the security.

We have been trying to bring attention to the problem. We have been working with trade associations, business associations, bar associations, the media, insurance professionals, and public interest groups, trying to focus the attention of people on computer security and computer crime.

We attempt to improve security through the loss prevention methods that I have mentioned, as well as working with vendors of security systems and devices, consultants, and larger computer users. We take what we learn from the larger computer users and try to make that information available to our smaller customers.

These efforts, though, have had limited success. We have been talking with each of the other major stakeholders in the problem, but not as a group. There is very little communication between the stakeholders. It has been a one-on-one type of thing.

While we have begun this dialog with the various stakeholders we feel that we have not initiated any meaningful effort to provide a forum for discussion of computer crime and cannot initiate such an effort.

A forum for the sharing of information and resources is required to address the problem comprehensively. It can only be done through the auspices of someone like the SBA.

We have discussed the attention that is currently being paid to the problem, particularly in the media, and the question has come up, do we really need to create a task force? We feel there is no clear understanding of the scope of computer crime.

Computer users and data processing service professionals all agree that only the tip of the iceberg is known; that we really have no idea how big the problem is.

All four of the stakeholders that I mentioned in computer security address the problem, but it is from their own point of view. The exchange of information is extremely limited between these groups. They don't often talk the same language. There is very little understanding that occurs when we are talking different languages.

Insurance companies say you need to buy more insurance. The vendors of computer systems, security systems, say, "Let's have some more security systems." Law enforcement people and lawyers say, "Let's have some more laws and tougher enforcement." The small businessman is sitting there wondering, is my problem significant enough that I need to spend the money to protect myself from computer crime?

Most of the attention is centered on the larger risks, the larger computer users, the larger data processing services organizations.

One problem we find is that there is no commonly agreed to yardstick for the measurement of the effectiveness of security systems or devices. The small businessman has no basis of comparison between one system and device and another. Not knowing the language, not knowing the technology, they are at a loss. It is not like a burglar alarm system where there are standards set and that standard means something to people. You have a local alarm system or central station. That is all a person needs to know to understand the protection that he is getting.

Through a forum under the auspices of the SBA, these stakeholders can exchange information with each other and agree to common approaches to preventing computer crime. The major stakeholders in the prevention of computer crime have had only limited success in seeing beyond their own field of expertise. The actions and activities of these groups are disorganized and fail to focus on a comprehensive and cohesive approach.

The passage of the bill before you will provide the major stakeholders in the prevention of computer crime a forum for the exchange of ideas and information, a structure to focus on comprehensive solutions to the problem, and help in educating all of those involved.

Thank you.

[The prepared statement of Mr. Kaiser follows:]

STATEMENT BY

DAVID P. KAISER, UNDERWRITING OFFICER,

ST. PAUL FIRE AND MARINE INSURANCE COMPANY

BEFORE THE

SENATE COMMITTEE ON SMALL BUSINESS

March 7, 1984

Computer crime and its ramifications for small businesses are a new phenomenon in our society. As one of the leading computer insurers, we at The St. Paul have long been aware of the threats of criminal computer activity. Through our work with the American Electronics Association (AEA) and the Association of Data Processing Service Organizations (ADAPSO) we keep in close touch with developing problem areas and the growing technology to meet security needs. The network of information for large data centers is well established and security expertise is cost/effective for both businesses and law enforcement agencies. Computer theft or vandalism in a large data center quickly hits the six digit mark and qualifies as major crime. Legal and technical expertise has focused its attention in this area for some time.

Not so with small business and its computers. Technology for the small business computer itself is really in a developmental stage. The security threats to that technology similarly develop in response to new criminal opportunities. But we are confident that computer crime as it threatens small businesses is a very real and growing social and economic problem.

The issue of computer protection for small businesses becomes a problem because small businessowners fail to recognize existing dangers. Other perils such as

fire, flood or wind damage have predictable results due to the fact that humanity has suffered their effects for centuries.

Computers and their role in business life are a new and developing phenomenon. Threats to their operation go beyond traditional perils. And new threats emerge every day. The extent to which a business may have become dependent on the computers' operation is not really understood or appreciated -- especially in small or new businesses, where day-to-day existence may be the top priority.

So small businessowners fail to build into their business plans the costs of securing their computer systems once they have purchased them. In addition, as standard property insurance forms gradually expand to cover physical damage to computers, businessowners are lulled into believing they have purchased protection and the need for risk management efforts, such as security safeguards and data protection devices, is taken care of.

The task before all of us is to find the best ways to prevent computer crime from reaching large proportions in the small business environment.

What is needed, in our view is a cooperative effort between the makers of computer security devices, the computer users themselves, insurers and law enforcement agencies at every level. This cooperative effort should be to focus public attention on the potential perils of this developing technology.

From our perspective, each of these groups presently has little knowledge of the others' concerns or the extent to which each group is aware of the problem.

Computer security specialists tell us the same thing. In addition, small business computer theft or abuse isn't documented, nor, in some cases, is it even reported. Fear of loss of customer confidence keeps computer crime under wraps. Lack of a centralized system for quantifying and reporting such crimes keeps law enforcement officials in the dark. And the changing nature and capability of the technology prevents small businessowners from feeling confident about making decisions about security devices.

We think two things are needed. The first is to provide a forum for these groups to gain common understanding of the problem. We at The St. Paul often find ourselves caught between computer users who are searching for adequate security measures and the computer security experts who are developing the technology. Neither is talking the same language. Nor do they share a common understanding of the problems.

Before we can hope to find solutions to the computer crime problems of small businessowners, we need to arrive at a common definition of the problem. The only way we'll find solutions is if all the parties understand each others' role in deterring computer crime. The vehicles for this vary. But the need, in our minds, to reach common understanding, is critical. We believe the most effective way of achieving this is through the process outlined in the bill before you today.

The second thing that's needed is a recognized evaluation source for computer security devices. It's needed by small businesses, law enforcement agencies, computer security experts and insurers alike. For those of us in the insurance business, however, there are obvious analogies. In order to underwrite fire

insurance, we have nationally tested sprinkler systems to require and rely on. In order to write burglary insurance, burglar alarms, tested and approved by Underwriters Laboratory, are widely available.

No such standardized technical evaluation source exists in the computer industry. Until it does, all of the groups with a stake in small business computer crime will be without a benchmark for evaluating relative costs and protection capability and adequacy. And, the insurance industry cannot reasonably recommend tools for loss prevention.

We cannot predict where such a standard evaluation system should ultimately reside. Existing precedents, such as Underwriters Laboratory, have developed in the private sector. On the other hand, if work is already underway in the National Bureau of Standards, perhaps it should be allowed to progress there.

It is, however, our belief that without systematically evaluated security devices, progress in minimizing small business computer crime will be limited. And, without a common understanding of small business computer crime, all those concerned with the issue cannot hope that the adequate devices will be developed.

We at The St. Paul, because of our long history and obvious business stake in this issue, are eager to play a role in reaching these two objectives. We want to see the security analysis available to our potential customers. But more importantly, we look forward to the day when the threat of computer crime is not so potentially harmful because small business will have made themselves less vulnerable than we believe they are today.

Senator TSONGAS. Do you have any kind of group coverage for small businesses? For example, if SBANE approached you for some kind of group plan, are you in a position to provide something like that?

Mr. KAISER. Yes, we are. We currently have programs for the Association of Computer Users, which provides physical damage coverage including theft for the computers, the software, the media, and data.

We have a program for the Independent Computer Consultants of America, which is a group of small computer consultants. We also have a program for the Association of Data Processing Service Organizations, which is primarily the larger computer users and data processing service organizations.

So, yes, we would like to be of help. We can get the cost down and we can provide loss prevention services to these people much more efficiently.

Senator TSONGAS. Give me an example of a claim made against the policy.

Mr. KAISER. A common claim is what we call a head crash. Something in the machine goes wrong. The media may be destroyed and the data may be destroyed. We provide insurance coverage for the cost to re-create what was lost or damaged.

There may be vandalism, getting back to your disgruntled employee that destroys the records. We will provide the financial assistance for the customer to re-create those records.

If accounts receivable are lost, we will provide financial assistance to re-create the record as well as to reimburse them for accounts receivable that are just lost, that they cannot bill a customer for.

Senator TSONGAS. How do you determine that?

Mr. KAISER. Based on past records. Looking at the last 12 months of records, you can determine what approximately the accounts receivable for that month should have been and what he actually collected, and then we pay the difference.

Senator TSONGAS. How often have you had experience where someone's accounts receivable were destroyed?

Mr. KAISER. It is a very uncommon occurrence, and with keeping of proper duplicate records it is a very minor loss to most businesses.

Senator TSONGAS. Caused by whom?

Mr. KAISER. Generally, it is caused by a physical problem—fire, water damage—rather than a person getting in and scrambling the records.

Senator TSONGAS. Have you had examples of individuals in a company committing computer crime and then having claims made against you?

Mr. KAISER. Yes, we have. The accounting and bookkeeping function of any company is the primary source of those types of claims, where it is someone within the corporation who is channeling funds away from where they are supposed to be, and that is a common coverage that most companies do buy.

Senator TSONGAS. If somebody makes a claim, they have to know that they have been victimized, by definition. In what percentage of those cases is the perpetrator discovered?

Mr. KAISER. If it is a person within the small business we have very good success in identifying the person through standard means—finding out one of the employees whose standard of living has changed significantly. For someone outside the corporation, it is far more difficult. Small business people are probably not going to spend the money to attach a device to their system that tells them who is trying to get into their system, their telephone number, that type of thing.

Senator TSONGAS. Do you find any correlation between people who buy your insurance and sort of going past the problem in their own minds and not taking the precautions?

Mr. KAISER. We find that to be far more common than we would care to think, or we would care to have; that many people feel that the buying of insurance is all they need to do, and then ignore the security measures that need to be taken.

We provide coverage under our policies for mechanical breakdown of computer systems, errors in design or manufacture, so that if a computer breaks down, we will reimburse people for the cost to repair the damage.

Most computer users should buy a service contract from the manufacturer; then the manufacturer agrees to fix anything and everything that goes wrong with the machine.

When we began to provide coverage for losses that are covered by a service contract, most customers started dropping the service contract because the insurance was cheaper. We find that to be beginning in the computer security field, also.

Senator TSONGAS. Would anybody like to comment on the responses of anybody else on the panel?

[No response.]

Senator TSONGAS. We have questions here which we will submit to you, and we would appreciate it if you could respond in writing.

[Subsequent information was received and follows:]

United States Senate
COMMITTEE ON SMALL BUSINESS
WASHINGTON, D.C. 20510

March 12, 1984

Mr. David Kaiser
Underwriting Officer for
Commercial Accounts
385 Washington Street
St. Paul, Minnesota 55102

Dear Mr. Kaiser:

We would like to extend to you our thanks for testifying at the March 7, 1984 hearing on S. 1920, the Small Business Computer Crime Prevention Act. Your testimony will be very helpful to the Members of the Senate Small Business Committee.

Due to the time constraints of the hearing, there were some questions we did not get a chance to ask you. In order to make the testimony complete, the Committee would greatly appreciate it if you would consider these issues now and provide written responses for inclusion in the permanent hearing record.

1). Would you agree that the most effective role the Federal Government can play in assisting small businesses with computer security controls is to support and sponsor educational efforts in cooperation with the private sector?

2). S. 1920 states that it will be the function of the Task Force to "define the nature and scope of computer crimes committed against small business concerns." Can the scope of computer crimes committed against small businesses be defined with any certainty? Even if it can be, is such a definition of scope necessary to facilitate management assistance by the SBA to small businesses concerning computer security?

3). Is there any way of empirically determining the effectiveness of state legislation as opposed to security equipment in preventing computer crimes against small business concerns?

4). Is it necessary for the SBA to create a resource center as called for by S. 1920 in order to meet the information and assistance needs of small businesses concerning computer security?

5). There is general agreement about the need to educate the small business community about computer security controls. The SBA is ready to proceed immediately to provide information to small businesses on computer security. Do you support the SBA approach to proceed without the task force and 18-month study period?

Please send your responses to Mike Morris, Counsel of the Small Business Committee staff at 428A Russell Senate Office Building, Washington, D.C. 20510. Should you have any questions about the hearing or this request, please feel free to call Mr. Morris at 224-2016, or Alan Chvotkin, Minority Chief Counsel, at 224-8497.

Thank you in advance for your cooperation and prompt attention to this matter. Again, your participation in this hearing was greatly appreciated.

Sincerely,

PAUL TSONGAS
United States Senator

LOWELL WEICKER, Jr.
Chairman
Senate Committee on
Small Business

St. Paul Fire and Marine Insurance Company
385 Washington Street, St. Paul, Minnesota 55102
Telephone (612) 221 7911

Property & Liability
Insurance

April 5, 1984

Mr. Mike Morris
Counsel; Small Business Committee
428A Russell Senate Office Building
Washington, D.C. 20510

Re: S. 1920

Dear Mr. Morris:

The following are any responses to the additional questions posed by the Committee in the letter from Senators Tsongas and Weicker March 12th.

Questions: Would you agree that the most effective role the Federal Government can play in assisting small businesses with computer security controls is to support and sponsor educational efforts in cooperation with the private sector?

Response: This is the most effective long term role. Both the Federal Government and the private sector have unique resources and abilities available to them that when combined in an educational effort will be effective.

Question: S. 1920 states that it will be the function of the Task Force to "define the nature and scope of computer crime committed against small business concerns." Can the scope of computer crimes committed against small businesses be defined with any certainty? Even if it can be, is such a definition of scope necessary to facilitate management assistance by the SBA to small businesses concerning computer security?

Response: In order to provide small business the most comprehensive information possible to combat computer crime all types and methods of computer crime must be known. Even if all types of computer crime and means of perpetrating it are known, I do not believe all that knowledge currently resides in one person or organization.

In order to convince small business that computer crime is a problem that deserves their attention and action the scope of the problem must be reasonable well defined. Again, this information is not currently collected by any one organization. The collection of this information should take a relatively short period of time.

33-723 O - 84 - 8

Question: Is there any way of empirically determining the effectiveness of state legislation as opposed to security equipment in preventing computer crimes against small business concerns?

Response: While this is not an area in which I am an expert it would seem that in the strict sense of "empirical" the answer is no. However, I do believe that generalizations can be inferred from studying how both mechanisms function to deter the various types of computer crime.

Question: Is it necessary for the SBA to create a resource center as called for by S. 1920 in order to meet the information and assistance needs of small businesses concerning computer security?

Response: Most definitely! The various resources available in the Federal Government need to be available in one location. In addition, information available from the private sector, state and local government could be made available through the same center. I cannot emphasize too much the need for business to have one easy to contact center for information and one easy to contact center for those concerned about computer crime to make available information and resources they have.

Question: There is general agreement about the need to educate the small business community about computer security controls. The SBA is ready to proceed immediately to provide information to small businesses on computer security. Do you support the SBA approach to proceed without the task force and 18-month study period?

Response: The SBA will be making available information currently on hand or currently in process. This information does not have the input of the insurance market, probably very little if any input from security experts or business consultants who know first hand the practical side of small business capabilities and willingness to confront this problem. I have additional concerns about the quantity and quality of input from local, state and federal law enforcement, elected representatives and people in small business.

It appears the SBA has decided what the problem is, how large the problem is and how to deal with the problem without the input of those most affected by the problem.

Thank you for the opportunity to present my views.

Sincerely,

David Kaiser
Underwriting Officer

Senator TSONGAS. Let us take 20 minutes and hear from the administration about their reactions to all of this.

Thank you very much.

Mr. Thomson of SBA and Dr. Katzke of Commerce.

STATEMENT OF JAMES THOMSON, ASSOCIATE ADMINISTRATOR FOR MANAGEMENT ASSISTANCE, SMALL BUSINESS ADMINISTRATION, ACCOMPANIED BY JOHN BJORK, COMPUTER SECURITY PROGRAM MANAGER; AND JOHN SWEENEY, DEPUTY ASSOCIATE ADMINISTRATOR FOR MANAGEMENT ASSISTANCE

Mr. THOMSON. Mr. Chairman, I am the Associate Administrator for Management Assistance in the Small Business Administration, and I have been for the past 15 months. Prior to that, I was in the small business community in Illinois for a period of 21 years, from purchasing to sales to sales manager to president of a small manufacturing company.

I have a bachelor's degree from Bradley University back in Peoria, Ill.

On my right I have John Bjork, who is the Computer Security Program Manager for the Small Business Administration; and I also have John Sweeney, who is my Deputy Associate Administrator in Management Assistance in the SBA.

Senator TSONGAS. Do we have a copy of your statement?

Mr. THOMSON. Yes, sir, you should.

Mr. Chairman and members of the committee, I am pleased to appear before you today to discuss an issue of increasing significance for the small business community, computer security.

We commend you, Senator, and also Senators Nunn and Boschwitz, for sponsoring S. 1920, a bill to establish a small business computer crime task force. This legislation is heightening the awareness of the critical need to assist small business to combat computer crime and abuse.

The Small Business Administration looks forward to cooperating with others to help small businesses improve the management of their computer technology and to encourage them to protect it from abuse.

I will first present the agency position on the legislation at hand and then elaborate on a variety of efforts to reduce computer crime. While we agree that computer crime is a legitimate, growing small business concern, and that the Federal Government is rightfully charged with the responsibility to help educate the small business community to protect itself from these abuses, SBA cannot support enactment of S. 1920 for the following reasons:

It is not necessary to establish a special task force to study the impact of computer security problems on small businesses. The general area of computer crime and abuse has been sufficiently studied and researched by Federal and private specialists, and all concur that the lack of computer security controls poses a serious threat for large and small businesses alike.

The bill calls for the task force to define the nature and scope of computer crimes against small businesses. This would be extremely difficult to pinpoint exactly, particularly as to scope, because stud-

ies on computer-related crime do not necessarily differentiate between large and small companies.

Small can range from a sole proprietorship to a relatively large concern with millions of dollars in sales and hundred of employees. And, most importantly, from a computer security standpoint, it is the complexity and extent of the data processing function, and the nature of the business—not the size of the company—that determines vulnerability.

Finally, because only a very low percentage of computer crime is reported, it would be an enormous, expensive task to reach any meaningful conclusions about the unique susceptibility of small businesses to computer crime.

The legislation also requires the task force to ascertain the effectiveness of State legislation and available security equipment in preventing computer crime against small businesses. While some States have laws geared to deterring computer crime, it would be exceedingly difficult to determine their precise impact on computer crime.

Available technical, administrative and physical security controls, as well as security awareness programs for data processing environments, however, provide excellent barriers to minimize the likelihood of computer-related crime and abuse.

Senate bill 1920 also includes a provision mandating that the task force and the National Bureau of Standards develop guidelines to assist small businesses evaluate the security of computer systems. This information is already available from the Federal Government and the private sector, and more is published every day.

We question the wisdom of establishing a special task force to study a topic already so thoroughly researched. We propose instead to eliminate the formal study phase and proceed immediately to provide state-of-the-art information to small businesses on computer-related crime and abuse, along with management assistance on associated computer security controls.

We have had very few requests for computer security assistance, which leads us to believe that many in the small business community are not sufficiently concerned about its damage potential. Conversations with the Computer Security Institute confirm our experience.

Many small businesses have yet to learn how to use computers effectively, how to protect their information, and how to safeguard their computers from accidental and deliberate misuse. We want to educate our small business constituency.

SBA has already taken some important steps within our management assistance program. As you know, in recent years management assistance has developed a large network of voluntary and cooperative resources. Together they multiply and augment MA's training and counseling efforts, making it possible for the agency to help many more small businesses than could be reached by SBA staff alone.

As a delivery mechanism for information on computer fraud and security, we have in place the following local networks: SCORE and ACE, SBDC's, the SBI's, chambers of commerce, and the American Association of Community and Junior Colleges. In addition, we

have a large network of organizations who have signed statements of cooperation with the management assistance program to help wherever possible.

Using these delivery systems, we are implementing the following: One, publication of a Small Business Administration brochure entitled, "Computer Security Considerations for Small Business Systems." This publication will provide guidelines on technical, administrative, physical, personnel, and communications controls available to small businesses to safeguard hardware, software and information from espionage, fraud, sabotage, and loss from theft and environmental threats. Also included will be a recommended reading list on these subjects.

Two, stocking of the National Bureau of Standards computer security bibliography covering their publications on the topic. This includes new publications on protecting small computer systems.

Three, stocking of the Computer and Business Equipment Manufacturers Association's comprehensive bibliography of books, studies, articles and publications on computer information security.

Four, computer security film, "Time Bomb," available from SBA for viewing.

Five, addition to SBA publications on purchasing personal computers, addressing security controls.

Six, periodic participation in conferences and workshops by SBA computer security manager.

We would also be pleased to receive additional suggestions from you.

Mr. Chairman and members of the committee, SBA needs your assistance to develop the link between the private sector and the Federal Government to deliver current knowledge on computer security to the small business community. As you know, we are prohibited from cooperating with profitmaking organizations in providing counseling, training, and other varieties of management assistance.

Senator Weicker has introduced a bill, Senate bill 1203, which would amend the Small Business Act to permit us to cooperate with profitmaking organizations in providing management assistance to small businesses. We urge prompt, favorable consideration of this legislation.

The use of profitmaking institutions in our training delivery system would help us improve substantially both the quantity and quality of our management assistance programs. It would accomplish several valuable goals. It would provide access to training resources unavailable in the nonprofit arena.

For example, in the fields of computer technology and communications, almost all resources are concentrated in profitmaking firms. A major thrust in these and other high-tech fields is toward small business application. The agency must be able to assist small businesses in these crucial areas. Access to the revolution in information science will make the difference in survival or failure of many small businesses.

Enactment of this legislation would allow us to use the contribution already made by profitmaking resources and permit a cost-effective expansion of these contributions. Currently, we may use do-

nated resources such as training facilities and speakers, but we cannot accept the contributor as a cosponsor.

Further, we may enter into contracts and pay firms and professionals to provide training. We are confident that we could persuade many of these valuable resources to act as cosponsors free of charge.

We understand and share the concern that the Federal Government should not appear to endorse particular products or services. The authority given to the management assistance program to cosponsor training with profitmaking institutions would be strictly controlled.

Before any consponsored events are undertaken, the program and the cosponsor would enter into a written agreement to define clearly the cosponsorship terms. While I think that you would agree it is only fair that the cosponsor be identified in any material describing the event, no situation or statements will be permitted to allow the cosponsor to publicize his product or service.

The involvement of the private sector in assisting small business is an important end in itself. This end is enhanced by the fact that this involvement may provide small business its only access to critical technology. The authority to cosponsor with these institutions will broaden our ability to encourage economic integration and have a direct effect on the survival of small businesses.

The concern of a profitmaking firm unfairly promoting its product at the expense of our reputation is a real one. It is management's responsibility to assure that this does not occur. Maintaining our present restricted statute, while perhaps allowing us to avoid that responsibility, causes the loss of meaningful, cost-effective assistance to the small business community. We urge you to enact legislation to correct this inequity.

Mr. Chairman, this concludes my statement. I will be pleased to respond to any questions that you may have.

[The prepared statement of Mr. Thomson follows:]

SBA U.S. Small Business Administration Washington, DC 20416

STATEMENT OF
JAMES THOMSON, ASSOCIATE ADMINISTRATOR
FOR MANAGEMENT ASSISTANCE
SMALL BUSINESS ADMINISTRATION
BEFORE THE
COMMITTEE ON SMALL BUSINESS
UNITED STATES SENATE

March 7, 1984

MR. CHAIRMAN, MEMBERS OF THE COMMITTEE, I AM PLEASED TO APPEAR BEFORE YOU TODAY TO DISCUSS AN ISSUE OF INCREASING SIGNIFICANCE FOR THE SMALL BUSINESS COMMUNITY, COMPUTER SECURITY.

WE COMMEND SENATORS TSONGAS, NUNN AND BOSCHWITZ FOR SPONSORING S. 1920, A BILL TO ESTABLISH A SMALL BUSINESS COMPUTER CRIME TASK FORCE. THIS LEGISLATION IS HEIGHTENING THE AWARENESS OF THE CRITICAL NEED TO ASSIST SMALL BUSINESS COMBAT COMPUTER CRIME AND ABUSE. THE SMALL BUSINESS ADMINISTRATION LOOKS FORWARD TO COOPERATING WITH OTHERS TO HELP SMALL BUSINESSES IMPROVE THE MANAGEMENT OF THEIR COMPUTER TECHNOLOGY AND TO ENCOURAGE THEM TO PROTECT IT FROM ABUSE.

I WILL FIRST PRESENT THE AGENCY POSITION ON THE LEGISLATION AT HAND, AND THEN ELABORATE ON A VARIETY OF EFFORTS TO REDUCE COMPUTER CRIME. WHILE WE AGREE THAT COMPUTER CRIME

IS A LEGITIMATE, GROWING SMALL BUSINESS CONCERN, AND THAT THE FEDERAL GOVERNMENT IS RIGHTFULLY CHARGED WITH THE RESPONSIBILITY TO HELP EDUCATE THE SMALL BUSINESS COMMUNITY TO PROTECT ITSELF FROM THESE ABUSES, SBA CANNOT SUPPORT ENACTMENT OF S. 1920 FOR THE FOLLOWING REASONS.

IT IS NOT NECESSARY TO ESTABLISH A SPECIAL TASK FORCE TO STUDY THE IMPACT OF COMPUTER SECURITY PROBLEMS ON SMALL BUSINESSES. THE GENERAL AREA OF COMPUTER CRIME AND ABUSE HAS BEEN SUFFICIENTLY STUDIED AND RESEARCHED BY FEDERAL AND PRIVATE SPECIALISTS, AND ALL CONCUR THAT THE LACK OF COMPUTER SECURITY CONTROLS POSES A SERIOUS THREAT FOR LARGE AND SMALL BUSINESSES ALIKE.

THE BILL CALLS FOR THE TASK FORCE TO DEFINE THE NATURE AND SCOPE OF COMPUTER CRIMES AGAINST SMALL BUSINESSES. THIS WOULD BE EXTREMELY DIFFICULT TO PINPOINT EXACTLY, PARTICULARLY AS TO SCOPE, BECAUSE STUDIES ON COMPUTER-RELATED CRIME DO NOT NECESSARILY DIFFERENTIATE BETWEEN LARGE AND SMALL COMPANIES. "SMALL" CAN RANGE FROM A SOLE PROPRIETORSHIP TO

A RELATIVELY LARGE CONCERN WITH MILLIONS OF DOLLARS IN SALES AND HUNDREDS OF EMPLOYEES. AND MOST IMPORTANTLY, FROM A COMPUTER SECURITY STANDPOINT, IT IS THE COMPLEXITY AND EXTENT OF THE DATA PROCESSING FUNCTION AND THE NATURE OF THE BUSINESS, NOT THE SIZE OF THE COMPANY THAT DETERMINES VULNERABILITIES. FINALLY, BECAUSE ONLY A VERY LOW PERCENTAGE OF COMPUTER CRIME IS REPORTED, IT WOULD BE AN ENORMOUS, EXPENSIVE TASK TO REACH ANY MEANINGFUL CONCLUSIONS ABOUT THE UNIQUE SUSCEPTIBILITY OF SMALL BUSINESSES TO COMPUTER CRIME.

THE LEGISLATION ALSO REQUIRES THE TASK FORCE TO ASCERTAIN THE EFFECTIVENESS OF STATE LEGISLATION AND AVAILABLE SECURITY EQUIPMENT IN PREVENTING COMPUTER CRIME AGAINST SMALL BUSINESSES. WHILE SOME STATES HAVE LAWS GEARED TO DETERRING COMPUTER CRIME IT WOULD BE EXCEEDINGLY DIFFICULT TO DETERMINE THEIR PRECISE IMPACT ON COMPUER CRIME. AVAILABLE TECHNICAL, ADMINISTRATIVE AND PHYSICAL SECURITY CONTROLS, AS WELL AS SECURITY AWARENESS PROGRAMS FOR DATA PROCESSING ENVIRONMENTS, HOWEVER, PROVIDE EXCELLENT BARRIERS TO MINIMIZE THE LIKELIHOOD OF COMPUTER RELATED CRIME AND ABUSE.

S. 1920 ALSO INCLUDES A PROVISION MANDATING THAT THE TASK FORCE AND THE NATIONAL BUREAU OF STANDARDS DEVELOP GUIDELINES TO ASSIST SMALL BUSINESSES EVALUATE THE SECURITY OF COMPUTER SYSTEMS. THIS INFORMATION IS ALREADY AVAILABLE FROM THE FEDERAL GOVERNMENT AND THE PRIVATE SECTOR, AND MORE IS PUBLISHED EVERY DA[illegible]

WE QUESTION THE WISDOM OF ESTABLISHING A SPECIAL TASK FORCE TO STUDY A TOPIC ALREADY SO THOROUGHLY RESEARCHED. WE PROPOSE INSTEAD TO ELIMINATE THE FORMAL STUDY PHASE AND PROCEED IMMEDIATELY TO PROVIDE STATE OF THE ART INFORMATION TO SMALL BUSINESSES ON COMPUTER-RELATED CRIME AND ABUSE, ALONG WITH MANAGEMENT ASSISTANCE ON ASSOCIATED COMPUTER SECURITY CONTROLS.

WE HAVE HAD VERY FEW REQUESTS FOR COMPUTER SECURITY ASSISTANCE, WHICH LEADS US TO BELIEVE THAT MANY IN THE SMALL BUSINESS COMMUNITY ARE NOT SUFFICIENTLY CONCERNED ABOUT ITS DAMAGE POTENTIAL. CONVERSATIONS WITH THE COMPUTER SECURITY INSTITUTE CONFIRM OUR EXPERIENCE. MANY SMALL BUSINESSES HAVE YET TO LEARN HOW TO USE COMPUTERS EFFECTIVELY, HOW TO PROTECT THEIR INFORMATION, AND HOW TO SAFEGUARD THEIR COMPUTERS FROM ACCIDENTAL AND DELIBERATE MISUSE. WE WANT TO EDUCATE OUR SMALL BUSINESS CONSTITUENCY.

SBA HAS ALREADY TAKEN SOME IMPORTANT STEPS WITHIN OUR MANAGEMENT ASSISTANCE PROGRAM. AS YOU KNOW, IN RECENT YEARS MANAGEMENT ASSISTANCE HAS DEVELOPED A LARGE NETWORK OF VOLUNTARY AND COOPERATIVE RESOURCES. TOGETHER THEY MULTIPLY AND AUGMENT MA'S TRAINING AND COUNSELING EFFORTS, MAKING IT POSSIBLE FOR THE AGENCY TO HELP MANY MORE SMALL BUSINESSES THAN COULD BE REACHED BY SBA STAFF ALONE. AS A DELIVERY MECHANISM FOR INFORMATION ON COMPUTER FRAUD AND SECURITY, WE HAVE IN PLACE THE FOLLOWING LOCAL NETWORKS: SCORE AND ACE, SBDCS, SBIS, CHAMBERS OF COMMERCE AND THE AMERICAN ASSOCIATION OF COMMUNITY AND JUNIOR COLLEGES. IN ADDITION, WE HAVE A LARGE NETWORK OF ORGANIZATIONS WHO HAVE SIGNED STATEMENTS OF COOPERATION WITH THE MANAGEMENT ASSISTANCE PROGRAM TO HELP WHEREVER POSSIBLE.

USING THESE DELIVERY SYSTEMS, WE ARE IMPLEMENTING THE FOLLOWING:

1. PUBLICATION OF A SMALL BUSINESS ADMINISTRATION BROCHURE ENTITLED."COMPUTER SECURITY CONSIDERATIONS FOR SMALL BUSINESS SYSTEMS." THIS PUBLICATION WILL PROVIDE GUIDELINES ON TECHNICAL, ADMINISTRATIVE, PHYSICAL, PERSONNEL AND COMMUNICATIONS CONTROLS AVAILABLE TO SMALL

BUSINESSES TO SAFEGUARD HARDWARE, SOFTWARE AND INFORMATION FROM ESPIONAGE, FRAUD, SABOTAGE, AND LOSS FROM THEFT AND ENVIRONMENTAL THREATS. ALSO INCLUDED WILL BE A RECOMMENDED READING LIST ON THESE SUBJECTS.

2. STOCKING OF THE NATIONAL BUREAU OF STANDARDS COMPUTER SECURITY BIBLIOGRAPHY COVERING THEIR PUBLICATIONS ON THE TOPIC. INCLUDES NEW PUBLICATIONS ON PROTECTING SMALL COMPUTER SYSTEMS.

3. STOCKING OF THE COMPUTER AND BUSINESS EQUIPMENT MANUFACTURERS ASSOCIATION'S COMPREHENSIVE BIBLIOGRAPHY OF BOOKS, STUDIES, ARTICLES AND PUBLICATIONS ON COMPUTER INFORMATION SECURITY.

4. COMPUTER SECURITY FILM, "TIME BOMB," AVAILABLE FROM SBA FOR VIEWING.

5. ADDITION TO SBA PUBLICATIONS ON PURCHASING PERSONAL COMPUTERS, ADDRESSING SECURITY CONTROLS.

6. PERIODIC PARTICIPATION IN CONFERENCES AND WORKSHOPS BY SBA COMPUTER SECURITY MANAGER.

WE WILL BE PLEASED TO RECEIVE ADDITIONAL SUGGESTIONS FROM YOU.

MR. CHAIRMAN AND MEMBERS OF THE COMMITTEE, SBA NEEDS YOUR ASSISTANCE TO DEVELOP THE LINK BETWEEN THE PRIVATE SECTOR AND THE FEDERAL GOVERNMENT TO DELIVER CURRENT KNOWLEDGE ON COMPUTER SECURITY TO THE SMALL BUSINESS COMMUNITY. AS YOU KNOW, WE ARE PROHIBITED FROM COOPERATING WITH PROFITMAKING ORGANIZATIONS IN PROVIDING COUNSELING, TRAINING AND OTHER VARIETIES OF MANAGEMENT ASSISTANCE. SENATOR WEICKER HAS INTRODUCED A BILL, S. 1203, Which WOULD AMEND THE SMALL BUSINESS ACT TO PERMIT US TO COOPERATE WITH PROFITMAKING ORGANIZATIONS IN PROVIDING MANAGEMENT ASSISTANCE TO SMALL BUSINESSES. WE URGE PROMPT, FAVORABLE CONSIDERATION OF THIS LEGISLATION.

THE USE OF PROFITMAKING INSTITUTIONS IN OUR TRAINING DELIVERY SYSTEM WOULD HELP US IMPROVE SUBSTANTIALLY BOTH THE QUANTITY AND QUALITY OF OUR MANAGEMENT ASSISTANCE PROGRAMS. IT WOULD ACCOMPLISH SEVERAL VALUABLE GOALS. IT WOULD PROVIDE ACCESS TO TRAINING RESOURCES UNAVAILABLE IN THE NONPROFIT ARENA. FOR EXAMPLE, IN THE FIELDS OF COMPUTER TECHNOLOGY AND COMMUNICATIONS, ALMOST ALL RESOURCES ARE CONCENTRATED IN PROFITMAKING FIRMS. A MAJOR THRUST IN THESE AND OTHER "HIGH TECH" FIELDS IS TOWARDS SMALL BUSINESS

APPLICATION. THE AGENCY MUST BE ABLE TO ASSIST SMALL BUSINESSES IN THESE CRUCIAL FIELDS. ACCESS TO THE REVOLUTION IN INFORMATION SCIENCE WILL MAKE THE DIFFERENCE IN SURVIVAL OR FAILURE OF MANY SMALL BUSINESSES.

ENACTMENT OF THIS LEGISLATION WOULD ALLOW US TO USE THE CONTRIBUTION ALREADY MADE BY PROFITMAKING RESOURCES AND PERMIT A COST EFFECTIVE EXPANSION OF THESE CONTRIBUTIONS. CURRENTLY, WE MAY USE DONATED RESOURCES SUCH AS TRAINING FACILITIES AND SPEAKERS BUT WE CANNOT ACCEPT THE CONTRIBUTOR AS A COSPONSOR. FURTHER, WE MAY ENTER INTO CONTRACTS AND PAY FIRMS AND PROFESSIONALS TO PROVIDE TRAINING. WE ARE CONFIDENT WE COULD PERSUADE MANY OF THESE VALUABLE RESOURCES TO ACT AS COSPONSORS FREE OF CHARGE.

WE UNDERSTAND AND SHARE THE CONCERN THAT THE FEDERAL GOVERNMENT SHOULD NOT APPEAR TO ENDORSE PARTICULAR PRODUCTS OR SERVICES. THE AUTHORITY GIVEN TO THE MANAGEMENT ASSISTANCE PROGRAM TO COSPONSOR TRAINING WITH PROFITMAKING INSTITUTIONS WOULD BE STRICTLY CONTROLLED. BEFORE ANY COSPONSORED EVENTS ARE UNDERTAKEN THE PROGRAM AND THE COSPONSOR WOULD ENTER INTO A WRITTEN AGREEMENT TO DEFINE CLEARLY THE COSPONSORSHIP TERMS. WHILE I THINK YOU WOULD AGREE IT IS ONLY FAIR THAT THE COSPONSOR BE IDENTIFIED IN ANY MATERIAL DESCRIBING THE EVENT, NO SITUATION OR

STATEMENTS WILL BE PERMITTED TO ALLOW THE COSPONSOR TO PUBLICIZE HIS PRODUCT OR SERVICE.

THE INVOLVEMENT OF THE PRIVATE SECTOR IN ASSISTING SMALL BUSINESS IS AN IMPORTANT END IN ITSELF. THIS END IS ENHANCED BY THE FACT THAT THIS INVOLVEMENT MAY PROVIDE SMALL BUSINESS ITS ONLY ACCESS TO CRITICAL TECHNOLOGY. THE AUTHORITY TO COSPONSOR WITH THESE INSTITUTIONS WILL BROADEN OUR ABILITY TO ENCOURAGE ECONOMIC INTEGRATION AND HAVE A DIRECT EFFECT ON THE SURVIVAL OF SMALL BUSINESSES.

THE CONCERN OF A PROFITMAKING FIRM UNFAIRLY PROMOTING ITS PRODUCT AT THE EXPENSE OF OUR REPUTATION IS A REAL ONE. IT IS MANAGEMENT'S RESPONSIBILITY TO ASSURE THAT THIS DOES NOT OCCUR. MAINTAINING OUR PRESENT RESTRICTED STATUTE, WHILE PERHAPS ALLOWING US TO AVOID THAT RESPONSIBILITY, CAUSES THE LOSS OF MEANINGFUL, COST-EFFECTIVE ASSISTANCE TO THE SMALL BUSINESS COMMUNITY. WE URGE YOU TO ENACT LEGISLATION TO CORRECT THIS INEQUITY.

MR. CHAIRMAN, THIS CONCLUDES MY STATEMENT. I WILL BE PLEASED TO RESPOND TO ANY QUESTIONS YOU MAY HAVE.

Senator TSONGAS. In terms of the priorities of your agency, where would you put computer crime if you had to list it? I would assume pretty far down the list.

Mr. THOMSON. I would say that is perhaps true, but I think as we get more involved in some of the special awareness programs in which we are indeed involved, that this could be a major portion of that.

Senator TSONGAS. How much response have you gotten from the materials that you sent out?

Mr. THOMSON. Up to this date, I think very marginal reponse. Perhaps John Bjork could answer that better than I, sir.

Mr. BJORK. Well, of course, we really haven't sent out any of this material yet. We are just gearing up to carry out these tasks.

Senator TSONGAS. How many people have asked to see the film "Time Bomb"?

Mr. BJORK. Well, again, sir, we haven't gotten this information out into the small business community yet. We have had some response within our own agency to view it.

Mr. THOMSON. If I can add, Mr. Chairman, "Time Bomb" is in the SBA library. It is available for use. As far as the various other bibliographies that we are publishing, they are being written, and we will stock these publications for use.

Senator TSONGAS. Do you see the need for an aggressive program of getting this information out? I mean, there is a difference between having it in a library and promoting the publications and films, and so forth.

Mr. THOMSON. I think the match of the resources that we have throughout the United States, when we talk about the SBDC's and the other resources that are available to small business, that we can provide more and more information through this broad base of activities that we have.

Senator TSONGAS. The information that we get from the small business community is that that information is not getting out. I can understand maybe some of the concern about the task force, but I think the issue of, in essence, mandating a more aggressive approach, and so forth, has merit.

Mr. THOMSON. I will not disagree with that, sir.

Senator TSONGAS. Do you want to tell us all the good things you are doing in your shop?

Dr. KATZKE. I hope so.

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

Dr. KATZKE. Mr. Chairman, I am Stuart Katzke, manager of the Computer Security Management and Evaluation Group of the Institute for Computer Sciences and Technology at the National Bureau of Standards.

With your permission, I would like to summarize my written statement, which I have submitted for the record.

Senator TSONGAS. Could the four of you give me your own personal backgrounds, what you were trained in?

Mr. BJORK. I am the computer security program manager at SBA, and I have had 13 years' experience in computer security within the Government, implementing and developing and managing computer security programs.

I teach computer security at both the graduate school, Department of Agriculture, and the Northern Virginia Community College, and I lecture and write on the topic.

Senator TSONGAS. What about educational background?

Mr. BJORK. I have a bachelor's degree from Western Michigan University and a master's degree from American University in Latin American Affairs and Spanish. [Laughter.]

Senator TSONGAS. I can see why you did not offer that. [Laughter.]

Mr. BJORK. It is a growing concern in South America. [Laughter.]

Mr. SWEENEY. I am John Sweeney. I have a master's in finance and a master's in business administration. The concentration in business administration was in data processing, and my thesis was on the use of computers in small business.

Senator TSONGAS. Mr. Thomson, you gave me your background.

Mr. THOMSON. Yes, sir.

Dr. KATZKE. I have a bachelor of science and a master of science in mathematics and a Ph. D. in computer science. I taught at the College of William and Mary for 3 years, both graduate and undergraduate computer science courses, and then joined the National Bureau of Standards.

Senator TSONGAS. I think that background disqualifies you from testifying here. [Laughter.]

Dr. KATZKE. Shall I continue?

Senator TSONGAS. Yes.

Dr. KATZKE. What I would like to do is focus on the technical products and services that may be particularly useful for small businesses and describe some cooperative activities with government, industry, and businesses.

We address computer security within the framework of helping organizations improve their overall management and use of computers. We are concerned about reducing losses, confidentiality, integrity, and availability of computer data and processing resources, from events of all kinds.

It is clear from the number of calls, letters, and requests for assistance we receive that computer users are becoming more aware of the vulnerability of their systems to both accidental and intentional acts and that they are seeking help to reduce those vulnerabilities.

With the widespread use of microcomputers and the trend toward networking of computers, security will become an increasingly visible and critical issue for government and industry in the years ahead.

As systems and users become more sophisticated, new and more sophisticated technical controls will be needed. We are investigating some of these issues, such as the integration of technical controls in computer networks and the use of microcomputers to perform security functions.

33-723 O - 84 - 9

However, many basic controls, both management and technical, are available today; they are cost effective and can be implemented by organizations large and small.

Users must take the first step to assess their vulnerabilities and select the appropriate controls. We have issued a number of documents to help users take that first step. I have submitted for the committee's information a copy of our computer security publications list, a checklist of basic activities that every organization should consider in setting up a computer security program, and our Executive Guide to Contingency Planning.

Additional areas in which we have developed or are developing guidance documents include analysis of risk to determine potential losses from accidental and intentional events, planning for physical security of computer systems, certification and accreditation activities for computer security, planning to assure continuity of computer services, security for small systems—that is, microcomputers, identification and authentication of system users including use of passwords, planning for security of computer applications, use of data encryption techniques, methods for data integrity, controlling the access to data and resources by authorized users, and security of systems and networks.

The guidance documents that we have already issued provide a broad range of available management controls and technical safeguards that organizations can select to achieve a balanced program of computer security based on their analyses of risk.

Next I would like to discuss our cooperative relationships with government, business, and industry. ICST is charged with providing technical support to the Federal Government, and to fulfill that mission, we develop management guides, test methods, performance measures, technical information and advice, guidelines, and standards.

In developing our products and services, we pay particular attention to the problems of Federal computer users. We have found, however, that State and local governments, business and industry users have similar problems, and that our technical products are used by the private sector as well as by the public sector.

In the area of computer security and risk management, as well as in other program areas, we work closely with users in large and small organizations to learn about their experiences and their needs for technical and management solutions to their computer utilization problems.

We sponsor and participate in conferences, workshops, and meetings to share information and to keep users and industry informed of our activities, as well as to learn what others are doing. We respond to requests for advice and consultation, and we provide direct technical assistance to Federal agencies on a reimbursable basis for a limited number of projects that relate to our program.

Some examples of these activities include evaluating the applicability of the computer security technology research performed by the Department of Defense. We transfer that technology, where appropriate, to the civilian side of government and to business.

Other activities include cosponsoring workshops and seminars with Federal, State, and professional organizations; providing briefings to business and industry organizations such as EDP auditors,

computer security professionals, internal auditors, universities, bankers, lawyers, and computer user groups; analyzing user experiences; identifying best practices for computer security; and disseminating information that we have collected.

We use publications as well as informal contacts with users for these purposes.

We are cooperating with industry in the development of national and international voluntary standards. We are working closely with the banking community to develop standards needed to protect electronic funds transfers.

Finally, we perform research in systems and network security, often cooperatively with other organizations.

Mr. Chairman, this concludes my formal presentation. I thank you for your interest in our program, and I will be happy to answer your questions.

[The prepared statement of Dr. Katzke follows:]

U.S. DEPARTMENT OF COMMERCE

STATEMENT OF DR. STUART W. KATZKE
MANAGER, COMPUTER SECURITY MANAGEMENT AND EVALUATION GROUP
INSTITUTE FOR COMPUTER SCIENCES AND TECHNOLOGY
NATIONAL BUREAU OF STANDARDS
BEFORE THE
COMMITTEE ON SMALL BUSINESS
U.S. SENATE

MARCH 7, 1984

MR. CHAIRMAN AND MEMBERS OF THE COMMITTEE:

I appreciate this opportunity to tell you about the computer security and risk management program of the Institute for Computer Sciences and Technology. I will focus on our cooperative relationships with government, business, and industry in carrying out our program, and will point out some technical products and services that may be particularly useful for small businesses.

For more than ten years, computer security and risk management activities have been an important part of our overall technical program which focuses on helping organizations use computer and network technologies effectively. Our technical program addresses a spectrum of technical issues related to computer and network use -- interconnecting terminals, computers, and systems through networks; improving the management of information resources;

making computer software more reliable and less costly; as well as protecting data and computer systems from losses of all kinds.

ICST is charged with providing technical support to the Federal government, and to fulfill that mission, we develop management guides, test methods, performance measures, technical information and advice, guidelines, and standards. In developing our products and services, we pay particular attention to the problems of Federal computer users. We have found, however, that State and local governments, business, and industry users have similar problems and that our technical products are used by the private sector as well as by the public sector.

In the area of computer security and risk management, as well as in other program areas, we work closely with users in large and small organizations to learn about their experiences and their needs for technical and management solutions to their computer utilization problems. We sponsor, and participate in, conferences, workshops, and meetings to share information and to keep users and industry informed of our activities, as well as to learn what others are doing. We respond to requests for advice and consultation, and we provide direct technical assistance to Federal agencies on a reimbursable basis for a limited number of projects that are related to our program.

I want to emphasize especially our work with the Department of Defense. DoD has conducted extensive research in the development of security technology for national defense applications. We are continually

evaluating the applicability of DoD's research activities to the civilian side of government and the private sector, and we perform technology transfer activities where appropriate. We recently hosted our sixth workshop on computer security with DoD. The workshops have been well attended by both government and industry participants.

We have cosponsored several workshops on computer security evaluation with the General Accounting Office and have provided briefings and seminars on computer security to many Federal and State government organizations. An example of our interactions with State and local government users is the workshop on networks and computer security that we cosponsored with the Florida Joint Select Committee on Electronic Processing of the Florida Legislature last summer. More recently, we participated in a seminar for ADP managers in the Florida executive departments and testified before the Florida Joint Committee on Information Technology Resources.

We also participate in meetings sponsored by business and industry organizations. We have provided briefings and seminars for EDP auditors, computer security professionals, internal auditors, universities, bankers, lawyers, and computer user groups. A list of selected activities that we have completed since 1980 is attached to this statement.

As a result of our interactions with these groups, we are in a position to analyze user experiences and to identify best practices based on currently available technology. We publish a variety of reports, documents, guides, and studies conveying what we have learned, and we recommend methods and sources of information and assistance. For example, we share information

that we have collected on computer security training opportunities, reading lists, and computer security services.

We cooperate with business and industry to develop national and international consensus standards for computers and networks. We can do this effectively because of our knowledge of user and industry needs for standards and the position of trust that we have as objective participants in the standards process. Our goal is to stimulate the development of off-the-shelf commercial products that will expand choices, provide for interoperability of components and systems, and broaden opportunities for applications of new technology.

We are working with standards development groups sponsored by the American National Standards Institute, Institute of Electrical and Electronics Engineers, the International Organization for Standardization, and other national and international groups. We also participate with the National Communications Systems and the General Services Administration to develop Federal Standards for telecommunications. We work closely with bankers and auditors to develop standards, guidelines, and practices that are needed for their communities and that are beneficial for the Federal government and other users.

The last general activity that I want to cover is our laboratory program which gives us the technical foundation for all of our program efforts. We have established about a dozen small laboratories where different system and network technologies can be tested and where prototype standards and test measures can be developed. We are working cooperatively with

industry in many of these testing activities. For example, we are testing network standards with COMSAT, using satellite communications technology, and we are developing secure network techniques with the banking community.

I will now highlight some of our technical activities in computer security and risk management.

As I stated previously, we are addressing computer security within the framework of helping organizations improve their overall management and use of computers. We are concerned about reducing losses of confidentiality, integrity, and availability of computer data and processing resources from events of all kinds. Computers and data must be protected from physical damage, destruction, misuse, errors, omissions, and accidents. While break-ins to shared systems and incidents of computer crime are serious threats to system security, they are only one aspect of the computer security problem.

Most experts agree that losses resulting from accidental events are greater than those from computer-related mischief or crime. Reducing vulnerability to accidental events should be the first line of defense that computer users adopt. Safeguards against accidental acts have a two-fold effect -- they reduce the potential for harmful effects and they reduce opportunities for fraud and abuse. An abundance of errors in a system can effectively mask criminal activity.

It is clear from the number of calls, letters, and requests for assistance

we receive that computer users are becoming more aware of the vulnerability of their systems to accidental and intentional acts, and that they are seeking help to reduce those vulnerabilities. With the widespread use of microcomputers and the trend toward networking of computers, security will be an increasingly visible and critical issue for government and industry in the years ahead. New users, such as small businesses, will need help in recognizing computer security problems and providing protection to their systems and data.

As systems and users become more sophisticated, new and more sophisticated technical controls will be needed. We are investigating some of these issues such as the integration of technical controls in computer networks and the use of microprocessors for security controls. However, many basic controls -both management and technical -- are available today; they are cost effective; and they can be implemented by organizations, large and small. Users must take the first step to assess their vulnerabilities and select the appropriate controls.

We have prepared three documents that will start users and organizations on the road to finding cost effective solutions to computer security problems. The first is a checklist of activities that form the basis for a comprehensive computer security program. The activities are organized into those basic activities that should be done by every organization and those optional activities that address specific vulnerabilities. The second document is an executive guide to contingency planning that explains in a brief question and answer format why contingency planning

is essential and how to develop plans. The third document is a list of our computer security publications. Our publications are available for sale by the Government Printing Office and the National Technical Information Service to the public. The checklist, the contingency planning guide, and the publication list can be requested from ICST. Copies accompany this statement.

I will briefly describe the areas that we are addressing.

- Risk Analysis. Risk analysis is a procedure for estimating potential losses from destruction and theft of computers and data, and disruption of processing services. The results of a risk analysis are used in the selection of cost effective safeguards that are appropriate for the size of the system, the uses that are made of it, and the user's dependence on the data processing service. We have issued Federal Information Processing Standards Publication (FIPS PUB) 65, Guideline for Automatic Data Processing Risk Analysis, which describes a methodology that has been successfully used by many organizations for estimating losses caused by accidents or disruptive events.

- Physical Security. A basic outline for planning a security program that is appropriate for all organizations, regardless of size, is contained in FIPS PUB 31, Guidelines for Physical Security and Risk Analysis.

- Certification and Accreditation. These management-oriented programs are described in FIPS PUB 102, Guideline for Computer Security Certification and Accreditation, currently being printed. Developed in cooperation

with Federal and private sector auditing and computer security communities, this guideline describes how to establish and how to carry out a certification and accreditation program for computer security. Certification consists of a technical evaluation of a sensitive system to determine how well it meets its security requirements. Accreditation is the official management authorization for the operation of the system and is based on the certification process. These kinds of programs improve management control over and increase awareness of computer security within an organization.

- Contingency Planning. FIPS PUB 87, Guidelines for Contingency Planning, deals with the planning and preparation that must be done to assure continuity of ADP services should an unexpected event occur. Contingency planning is an activity that every user organization, large and small, should address. The executive guide that I mentioned is abstracted from this document. To assist in contingency planning, we expect to issue a guide to selecting ADP back up resources.

- Small Systems. A guide to the special problem of protecting microcomputer systems is being developed and will be available in draft form in the next few months. This is an issue that will be increasingly important as more and more small systems are used. We are establishing a laboratory for research and development of procedures to protect networks of small systems. The results of this work should be of particular interest to small business.

- Personal Identification. Two guidelines provide assistance in

selecting methods for identifying users of computer systems. Both guidelines are based on work done in our laboratories to assess personal identification techniques. FIPS PUB 48, Guidelines on Evaluation of Techniques for Automated Personal Identification, discusses the performance of devices such as fingerprint, handwritten signature, hand geometry, and palmprint readers. FIPS PUB 83, Guideline on User Authentication Techniques for Computer Network Access Control, describes the use of passwords, identification tokens, and other authentication techniques. We are investigating the possibility of voice verification methods as a means of user authentication.

- Password Usage. Passwords are still the most cost-effective method of personal identification for ADP system users and, if properly implemented, provide a reasonable level of personal identification and authentication needed for controlling access to computer resources. We have completed a password usage standard which specifies ten factors and related security criteria to be considered in the design of secure password systems. This standard and accompanying guidance on how to apply the standard will be issued as a FIPS.

- Applications Security. FIPS PUB 88, Guideline on Integrity Assurance and Control in Database Applications, provides step-by-step procedures for examining and verifying the accuracy and completeness of a database and for establishing management controls over data input and processing. FIPS PUB 73, Guidelines for Security of Computer Applications, covers security activities that should be considered during the life cycle of a

computer application and discusses fundamental security controls such as user authentication and security variance detection.

- Data Encryption. The Data Encryption Standard (DES), FIPS PUB 46, provides a technical method for protecting, through the use of encryption, computer data that is transmitted between terminals and computers. We issued this standard in 1977 to protect unclassified computer data. It has been adopted by ANSI as a voluntary industry standard (ANSI X3.92-1981) and has been recommended to banks by the American Bankers Association for use in protecting electronic fund transfers.

Alternate methods of using the DES, varying according to the specific application, are covered in FIPS PUB 81, DES Modes of Operation. This standard has also been adopted by ANSI (ANSI X3.106-1983).

FIPS PUB 74, Guidelines for Implementing and Using the NBS Data Encryption Standard, supplies further help on when to use encryption and how to manage and protect the secret keys that are used in the encryption process.

The DES has become the basis for techniques to prevent modification of data, to block unauthorized access to systems, and to authenticate authorized users. Proper use of the DES and management of the keys can provide secure communications of computer data today.

- Data Integrity. Data integrity is the assurance that data has not

been modified during processing, storage, or transmission. A data integrity standard developed by ICST uses the DES to protect data from being modified, either accidentally or intentionally, by putting a "seal" on the data. This "sealing" attaches an integrity code to the data that enables unauthorized modifications to be detected. This technique has been adopted by ANSI as a way to protect financial transactions. We have implemented the data integrity procedures in our laboratory as a Key Notarization System, and we are working with the banking community to adapt the notarization system for the banking environment. Two of our computer scientists have been awarded a U.S. patent for their work in this area.

- User Access Authorization. We are investigating techniques to control user access to data and resources of a computer system once user authentication has been established. A guideline on how to establish access authorization requirements and implement the necessary access control mechanisms is presently being developed.

- Open System Interconnection Security. Network security will be the foremost security issue in the future. The Open System Interconnection model of the International Organization for Standardization is a conceptual architecture for standards required to interconnect information systems. We are investigating integrity and security issues for that model.

I have summarized only the highlights of the computer security and risk management activities at ICST. Some of our other activities are also appropriate to the needs of small business. For example, we are assessing microcomputer technology, its uses, and ways that organizations can help

their small computer users. We have issued a review of Federal agency experiences using small computers and will soon publish a guide to assist end users in selecting software packages as a cost effective alternative to developing new software. Exchange of electronic messages and documents between small systems is another problem that we are investigating. We recently issued a guide to preventing electric power and grounding problems, such as loss of system availability, and loss of data from interruptions to power supplies.

Information about new publications and our conference schedule is included in the ICST newsletter which is issued three to four times a year. Requests to be placed on the mailing list for the newsletter may be sent to ICST, A209 Administration Building, National Bureau of Standards, Washington, D.C. 20234. We are also trying out other ways to exchange information with users. We have started teleconferences with State and local governments and with industry users. We also have set up three experimental electronic bulletin boards for message and information exchange and are considering one for computer security topics.

We welcome the opportunity to extend our information outreach to small businesses and we thank you for your interest in our programs.

Senator TSONGAS. How many people do you have in your shop?

Dr. KATZKE. We have the equivalent of about eight full-time people.

Senator TSONGAS. And you service the entire Federal Government?

Dr. KATZKE. That is correct. We also work very closely with private industry and business.

Senator TSONGAS. Do you mean within your spare time?

Dr. KATZKE. Well, we find that in order for us to do our jobs with the Federal community, we have to be interacting with private industry organizations and the vendor community, to find out what they are doing and to coordinate our activities so that we do not duplicate their efforts.

Senator TSONGAS. Your budget is proposed to be affected in the next fiscal year, is that correct?

Dr. KATZKE. That is correct.

Senator TSONGAS. In half?

Dr. KATZKE. That is correct, as I understand it.

Senator TSONGAS. What do you think of all that?

Dr. KATZKE. Well, as I understand the situation, that would mean that our activities in the computer security program would be curtailed or possibly even eliminated. If you would like more information about the impact of that, I could provide that to you in writing.

Senator TSONGAS. Well, I mean, have you ever thought of transferring over to DOD? You wouldn't have any problems over there. [Laughter.]

You would expand rapidly. Do you think I am kidding? But, I mean, I think that is the point. If we are going to take this issue seriously, all the rhetoric is nice, but the question is, where do you put your resources? To the extent that there is a problem, since you are the lead agency to deal with it and your funds are being slashed, I think it does send a very clear message.

How would you transfer the information and expertise that you have developed into the small business community, given the tasks that they have before them? I mean, how does that interface take place and what recommendations would you make?

Dr. KATZKE. Is that under the assumption that we had the resources to do it, or as we are now?

Senator TSONGAS. Well, your shop has a certain expertise.

Dr. KATZKE. That is correct.

Senator TSONGAS. How do you get that out to a small businessman in Michigan?

Dr. KATZKE. We would make the information that we have, the publications and publication lists, available to the Small Business Administration and have them distribute them through their interactions with the small business associations.

Senator TSONGAS. Are you in the process of doing that? Do you two work together on this issue?

Mr. THOMSON. We have some interworking here, and certainly it was our talking here that we would stock their informational pieces and distribute it into the field, and that we would have a broad coverage.

Senator TSONGAS. Is it fair to say that his. operation is "the" center of knowledge in this particular issue? Is that a fair statement?

Mr. BJORK. I would certainly say that is a very fair statement in the Government arena. They are responsible, of course, for establishing standards of how we operate our computer security programs and how we put safeguards in Federal systems. We look to Stu's shop for guidance in that, and they have been very helpful over the years.

Senator TSONGAS. So one would presume that if his operation were eliminated, that would hamper the capacity to get information out.

Mr. BJORK. Well, as you probably are aware, we are rewriting the Federal regulation from OMB now on how computer security functions within the Government. It is a rewrite of Transmittal Memorandum No. 1 to A-71. I mean, the core of that whole rewrite is NBS, and we are looking to them for guidance on standards.

If you eliminate them, forget the Federal computer security program. It wouldn't exist. They are absolutely the pivotal point in the whole process. That was mandated by the original TM-1 to A-71.

Senator TSONGAS. It is a good thing you have a background in something else, just in case. [Laughter.]

You don't get used to straight answers in this business, so I commend you for your comment.

Just one question that has been handed to me. You testified that the SBA is ready to proceed immediately to provide information to small businesses on computer security. Do you need some more money to do that?

Dr. KATZKE. I am sorry; were you addressing the question to me?

Senator TSONGAS. No, Mr. Thomson. We are just trying to keep you where you are. [Laughter.]

Dr. KATZKE. You were looking at me. I wasn't quite sure.

Mr. THOMSON. I think basically, Mr. Chairman, what we need is the law enacted to work with the profitmakers out there, to broaden the expanse that we have to small business and also to gain the expertise that is already out there in place that has information available that we can share.

Senator TSONGAS. I think I agree with that. But beyond that, do you think you have the internal resources to do the job?

Mr. THOMSON. Yes, sir, I do.

Senator TSONGAS. Mr. Sweeney, do you agree with that?

Mr. SWEENEY. Yes, sir, we do. We are hindered right now in the high-technology area as a whole—computers, computer security, communications—in that our usual delivery mechanisms to train and counsel small business are heavily dependent on retired executives, for example, who don't have the high-technology backgrounds. Most of that expertise is locked up in private firms, and we cannot go in and cosponsor with them.

We believe we can hit a much larger market of small business people in these areas if we can in fact be allowed to cosponsor with them.

Mr. THOMSON. I think, also, in addition to that, Mr. Chairman, is the additional colleges and universities that we are working with

33-723 O - 84 - 10

throughout the United States, not only the 2-year but the 4-year colleges, who are expanding very broadly into the computerization and data processing areas.

I am talking specifically in the SBDC's which we now have in 31 States.

Senator TSONGAS. Does anybody want to comment on any of the observations made by earlier witnesses?

Mr. SWEENEY. If I may, I would like to do that. Just to reinforce our point, I believe it was Congressman Weber who said that it all comes down to education. Professor Mirabito said it is an education process; that SBA should make small businesses aware. Mr. Schuldenfrei said that it is appropriate for SBA to sponsor seminars in computer security, and that is our field; we are good at it. We train about 300,000 business people a year in our program.

But we have a serious weakness in the high-technology area. We would like to overcome that weakness by cosponsoring. For example, of the business people who spoke here today who are the experts, they are, for the most part, private business people. We can invite them in to be speakers at a seminar. What we cannot do is go in and cosponsor with them, and we would like to have some ability to do that.

Senator TSONGAS. What we will do is, we will take the notion of cosponsorship, which I think has pretty broad support, and see how the business community would react, not only to that specifically, but does that solve the other problems that we are dealing with here today.

Thank you very much, and we will get back to you. These questions will be given to you, and if you could respond in writing, we would appreciate it.

[Subsequent information was received and follows:]

United States Senate
COMMITTEE ON SMALL BUSINESS
WASHINGTON, D.C. 20510

March 12, 1984

Dr. Stuart W. Katze
Manager
Computer Security Management Group
Institute for Computer Sciences
National Bureau of Standards
Department of Commerce
Building 225, B266
Washington, D. C. 20234

Dear Dr. Katzke:

We would like to extend to you our thanks for testifying at the March 7, 1984 hearing on S. 1920, the Small Business Computer Crime Prevention Act. Your testimony will be very helpful to the Members of the Senate Small Business Committee.

Due to the time constraints of the hearing, there were some questions we did not get a chance to ask you. In order to make the testimony complete, the Committee would greatly appreciate it if you would consider these issues now and provide written responses for inclusion in the permanent hearing record.

1). There is general agreement about the need to educate the small business community about computer security controls. Do you support the establishment of a SBA resource center as the most cost effective approach to providing small businesses information about computer security?

2). In your opinion what would represent the most cost effective approach to providing small businesses information about computer security?

3). Would additional funds be needed or would existing resources be sufficient?

4). How would you go about increasing outreach to small businesses?

Please send your responses to Mike Morris, Counsel of the Small Business Committee staff at 428A Russell Senate Office Building, Washington, D.C. 20510. Should you have any questions about the hearing or this request, please feel free to call Mr. Morris at 224-2016, or Alan Chvotkin, Minority Chief Counsel, at 224-8497.

Thank you in advance for your cooperation and prompt attention to this matter. Again, your participation in this hearing was greatly appreciated.

Sincerely,

PAUL TSONGAS
United States Senator

LOWELL WEICKER, Jr.
Chairman
Senate Committee on
Small Business

UNITED STATES DEPARTMENT OF COMMERCE
National Bureau of Standards
Washington, D.C. 20234

APR 08 1984

Honorable Lowell Weicker, Jr.
Chairman, Committee on Small Business
United States Senate
Washington, D.C. 20510

Dear Senator Weicker:

I am replying to your March 12 letter concerning my testimony before the Committee on Small Business. I am happy to provide the following information in response to the questions that were raised in your letter.

1. There is general agreement about the need to educate the small business community about computer security controls. Do you support the establishment of a SBA resource center as the most cost effective approach to providing small businesses information about computer security?

We have not evaluated, nor are we in a position to evaluate, the cost effectiveness of the resource center or some other mechanism that the Small Business Administration could use to distribute information on computer security.

2. In your opinion what would represent the most cost effective approach to providing small businesses information about computer security?

The least costly approach for the Institute for Computer Sciences and Technology would be to provide information about ICST products and services to the Small Business Administration for distribution to small businesses. In addition, other Federal agencies such as the Department of Defense and the intelligence agencies might have information that could be distributed by SBA.

3. Would additional funds be needed or would existing resources be sufficient?

ICST's current funding is sufficient to provide the Small Business Administration with information about ICST products and services to distribute to small businesses.

4. How would you go about increasing outreach to small businesses?

Services such as the following would increase outreach to small businesses:

- technical briefings through teleconferencing

- information exchange through small business associations

- a telephone hotline

- conferences and workshops specifically for small businesses

- bulletin board services through electronic information exchange

Since we are not mandated to serve small businesses directly, it is not appropriate for us to use our regular program funds for this purpose.

We appreciate the Committee's interest in our programs and will be happy to provide additional information that you may need.

Sincerely,

Stuart W. Katzke

Stuart W. Katzke
Manager, Computer Security, Evaluation and Management
Institute for Computer Sciences and Technology

cc: Honorable Paul Tsongas

United States Senate
COMMITTEE ON SMALL BUSINESS
WASHINGTON, D.C. 20510

March 12, 1984

Mr. James Thomson
Associate Administrator
Management Assistance
Small Business Administration
1441 L Street, N.W.
Washington, D. C. 20416

Dear Mr. Thomson:

We would like to extend to you our thanks for testifying at the March 7, 1984 hearing on S. 1920, the Small Business Computer Crime Prevention Act. Your testimony will be very helpful to the Members of the Senate Small Business Committee.

Due to the time constraints of the hearing, there were some questions we did not get a chance to ask you. In order to make the testimony complete, the Committee would greatly appreciate it if you would consider these issues now and provide written responses for inclusion in the permanent hearing record.

1). You testified that the SBA is ready to proceed immediately to provide information to small businesses on computer security. Will additional funding be needed to implement this new initiative or would existing resources be sufficient?

2). In your testimony you question the wisdom of establishing a task force to study a topic already so thoroughly researched. Have you made an estimate of the cost of convening such a task force for an 18-month study?

3). There is general agreement about the need to educate the small business community about computer security controls. Do you support the establishment of an SBA resource center as the most cost effective approach to providing small business information about computer security?

4). Is it your opinion that management assistance working together with SBA regional offices, ICST, for profit and not for profit groups can provide the most cost effective help to the small business community concerning computer security?

Please send your responses to Mike Morris, Counsel of the Small Business Committee staff at 428A Russell Senate Office Building, Washington, D.C. 20510. Should you have any questions about the hearing or this request, please feel free to call Mr. Morris at 224-2016, or Alan Chvotkin, Minority Chief Counsel, at 224-8497.

Thank you in advance for your cooperation and prompt attention to this matter. Again, your participation in this hearing was greatly appreciated.

Sincerely,

PAUL TSONGAS
United States Senator

LOWELL WEICKER, Jr.
Chairman
Senate Committee on
Small Business

U.S. SMALL BUSINESS ADMINISTRATION
WASHINGTON, D.C. 20416

Honorable Lowell Weicker, Jr.
Chairman
Senate Committee on
Small Business
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

I would like to thank you for the opportunity of testifying at the March 7, 1984, hearing on S. 1920, the Small Business Computer Crime Prevention Act. In your letter of March 12, 1984, you requested additional information on the subject and I am pleased to have the opportunity to respond.

1. You testified that the SBA is ready to proceed immediately to provide information to small businesses on computer security. Will additional funding be needed to implement this new initiative or would existing resources be sufficient?

   The additional cost of stocking publications and upgrading training to provide information to small business on computer security should be possible through present SBA resources. If, however, we are to establish a major Computer Security Task Force or other very signficantly expensive efforts it is very likely that additional funding will be necessary.

2. In your testimony you question the wisdom of establishing a task force to study a topic already so thoroughly researched. Have you made an estimate of the cost of convening such a task force for an 18-month study?

   We can only make a very rough estimate of the cost of convening a Computer Security Task Force. The cost of the actual task force meetings and the salaries and expense of Federal employees necessary to develop and support the task force would probably be $100,000 to $150,000.

   The major expense would be the development of a data base. At the present time there is very little information on how many and what kind of businesses use computers, how many of those use adequate computer security and what losses and crimes have been experienced by small business. In that the Small Business Administration has little expertise in developing crime and law enforcement data, and the task force is also unlikely to have the time or the necessary expertise, a consultant would have to be employed to build the data base and to interpret its meaning to the task force. Without that information the task force would be ineffectual. An effort of this nature seems likely to cost $400,000 to $600,000.

   Thus, the total cost of this effort would seem to approximate $500,000 to $750,000.

3. There is general agreement about the need to educate the small business community about computer security controls. Do you support the establishment of an SBA resource center as the most cost effective approach to providing small business information about computer security?

The establishment of an SBA Computer Security Resource Center does not seem to be a cost effective approach to providing small business information about computer security.

SBA has undertaken a number of efforts to inform small business about computer security concerns.

- We are preparing a new publication entitled, "Computer Security Considerations for Small Business Systems." We are doing everything we can to expedite the writing and publishing of this pamphlet, which will be made available to the public through our publications distribution system.
- We are stocking the National Bureau of Standards computer security bibliograhpy covering their publications on the topic.
- We are stocking the Computer and Business Equipment Manufacturers Association's bibliography of books, studies, articles and publications on computer information security.
- We have purchased, for our inventory of training films, copies of the computer security film, "Time Bomb."
- We are updating present publications on business computers with further information on computer security.
- We are encouraging cosponsored training to small business on the topic of computer security.

We think that these efforts will have a very substantial impact on small business. The establishment of a resource center will increase expenses far more than it will add to our ability to assist small business.

4. Is it your opinion that management assistance working together with SBA regional offices, ICST, for profit and not for profit groups can provide the most cost effective help to the small business community concerning computer security?

Yes. While there is some interest by small business in computer security, it seems to be relativel minimal. The first effort must be to sensitize small businesspersons to the potential damage that can occur to their companies because of a careless attitude toward the subject. Our publications and general small business computer training can be instrumental in providing this subject awareness. The implementation of new training programs specializing in the subject of computer security would then be better attended.

A key to this effort will be our ability to cosponsor with profitmaking organizations. The field of computer security, as well as the entire computer field and other high technology subjects such as the new communications technologies are becoming critically important to small business. Most of the expertise in these areas is employed by large profitmaking businesses with whom we cannot presently cosponsor. We believe these firms will work with us in helping small business when the proposed legislative change is enacted. Our mandate is to counsel and train small businesspersons and make them aware of potential problems. Utilization of profitmaking entities will enable us to outreach with the private sector in a shorter period of time, with dramatically reduced costs.

Thank you for this opportunity. If you require any further information or explanations, please feel free to call me.

Sincerely,

James N. Thomson
Associate Administrator
for Management Assistance

Senator TSONGAS. The committee record will remain open for an additional 2 weeks for statements by other members of the committee and for answers to questions coming back from the witnesses and any other comments any of the witnesses would want to make about today's hearing.

I would say to those earlier witnesses that if you wish to comment on statements made by following witnesses, you can do that.

There are also documents which will be included in the review of the legislation.

I also would like to commend Aviva Breshnev of my staff and Cynthia Ford, who is an intern on the Democratic staff of the committee. They are the ones who have done the work, putting all this together.

I would like to thank Chairman Weicker for his interest. I believe he is on the floor with the school prayer amendment to the SBA Act. [Laughter.]

So, he is otherwise occupied.

Thank you very much for coming.

Mr. THOMSON. Thank you, Mr. Chairman.

Senator TSONGAS. The committee will stand in recess.

[Whereupon, at 12:11 p.m., the committee recessed, to reconvene at the call of the Chair.]

○

END