COMPUTER SECURITY

HEARING

BEFORE THE

SUBCOMMITTEE ON
TECHNOLOGY AND COMPETITIVENESS

OF THE

COMMITTEE ON
SCIENCE, SPACE, AND TECHNOLOGY
U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED SECOND CONGRESS

FIRST SESSION

JUNE 27, 1991

[No. 42]

Printed for the use of the
Committee on Science, Space, and Technology

U.S. GOVERNMENT PRINTING OFFICE

46-040 WASHINGTON : 1991

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-035475-7

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

GEORGE E. BROWN, JR., California, *Chairman*

JAMES H. SCHEUER, New York
MARILYN LLOYD, Tennessee
DAN GLICKMAN, Kansas
HAROLD L. VOLKMER, Missouri
HOWARD WOLPE, Michigan
RALPH M. HALL, Texas
DAVE McCURDY, Oklahoma
NORMAN Y. MINETA, California
TIM VALENTINE, North Carolina
ROBERT G. TORRICELLI, New Jersey
RICK BOUCHER, Virginia
TERRY L. BRUCE, Illinois
RICHARD H. STALLINGS, Idaho
JAMES A. TRAFICANT, JR., Ohio
HENRY J. NOWAK, New York
CARL C. PERKINS, Kentucky
TOM McMILLEN, Maryland
DAVID R. NAGLE, Iowa
JIMMY HAYES, Louisiana
JERRY F. COSTELLO, Illinois
JOHN TANNER, Tennessee
GLEN BROWDER, Alabama
PETE GEREN, Texas
RAY THORNTON, Arkansas
JIM BACCHUS, Florida
TIM ROEMER, Indiana
BUD CRAMER, Alabama
DICK SWETT, New Hampshire
MICHAEL J. KOPETSKI, Oregon
JOAN KELLY HORN, Missouri

ROBERT S. WALKER, Pennsylvania*
F. JAMES SENSENBRENNER, JR., Wisconsin
SHERWOOD L. BOEHLERT, New York
TOM LEWIS, Florida
DON RITTER, Pennsylvania
SID MORRISON, Washington
RON PACKARD, California
PAUL B. HENRY, Michigan
HARRIS W. FAWELL, Illinois
D. FRENCH SLAUGHTER, JR., Virginia
LAMAR SMITH, Texas
CONSTANCE A. MORELLA, Maryland
DANA ROHRABACHER, California
STEVEN H. SCHIFF, New Mexico
TOM CAMPBELL, California
JOHN J. RHODES III, Arizona
JOE BARTON, Texas
DICK ZIMMER, New Jersey
WAYNE T. GILCHREST, Maryland

RADFORD BYERLY, JR., *Chief of Staff*
MICHAEL RODEMEYER, *Chief Counsel*
CAROLYN C. GREENFELD, *Chief Clerk*
DAVID D. CLEMENT, *Republican Chief of Staff*

SUBCOMMITTEE ON TECHNOLOGY AND COMPETITIVENESS

TIM VALENTINE, North Carolina, *Chairman*

DAN GLICKMAN, Kansas
NORMAN Y. MINETA, California
ROBERT G. TORRICELLI, New Jersey
RAY THORNTON, Arkansas
TIM ROEMER, Indiana
JOAN KELLY HORN, Missouri
RICK BOUCHER, Virginia
JOHN TANNER, Tennessee
JIM BACCHUS, Florida
DICK SWETT, New Hampshire

TOM LEWIS, Florida
DON RITTER, Pennsylvania
PAUL B. HENRY, Michigan
DANA ROHRABACHER, California
TOM CAMPBELL, California
WAYNE T. GILCHREST, Maryland
CONSTANCE A. MORELLA, Maryland

---

*Ranking Republican Member.

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

GEORGE E. BROWN, JR., California, *Chairman*

JAMES H. SCHEUER, New York
MARILYN LLOYD, Tennessee
DAN GLICKMAN, Kansas
HAROLD L. VOLKMER, Missouri
HOWARD WOLPE, Michigan
RALPH M. HALL, Texas
DAVE McCURDY, Oklahoma
NORMAN Y. MINETA, California
TIM VALENTINE, North Carolina
ROBERT G. TORRICELLI, New Jersey
RICK BOUCHER, Virginia
TERRY L. BRUCE, Illinois
RICHARD H. STALLINGS, Idaho
JAMES A. TRAFICANT, JR., Ohio
HENRY J. NOWAK, New York
CARL C. PERKINS, Kentucky
TOM McMILLEN, Maryland
DAVID R. NAGLE, Iowa
JIMMY HAYES, Louisiana
JERRY F. COSTELLO, Illinois
JOHN TANNER, Tennessee
GLEN BROWDER, Alabama
PETE GEREN, Texas
RAY THORNTON, Arkansas
JIM BACCHUS, Florida
TIM ROEMER, Indiana
BUD CRAMER, Alabama
DICK SWETT, New Hampshire
MICHAEL J. KOPETSKI, Oregon
JOAN KELLY HORN, Missouri

ROBERT S. WALKER, Pennsylvania*
F. JAMES SENSENBRENNER, JR., Wisconsin
SHERWOOD L. BOEHLERT, New York
TOM LEWIS, Florida
DON RITTER, Pennsylvania
SID MORRISON, Washington
RON PACKARD, California
PAUL B. HENRY, Michigan
HARRIS W. FAWELL, Illinois
D. FRENCH SLAUGHTER, JR., Virginia
LAMAR SMITH, Texas
CONSTANCE A. MORELLA, Maryland
DANA ROHRABACHER, California
STEVEN H. SCHIFF, New Mexico
TOM CAMPBELL, California
JOHN J. RHODES III, Arizona
JOE BARTON, Texas
DICK ZIMMER, New Jersey
WAYNE T. GILCHREST, Maryland

RADFORD BYERLY, JR., *Chief of Staff*
MICHAEL RODEMEYER, *Chief Counsel*
CAROLYN C. GREENFELD, *Chief Clerk*
DAVID D. CLEMENT, *Republican Chief of Staff*

SUBCOMMITTEE ON TECHNOLOGY AND COMPETITIVENESS

TIM VALENTINE, North Carolina, *Chairman*

DAN GLICKMAN, Kansas
NORMAN Y. MINETA, California
ROBERT G. TORRICELLI, New Jersey
RAY THORNTON, Arkansas
TIM ROEMER, Indiana
JOAN KELLY HORN, Missouri
RICK BOUCHER, Virginia
JOHN TANNER, Tennessee
JIM BACCHUS, Florida
DICK SWETT, New Hampshire

TOM LEWIS, Florida
DON RITTER, Pennsylvania
PAUL B. HENRY, Michigan
DANA ROHRABACHER, California
TOM CAMPBELL, California
WAYNE T. GILCHREST, Maryland
CONSTANCE A. MORELLA, Maryland

---

*Ranking Republican Member.

CONTENTS

WITNESSES

COMPUTER SECURITY

THURSDAY, JUNE 27, 1991

HOUSE OF REPRESENTATIVES,
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY,
SUBCOMMITTEE ON TECHNOLOGY AND COMPETITIVENESS,
Washington, DC.

The subcommittee met, pursuant to call, at 10:10 a.m., in room 2325, Rayburn House Office Building, Hon. Dan Glickman presiding.

Mr. GLICKMAN. Thank you for coming. Let's go ahead and get started.

In the first place, my name is Dan Glickman. I'm not the chairman of the subcommittee but I'm a member of it, and I'm the author of the Computer Security Act of 1987, which is essentially the subject of these hearings today. The subject is "Computer Security." So Chairman Valentine has graciously asked me to chair this hearing today, a follow-up or an oversight hearing on the Computer Security Act of 1987, and I appreciate it.

And, without objection, his statement will appear first in the record before my opening statement. And I will have an opening statement and then I will recognize my distinguished colleague from Florida, Mr. Lewis, who is the ranking Republican on this subcommittee.

[The prepared opening statement of Mr. Valentine follows:]

OPENING STATEMENT FOR COMPUTER SECURITY

BY THE

HONORABLE TIM VALENTINE (D-NC)

JUNE 27, 1991

IN THE EARLY DAYS OF COMPUTER TECHNOLOGY, MOST SYSTEMS WERE STAND-ALONE SYSTEMS IN COMPUTER CENTERS. USERS HAD VERY LITTLE DIRECT INTERACTION WITH THE COMPUTER. VERY FEW PEOPLE OUTSIDE OF THE DEFENSE DEPARTMENT PAID MUCH ATTENTION TO COMPUTER SECURITY.

AS COMPUTER NETWORKING BECAME MORE PREVALENT IN THE 1970s, BUSINESSES AND GOVERNMENT AGENCIES BEGAN TO DEPEND MORE AND MORE ON THE USE OF DISTRIBUTED COMPUTER SYSTEMS FOR INFORMATION EXCHANGE AND PROCESSING. FOR THE FIRST TIME, THE ENTIRE COMPUTER COMMUNITY BEGAN TO PAY ATTENTION TO THREATS TO COMPUTER SECURITY.

TODAY, DATABASES THAT CONTAIN SENSITIVE INFORMATION NOT ONLY RELATED TO NATIONAL SECURITY BUT ALSO TO THE ENTIRE ECONOMIC INFRASTRUCTURE OF OUR NATION CAN BE ACCESSED THROUGH COMPUTER NETWORKS -- SOMETIMES EVEN USING A PERSONAL COMPUTER IN THE PRIVACY OF SOMEONE'S HOME. OBVIOUSLY THERE IS A NEED TO SECURE THESE SYSTEMS AND DATABASES.

WE ARE BECOMING INCREASINGLY AT RISK TO HACKERS AS WELL AS TO THOSE WITH CRIMINAL INTENT. I LOOK FORWARD TO HEARING TODAY FROM OUR DISTINGUISHED WITNESSES AS TO WHAT PROGRESS HAS BEEN MADE TOWARDS SECURING VITAL COMPUTER SYSTEMS AND DATABASES, AND WHAT ARE THE RAMIFICATIONS IF WE DO NOT CONTINUE TO IMPROVE COMPUTER SECURITY THROUGHOUT THE NATION.

Mr. GLICKMAN. This morning we will hear from witnesses on actions—being taken or recommended—to increase computer security in Federal computer systems. The timing of this hearing could not have come more propitiously. Yesterday, the entire telephone system of this part of the United States broke, stopped working, because of a computer glitch. And, while we have no reason to believe that the computer glitch in the system that broke yesterday was caused by terrorism, foul play, or as a result of any insidious motive, the fact of the matter is, whether through negligence, through technological complexity and failure, or through just dumb luck, the computers that operated the telephones in the Nation's Capital, the most important city in the world, broke down. And it relates very much to the subject of the hearing today—is how do we protect computers and the information stored within them.

Regrettably, concerns over the integrity of computer-based communications and financial systems continue to be a timely topic. All too frequently, when I pick up the newspaper, there are stories that increase my concern about our continuing vulnerability to computer crime. For instance, a small software company, angry that Revlon hadn't paid up, shut down two of the cosmetic giant's factories by pulling the plug on the software that runs them. Could disgruntled employees or contractors shut down the Social Security Administration systems, the Federal Aviation Administration systems or the telephone service as well.

My fears that led to the Computer Security Act are not allayed. The information contained in our Federal computer systems still is not being protected adequately. While some progress has been made since the Act was passed, technological advancements are making the threats to our computers' security more intense. Our efforts to protect the sensitive information in our Federal computer systems must increase with the same intensity.

A recent National Research Council report says that the modern thief "can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb." That is frightening. What is really frightening is that unless the appropriate computer system controls have been implemented, the nature of a theft or the extent of sabotage might not be readily apparent. I look forward to hearing testimony on this report.

Since the Sixties, hackers have targeted the phone companies, when they discovered that by whistling tones at various frequencies they could control the phone systems. At the same time, hackers are starting to target the neighborhood telephone "switch" or computer that controls all the phones in a neighborhood.

One hacker, in Atlanta, discovered he had the ability to reroute telephone calls or bring down switching centers or, in the extreme, knock out service across the Southeastern United States. Bell South used 42 investigators at a cost of $1.5 million to track the intruder.

Phone calls to a Delray Beach, Florida, probation officer were routed to a New York dial-a-porn line. Similarly lax security could lead to data transmission phone calls being rerouted anywhere in the world—destination unknown.

Our first three witnesses have great familiarity with computer security risks and will help us better understand the problems we face. Mr. Schwartau, a speaker and consultant in information security and computer crime, will identify current risks and threats to computer systems. Mr. Walker, a computer security expert, will discuss the recent National Research Council's report. And, Mr. Benington, a communication security expert, will discuss the recent Network Security Report.

For a change, I have decided to put the lay witnesses, as opposed to the government witnesses, on first. Too often we hear government witnesses come on board in this area and tell us everything we're doing, and in many respects give us a pathetic acknowledgment of what they haven't done. Today, I have chosen to put the experts on first to let us know what is happening out there in the world. Then we can challenge the government witnesses to see how they respond to this.

Following this panel, the witnesses will bring us up-to-date on computer security improvement efforts within the Government. I look forward to hearing from the GAO on the results of an investigation of computer security at the Justice Department which was conducted at the request of Congressman Wise and the Committee on Government Operations.

Last year, the GAO reported to this committee that of the 22 computer security plans reviewed in 10 agencies only 38 percent of the planned 145 measures were implemented and inadequate top management support was frequently a key reason why controls had not been implemented. Fortunately, the OMB, during the past year, with representatives of the NIST—the National Institute of Science and Technology—and the National Security Agency—NSA—have been working to meet this challenge. They have made a series of visits to senior agency officials across the government to focus senior management attention on computer security risks and to follow up on the Computer Security Act planning process. Due to an illness in the family of its witness, the OMB has submitted testimony for the record on the results of these visits, and is not here.

And finally, I'm most interested to hear from Mr. Ray Kammer on the progress that NIST has made since the last hearing. Particularly, I want to hear the accomplishments of the cooperative initiatives with the National Security Agency and the international standard efforts.

Before I recognize Mr. Lewis, I want to talk about the front page of the Post today. I think it's pretty relevant. You read the story and it says, "This failure"—the C&P failure, telephone—"ranked among the largest ever to hit the U.S. telephone industry and underscored how the advanced computer systems on which society is becoming increasingly dependent have the capacity"—well, you know, there we are; somebody took my computer information—"have the capacity to disruption, largely because the private lines that link the Federal agencies were unscathed. Across town, blocks of downtown buildings could receive no calls made within the 202 Area Code or from callers in the suburbs with the 703 and 301 Area Codes. Phones in the suburbs were in the same blight." Long distance calls couldn't be made. I must tell you that my mother

tried to get me yesterday and was very upset that the line wasn't available into my office, and that is probably one of the reasons that I'm most upset.

Mr. LEWIS. Wait till you get home.

Mr. GLICKMAN. Wait till I get home is right. [Laughter.]

In addition, the articles point out that the problem is much more severe because modernization in computer software have made the interconnection and interdependency of software more critical than it has ever been before, therefore one glitch, one key negligent mistake, one key terrorist act, can have the most incredible amount of damage to this country and to information stored within. So we are talking not about an abstract problem, we are talking about a very real problem that we saw yesterday in this community, and one that could have even more devastating consequences to us.

So, in that context, I appreciate the fact that these hearings are being held. And now I would call on my distinguished colleague from Florida, Mr. Lewis.

Mr. LEWIS. Thank you, Mr. Chairman. It's nice to have you back here again. And I'm glad today that your name is Glickman and not Glitchman. [Laughter.]

Since the subcommittee hearing last year the issue of computer system has received increasing attention, and the front page newspaper accounts announcing the National Research Council's report on Computers at Risk began with "America's increasingly computerized society will become dangerously vulnerable to attacks by criminals and high-tech terrorists unless new nationwide computer system security precautions are taken soon." And today, when we hear from these witnesses who are on the National Academy Committee and also from the government, it will tell us much about what we can do about this problem.

The Public Broadcasting System aired a one-hour NOVA program on catching international hackers. The scientist who was featured had appeared before this subcommittee at an earlier hearing. And, just yesterday, we suffered, as you heard and read about, the 6-hour telephone failure because of a computer failure here in the local area. And, while the telephone company says that the disruption was not caused by computer hackers, the question still remains, Could it have been? And one of today's witnesses has already stated that a similar disruption in January 1990 was the result of purposeful manipulation. Is that true of yesterday's failure?

In addition, the technology that would enhance computer break-in has become more sophisticated. This occurs at the same time that the number of computers in use is also increasing dramatically. Is the current computer security law adequate to provide protection? Are the actions and plans of the Federal Government adequate to meet the challenge of making computers secure? And what additional actions, if any, does Congress need to take in order to ensure adequate computer security both now and over the long term?

Mr. Chairman, I hope we can hear some of those answers today. Thank you.

Mr. GLICKMAN. Thank you, Mr. Lewis.

Mr. Rohrabacher?

Mr. ROHRABACHER. Mr. Chairman, I have no opening statement. Thank you very much.

Mr. GLICKMAN. Thank you.

[The prepared opening statement of Mr. Ritter follows:]

OPENING STATEMENT
HEARING ON COMPUTER SECURITY
HON. DON RITTER (R-PA)
JUNE 27, 1991

Thank you, Mr. Chairman.

In the United States, continuing advances in information and communications technologies have led to a profusion of major productivity-enhancing innovations and quality-of-life improvements.

Unfortunately, as we have become more dependent on the efficiencies and improvements afforded by the information economy, we have also quietly become more vulnerable to potential abuse, criminal intent, and even acts of terrorism.

By some estimates, computer crime in the United States may already cost up to $50 billion a year. But not only is our private property in jeopardy, so too are our personal privacy and national security potentially at risk.

We need to know more about such vulnerabilities as well as how we can protect America's computer and information systems from viruses, hackers, electronic theft and even potentially hostile foreign interests.

I'd like to welcome our distinguished witnesses and look forward to their testimony about these and other problems as well the potential need for tighter computer security or other possible congressional options. Thank you.

Mr. GLICKMAN. We're pleased to have this first panel here. We'll start with Mr. Schwartau.

I would tell you that all of your statements will be made a part of the record, so we would like you, to the extent you can, move through your formal statement as quickly as possible so that we can get to the questions. But I'm not going to stick you with any arbitrary 5-minute time length right now because we only have two panels. But the more we can focus on questions the better we can.

So, Mr. Schwartau, it is a pleasure to have you.

STATEMENTS OF WINN SCHWARTAU, EXECUTIVE DIRECTOR, INTERNATIONAL PARTNERSHIP AGAINST COMPUTER TERRORISM, NASHVILLE, TN; STEPHEN T. WALKER, PRESIDENT, TRUSTED INFORMATION SYSTEMS, INC., GLENWOOD, MD; AND HERBERT BENINGTON, CHAIRMAN, NETWORK SECURITY TASK FORCE, NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE, AND DIRECTOR OF PLANNING, UNISYS DEFENSE SYSTEMS, McLEAN, VA

Mr. SCHWARTAU. Well, Thank you, Mr. Chairman, and members of the subcommittee, for the opportunity to speak. Your opening remarks are certainly very poignant, especially in light of when we look at the General Dynamic situation in San Diego that occurred yesterday as well, where a defense contractor's systems were attacked by a virus for the Atlas Missile Program. And all of these things happening in one day was certainly very poignant, as you pointed out.

When we look at the Computer Security Act and the effect of the Computer Security Act on the security of government computers it is impossible to consider the Federal computer systems as isolated entities any longer. In a networked society, which we have become over the last dozen years, we have an interconnection of well over 50 million computers into a global network which has become the backbone, the blood and the oxygen of our culture. And today, we actually rely on approximately 50 percent of our gross national product to be run through our computer systems, and this is part and parcel of what American culture has become. Simply put, without computers we become a second-class nation.

Therefore, through these comments, there are three points that need to be underscored and remembered. Number one, that government and commercial computer systems are so poorly protected today that they can essentially be considered defenseless; essentially, an electronic Pearl Harbor waiting to occur. Number two, as a result of inadequate security and considerations on the part of both government and the private sector, the privacy of most Americans virtually disappears the minute that their name is entered into a computer with any data about them. And lastly, number three, the Computer Security Act of 1987 was an excellent first step in creating legislative mandates in protecting government systems, but for reasons that we'll see in a moment they are not truly addressing the modern threats to government computers.

As you mentioned, computer crime is a burgeoning business, with losses ranging as high as an estimated $50 billion currently,

with some people projecting losses as high as $500 billion if we continue to go unprotected over time. Based upon statistics from the FBI and the Justice Department, only 1 out of every 22,000 computer crimes ever result in a conviction. Using those figures in mind and the number of convictions we've received, that estimates over 1 million computer crimes are occurring all the time every year.

Computer crimes are also very unique, in that if the criminal desires he can retain absolute anonymity and remain invisible to law enforcement agencies. The tools that he uses are very cheap and commonly available, and the government itself is an ideal target and just as vulnerable, if not more so, than the private sector.

One of the things that the Computer Security Act began was the process of addressing the problem, but it did not specifically address the growth of technology, both on a defensive posture and an offensive posture. And, taking that into mind, I'd like to just briefly outline four types of popular computer weaponry that are being used today and are very likely to be used in the future by those groups who we now consider adversaries.

One is malicious software, the viruses. We understand that and there is no need to go into any detail on those.

The second is communications interception. We saw a portion of that yesterday when the entire public network can go down. But also, with the tools that are available now to listen in on faxes, on conventional computer conversations, on computer dial-up lines, essentially they are all wide open and open to eavesdropping, thereby we face not only a security problem but a devastating privacy problem.

The third large area of computer weaponry is electromagnetic eavesdropping. Very simply, all computers, modems, printers, all electronic equipment broadcasts unique electromagnetic signatures corresponding to the data that is being processed at the time. There are very, very simple and inexpensive techniques for picking up that information with a simple radio receiver tuned to the broadcast frequency of that computer. The price for such technology is under $100 and is available from catalogs today. And this is something that is not being specifically addressed outside of the military community, and something that is a threat to privacy and security today.

The fourth area, perhaps is on the fringe, but it is imminently doable and possible by high-tech groups who have a vested interest in performing these crimes. These refer to computer guns and computer bombs which are, specifically, electronic devices aimed at either disrupting computer systems, networks or communications systems, or if the guns are turned up, shall we say, loud enough, a magnetic bomb can actually cause all data on computers to be destroyed as well as the contents, the actual silicon chips within the computer, to be destroyed.

One of the classic examples that has been made in the past on this is, if such a bomb went off in the Wall Street area of New York City or, perhaps, here in Washington, we could see the devastating effects of losing thousands and thousands of computers upon a single crime.

The cumulative effects of computer weaponry is something else that has not been really examined through this Act or through other policies. We tend to think of the virus. We tend to think of the eavesdropper, what have you. But we have not considered the cumulative effects of what happens when all of these things occur simultaneously by a well-financed, well-organized and highly motivated adversary. When we begin to look at the cumulative effects of these various offensive computer techniques, we can begin to see some of the truly devastating things that can be done to the American economy.

What Congress can do is the purpose of these hearings, and step one, in my opinion, is for Congress and the American people to become acutely aware of how serious the problem is to the security and the privacy of individuals and corporations and organizations within this country. And along that line, a National Information Policy of some sort needs to address the concerns, and use that as a springboard to carry forward. Under the National Information Policy, we need to be able to gauge anew what information is valuable and what classification methods we use for that information.

Number two, we need to add definitions, and perhaps re-examine, civilian government classification levels to take into account the privacy concerns of the Americans with regards to the data that is being held inside of government-controlled computers.

Number three, we need to define some criteria by which the private sector actually controls its data, the security of it, within its computer systems and the methods of disclosure. There has been much issue made recently about privacy of data on the part of the private sector, and we need to address that in part and parcel of a National Policy.

We also need to recognize that as computer technology advances we end up with more and more powerful computers, so do the adversaries. And we need to be able to take that into effect when we are trying to establish some sort of policy that will not become so fixed as to be stagnant over the long haul.

Number five, we need to establish a formal relationship with the international computer security communities, primarily those in the EEC. At this point there are virtually none on a formal basis.

Number six, we need to bring current export controls more in line with the reality of the technology available worldwide. Current policies and procedures for export and multinational use of computer security technology is currently hindering international security cooperation and exports of the United States.

And, number seven, under the National Information Policy, create an effective national legislation for the legal tools to provide the ability to adequately prosecute computer crimes of all natures under a single banner, instead of merely requiring the various U.S. attorneys and other prosecutors to search out existing statutes that may or may not be applicable in any of these cases, and under which there are currently many conflicting judicial opinions.

In closing, Mr. Chairman, I recognize that there are a lot of issues here to be dealt with and that in this short time I only can cover them very, very briefly. But I do hope that, perhaps, under the leadership of this committee, in the future the Computer Secu-

rity Act can be expanded to take into consideration some of these points that I have been mentioning here.

I thank you, Mr. Chairman, and members of the committee, for this opportunity, and I'll be happy to answer any questions, if I might.

Mr. GLICKMAN. Thank you. Excellent statement.

[The prepared statement of Mr. Schwartau follows:]

INTER • PACT
International Partnership Against
Computer Terrorism

Winn Schwartau
Executive Director

June 24, 1991

Submitted Testimony:

**Committee on Science, Space and Technology,
Subcommittee on Technology and Competitiveness hearings.**

Mr. Chairman, and members of the subcommittee:

Introductory Comments

Since the main focus of these hearings is on the Computer Security Act of 1987, and its effect on the protection of Federal data, I will attempt to use that bill as a launch platform and landing strip for my comments.

But, as will soon be clear, the undercurrent of apathy for the sanctity of Federal computer systems and the information under their aegis is so endemic as to have contaminated the private sector with the same indifference.

It is impossible to consider the Federal computer systems as isolated entities. In a networked society, which we have well become in the last dozen years, the interconnection of 50,000,000 computers into a Global Network has become the backbone, the blood and oxygen of our culture. As America shifted to a service-oriented economy in the last decade, we developed and now rely on an incredibly complex information-processing infrastructure which sustains an estimated 50% of this country's Gross National Product.

It is no longer possible to look at Government computers as being the only ones that hold a national security interest. We must also consider the commercial sector's computers to be equally critical to the continuing economic and world leadership position

112 Blue Hills Court • Nashville, TN 37214 • (615) 883-6741 • Fax (615) 883-6761

we enjoy. Without computers, we become a second class nation.

Therefore, my comments will necessarily traverse the increasingly nebulous tenet that deems private computing systems and information networks to be of any less importance to this country than those operated by the Government.

There are three points that need to be underscored and remembered throughout this discussion.

1. Government and commercial computers are so poorly protected today, that they can be essentially considered defenseless. An electronic Pearl Harbor waiting to happen.

2. As a result of inadequate security planning and considerations, on the part of both the Government and the private sector, the privacy of most Americans virtually disappears once their names are entered into a computer.

3. The Computer Security Act of 1987 was an excellent first step in creating legislative mandates for protecting Government computer systems. However, for reasons that we will address, the bill has had little effect on thwarting real threats to Government computers.

Computer Crime

Computer crime is a burgeoning business that costs the economy as much as $50 Billion annually. While this figure may appear high, we need to remember that computer crime is a relatively new enterprise, and as it becomes an organized, the threat to business and Government alike, losses upwards of $500 Billion per annum are not unreasonable to expect. This staggering figure does not contemplate the effect to the security of this country.

The history of prosecution of computer crimes does not bode well for the future.

Based upon recent statistics only 1 out of every 22,000 computer crimes results in a conviction. Using current figures, that means there are over 1,000,000 computer crimes occurring every year, with few of them detected, fewer still reported, and only a handful prosecuted.

Computer Crimes have a number of inherent characteristics that make them highly profitable, very safe and thus very attractive. In the security field we call these attributes High-Reward/Low-Risk.

It is statistically safer to commit a computer crime than to drive your car to work. As the 1990 National Research Counsel report, "Computers At Risk" states, the computer will surpass the gun as the weapon of choice in the 1990's.

Computer Crimes are unique in the annals of criminology:

* The effects of a computer crime can be felt long after the perpetrator is far gone.

* The computer criminal can do his thing just as effectively from great distances as from near the victim.

* If the criminal so desires, he can remain invisible and retain absolute anonymity.

* The skill level to effect a computer crime is easily learned and the knowledge widely available.

* The tools are cheap and legally acquired.

* A single computer crime can have devastating and far reaching effects on multiple victims at the same time. I prefer to refer to these criminals as Computer Terrorists.

The Computer Security Act of 1987

The Computer Security Act of 1987 was an excellent first step to guard Government computer systems from compromise, but as we know, technology is on a upward spiral in sophistication and capability. So it is with computer crime. For the first time in history, the computer as a weapon is legally and necessarily available to anyone who desires to purchase one. Therein lies much of the problem. We promote the proliferation of the computer as a tool, yet we have failed to recognize the offensive capabilities of them as weapons, thereby leaving most computer systems, private and public, defenseless.

A misleading catch phrase became popularized by those in the information security community in 1988 after the passage of the Act. The slogan, 'C2 by '92' refers to the mandatory implementation of a specified security level across vast numbers of Government computers. Figures suggest that approximately 85% of Federal computing systems would fall under the C2 security specifications as defined by the Trusted Systems Evaluation Criteria, published in 1985 by the National Computer Security Center; a now disbanded division of the National Security Agency.

However, the Computer Security Act, most notably in its implementation, has not taken into acount, the myriad and increasingly real threats to our computing infrastructure.

Computer Weaponry

Computers can easily and cheaply be adapted to malevolent purposes. The nature of the crimes can be broadly labeled into four groups.

Malicious Software

Much media attention has been given to the infamous computer virus, and its subsets including Trojan Horses, Logic Bombs, WORMs, Stealth viruses and the like. Viruses are akin to a computer AIDS epidemic and no less malignant or costly to our society.

The potential damage that uncontrolled virus propagation causes cannot be overstated. The first viruses were recognized in 1985 with only a handful making an appearance. By April of 1991, an estimated 521 viruses were identified, and by mid June, of this year over 900 have been identified.

Some of the statistics are truly astounding.

* Experts in the Virus-Busting field claim upwards of 12 new computer viruses are being introduced every day, and that number is growing.

* Every network with more than 10 computers attached contains at least one virus.

* By 1995, there will be over 100,000 active computer viruses spread throughout our computing systems.

* Every computer in this country will be infected with at least one virus by 1995.

Considering the kinds of damage that viruses can cause, we need to take the threat seriously. Because viruses were not taken as a serious threat in 1987, the CSA does not specifically address them as concern, but the figures support additional attention:

* An estimated $116 million was spent to repair the damage caused by the Morris INTERNET WORM incident of 1988.

* Industry spent in excess of $100 million to mitigate the effects of the well anticipated "Columbus Day Virus", aka "Data Crime", of 1989.

* Congress itself was hit with a virus which cost taxpayers over $100,000 to repair. All for not having adequate security installed.

Communications Interception

When we think of communications interception we normally think of phone taps, bugs and the proverbial 'being wired'.

In this networked society, though, the real problems are much more sinister.

* The telephone companies are under constant siege by hackers and others with an interest in compromising individual privacy. There are those who believe that the phone system interruption of January 1990 was the result of purposeful manipulation to make a political statement: it occurred on Martin Luther King's birthday. The phone company admitted that there was a software error which caused the disruption, they blamed errant programming code, but in either case we must recognize the vulnerability of public switched networks to compromise.

* Computer transmissions are made in a number of ways: modems, public lines, dedicated private lines, dial-up ports, direct connections etc. In virtually all cases, the data of those transmissions is wide open to eavesdropping using inexpensive and readily available line monitors. There are solutions to the problem, but little if anything has been done. In the case of civilian agencies, the IRS is a glaring example of potential compromise.

For example, the IRS uses tens of thousands of laptop computers by which field agents can access the central computers. Every single transmission they make, to retrieve taxpayer information or to scan the main computer's data base is absolutely susceptible to interception and unauthorized detection. In 1987, the IRS participated in demonstrations which showed how the protection of their data and the privacy of taxpayers could be effected. Since that date, no progress has been made in such protection, according to the IRS because of inadequate ADP and security funding.

Obviously, the average taxpayer would like to believe that the most private and personal information about him, his family and his business is properly protected from compromise. Unfortunately, that is the opposite of the truth.

FAX transmissions have become a staple of modern business activity, yet they too, are totally without any means of protection in most civilian government and private enterprises. In fact, some companies specialize in the manufacture and sale of FAX interception devices which are no more complicated nor expensive than the FAX machine itself.

The technical means to achieve adequate levels of information security and privacy protection are commonly available, if only we would use them. Or as the case of the IRS and other agencies illustrates, adequate legislative funding was provided.

In the meantime, we and our information resources stand naked to inspection by anyone with the desire.

Electromagnetic Eavesdropping

Electromagnetic eavesdropping is an under-publicized and under recognized threat to our information processing systems.

For less than $100, an amateur hobbyist can construct a device that permits him to listen in on another computer for distances of up to 2 miles!

Simply, every computer, or printer, or modem electromagnetically broadcasts radio signals that are ready and ripe for detection. This means that the so-called privacy afforded by walls and doors with locks is actually useless since the computer is indiscriminately transmitting its contents to the world. Every document printed out in any office may be simultaneously copied by the computer eavesdropper - undetected and undetectable, for he is using nothing more complicated than a radio receiver tuned to the computer's broadcast frequency.

The implications to privacy and security are staggering.

This phenomenon has been well known for over 40 years, and the defense community currently employs the TEMPEST program to electromagnetically protect information deemed worth protecting. The TEMPEST program is classified, and little if any effort has been made to popularize the threat to the civilian community and the private sector. Whether this restrictive policy has any true national security implications, or merely serves as a self perpetuating cover to permit continued domestic surveillance is unknown, but we cannot afford to overlook the fact that TEMPEST interception technology is now readily available and has been openly published in many popular media. It only seems prudent that defensive mechanisms be put in place to thwart a known and quantifiable threat to security and privacy.

Along the same lines, we need to recognize that keystrokes on a keyboard of any computer similarly broadcast the information being entered. This information ceases to be private or confidential the second it is entered into the computer. There is unfortunately no way to accurately gauge the magnitude of the current electromagnetic eavesdropping activities.

Perhaps the most visible example of remote keyboard interception is the ability to discover Banking ATM personal identification numbers and access codes to the unprotected repositories of almost 80,000 banking outlets. With up to $50,000 in cash stored in each ATM machine, there is a cash hoard of nearly $4 billion ripe for the taking. The opportunity and means for an organized effort at committing massive assualts against banking ATM's is here today.

Computer Guns and Computer Bombs

The last broad category of offensive computer technology is the computer equivalent of weapons of mass destruction.

HERF Guns stand for High Energy Radio Frequency Guns. For a few dollars and with a minimum of knowledge, a HERF gun may be pointed at a computer, or a communications system or a network and when 'fired', the system under attack will crash, thereby losing its current store of information.

Much like signal-jamming, HERF guns present a unique danger to information processing. HERF guns may be as small as a briefcase, carried and used incognito, or as large as required. They may be highly focussed at particular targets or may be omnidirectional, indiscriminately disrupting computer systems in all directions.

The following scenarios are well within the capability and budget of the amateur, much less the dedicated professional.

* Shoot a HERF gun at the same target every hour on the hour, effectively shutting down the target agency or corporation. Because the HERF gun represents an intermittent phenomenon, the ability to trace down the problem is drastically reduced - almost to zero. Special equipment and training is required to detect the interference, but the protective measures are simple and well known.

* From a highway overpass, fire the HERF gun at selected makes and or models of automobiles, causing the electronics of the car to cease functioning. Notwithstanding the chaos caused by creating thousands of simultaneously disabled vehicles, perhaps on the Beltway, the reputations of the car manufacturers affected would certainly suffer in the public perception.

To take the HERF problem to its logical conclusion, we can easily increase the power of the electromagnetic emanation and end up with what is referred to as an EMP-T Bomb. EMP-T stands for ElectroMagnetic Pulse Transformer, and the acronym EMP-T is quite apt, since that is what happens to a computer which is exposed to an EMP-T Bomb. It's contents are erased and the circuitry within it is actually destroyed.

An EMP-T Bomb is more complex than a HERF gun, but with new technology including portable lasers and high temperature superconductors, generating high amplitude pulses is a viable weapon which can shut down computer operations over vast distances.

Targets of HERF guns and EMP-T Bombs that would have profound effects on the economy include, for illustration's sake:

* Exploding an EMP-T Bomb in New York's financial district. Major banks, international traders and the Stock Exchanges would find that their computers simply no longer work.

* Traffic light systems can be brought to their knees.

* The Social Security System could be destroyed rendering payments impossible.

* Airplanes may be electronically disabled with disasterous consequences.

* The IRS could find itself without millions of necessary records with a single magnetic explosion.

* Law Enforcement computers could be so disrupted as to render them unusable.

* Insurance companies could find their computer networks permanently disrupted.

In short, strategically placed magnetic weapons of mass destruction to computers are capable of shutting down significant portions of the American economy.

Cumulative Effects of Computer Weaponry

Each of the described offensive weapons can by themselves have profound impact upon the Government's ability to continue public service, and as has been already demonstrated, can cost private industry untold billions.

However, we need to also examine the cumulative effects of these technologies.

No longer can we view the threat as merely isolated incidents by hackers or other disgruntled individuals. Since the described technology is now extremely inexpensive and available, we must consider the effects of a well organized, well financed and highly motivated group who might have reason to target any or all of the American infrastructure by attacking our computers, communications and networks.

There is no shortage of adversaries who might be pleased to see American pre-eminence diminish with a well coordinated successful assault. Getting into specific and likely adversaries is outside the scope of this presentation, however, we should paint a wide brush stroke and remain aware of potential enemies who wish Electronic Armageddon to befall us.

International Political Adversaries
International Military Adversaries
International Terrorists
Drug Cartels
Domestic Political Foes - High Tech Watergate
The recent Wilder-Robb conflict.

Lobbyists and Special Interest Groups
Popular Causes ie., anti-nuclear activists, etc.
Organized Crime
Corporate Espionage

What Congress Can Do

Simply put, it is the opinion of this author that Congress recognize the value of information, computer and communications systems to the continued viability of the United States as an economic leader and World Power.

Subsequently, Congress, perhaps under the leadership of this committee, must put forth diligent effort in the creation of a National Information Policy with several clearcut goals.

The theme that runs throughout the concept of the National Information Policy is an expansion of the scope and detail to an updated Computer Security Act that will truly serve the needs of this nation.

1. Establish a non-partisan National Information Policy Board to create criteria by which the relative value of information and information systems can be gauged with respect to disclosure, destruction from both a security and a privacy vantage point. Business and Government need to work together to find real solutions to real problems.

2. Redefine what the Government means by sensitive but unclassified, confidential and other data classification levels to take into account the privacy concerns of American citizens.

The media has often described what can be referred to as Classification Chaos. There is a portrayal that the Government overclassifies its files and data for a variety of reasons, and thus sustains a monolithic over-seeing bureaucracy to control the system.

Today there is good reason to pause and question what we mean by classification. There are grades of security imposed on certain types of data; those classification ranging from sensitive but not confidential, confidential, secret, top secret and the like. We understand and generally accept the fact that military secrets are to be protected as are international negotiations and other similarly sensitive data. Thus, when such data is classified as top-secret, we do not flinch.

However, what classification of data do we attribute to the tax returns of a hundred million Americans? Or the contents of their census information? Or criminal records, or any of hundreds of other data that is deemed and assumed by the public to be held securely and safely, away from prying eyes. Unfortunately, that is not the case. where the opposite is more close to the truth.

3. Define criteria by which information held in private computing networks should be protected. For example, what is the fiduciary responsibility of the private sector to protect the information it has collected on its customers or other individuals or corporations?

The legal questions brought up by the concerns over privacy are litigations waiting for a reason to rear their heads. The first wave of electronic privacy suits has already surfaced, and it is only a matter of time before the legal problems put us in the middle of fourth mmendment analysis of electronic privacy.

4. Recognize that as computer technology advances, so does security technology and the threat to our systems. The criteria must be flexible enough to be adjusted as new offensive computer technology threatens information systems. We must recognize and accept the threats by internal domestic forces and external organizations, and the kinds of damage that can be done by well coordinated organizations using available technology.

5. Establish a formal relationship with the international security community such as the ITSEC group.

A group of 4 European countries, England, Germany, Belgium and the Netherlands have formed a security alliance to define their security criteria by which their countries' computers will be secured. While there has been some levels of contact between NIST, NSA and the ITSEC group, the United States has yet to be forthwith regarding any involvement in international security standards.

To demonstrate just how crucially the European community views their information security and privacy, their proposed information protection regulations may well prohibit multi-national corporations from electronically moving certain information from one country to another. It is entirely feasible that if the Europeans continue this trend, and the United States remains segregated from the international security community, that this country could be electronically isolated from other parts of the world. All because we won't secure our data.

I am certainly not qualified to gauge the economic effect of such an occurrence, but I can say, with 100% assurity, that the current international security policies of this country do not in any way promote cooperation, and are a hindrance to the export of American technology. Indeed, our position may be even more shortsided. In many ways it can be said that the independent ITSEC effort was born by our steadfast refusal to jointly participate with the European community in developing internationally acceptable security criteria. As a result, we see that American technology is being bypassed in favor of new technology developed by the participating members. For all intent and purposes, we may have locked ourselves out of the European security market for good.

As one British security expert said, and I paraphrase from memory, "you (the Americans) have made it impossible to do business with us, so we'll just go out and bloody well do it ourselves."

It certainly appears, and a good argument can be made that this endemic isolationism does not bode well for America's technical leadership in this decade.

6. Bring current export controls more in line with the reality of the technology available world-wide.

Conflicting procedures and regulations for the export and multi-national use of security technology is hindering international security cooperation.

The National Security Agency, for example, has increasingly tight restrictions on the export of technology using DES, the Data Encryption Standard, which is heavily relied upon by the Dept. of Treasury, Federal Reserve Board and is used for Electronic Funds Transfer. In addition, DES is used as a de facto standard for encryption and thus the protection of data transmissions and storage of computer data.

The conundrum is simple.

DES is a public domain algorithm. available to anybody with a 29 cent stamp and the address of the National Institute of Standards and Technology. As a result, DES based encryption systems are now made in many European countries, rather than being imported from the United States.

Some skeptics believe that the NSA should have little concern since DES will be used with or without their approval, but at great cost to the export economy of this country. Others maintain that the NSA can crack DES encrypted files and is merely preventing export for political clout. This argument may carry come weight since they have prohibited the export of a modified DES technology called infinite encryption.

The influence of the NSA on cryptography is clearly evident in their handling of public-key encryption. The RSA algorithm has, too, become an almost de facto standard for protecting electronic mail from unauthorized snooping. Yet the NSA has refused to endorse it, give a reason why, or to offer a reasonable alternative.

With the advent of multi-national laws, especially among the EEC countries, that mandate privacy protection for the data held on their citizens and companies, the United States has yet another worry. European officials are considering restricting the legal transfer of data from EEC countries into the United States unless this country can adequately demonstrate concomitant protective measures.

At this juncture we are sadly behind the eight ball.

7. Create effective national legislation to prosecute computer crimes of all natures under a single banner designed exclusively for that purpose.

The issue of state's rights is one that should not be raised, even though 49 of the 50 states do have some sorts of computer crime legislation. Computer crime is truly of national interest and because the networking of America lends itself to inter-state computer criminal activities, they must be addressed on a centralized level.

The issue becomes quite clear when we look at the Hanover Hacker incident as portrayed by Clifford Stoll in "The Cuckoo's Egg". Tracking down the German hacker who invaded hundreds of civilian and military computer systems was severely hampered by the requisite and conflicting procedures by the states whose boundaries the hacker crossed daily.

In closing.

Mr. Chairman, I recognize that there are a multitude of issues to be considered, and that in this short time I can only cover the fundamental concerns in a most cursory fashion. However, I hope that this brief introduction to the problems of information security and personal privacy will persuade this committee to further the work they have already begun and expand the scope and purport of the Computer Security Act of 1987 to include the evolving threats to our security and privacy.

We must remember that technology marches on, and unless we react soon, we may find ourselves on the precipice of an Electronic Pearl Harbor.

I thank the Chairman and the members of this committee for their time.

If there are any questions, I will be happy to answer them to the best of my ability.

Submitted by

Winn Schwartau
Executive Director,
INTER.PACT

Mr. GLICKMAN. Mr. Walker?

Mr. WALKER. I, too, thank you for the opportunity to speak here this morning. I'm here as a member of the National Research Council panel that produced the "Computers at Risk" report, and I'm also here with observations from my membership now with the Computer Systems Security and Privacy Advisory Board, the board that was created by the Computer Security Act of '87. I have been a member for one meeting, but at the last three meetings, and I have several things I've observed from that I'd like to share with you.

I want to say first off my opinions here are my own. They're not the National Research Council. They're not necessarily those of other people on the panel or on the Advisory Board.

In my written testimony I gave a brief description of the problem. Winn has done a very good job of that, as have others. I would like to emphasize that the first problem with computer security is management. It is, if management cares that sensitive information or any other management issue be attended to, it will be attended to. If they don't care, it won't. And I think a very strong tribute to this subcommittee and its predecessors, for your continued diligence in pressing for computer security within the Federal Government is attributable to much of what has in fact happening. Now, more could happen and we would like more to happen, but please don't relax. Keep it going. Because if you don't, then others will view that management doesn't care and it will drift away.

Of course, computer security is a physical, procedural, administrative problem. You must adequately protect. If you have something that is very important, you better lock it up. And it is a technical problem only lastly, in the sense that if you do not do the physical and procedural things first no amount of technology is going to help you. On the other hand, if you have done the physical and procedural and administrative things, if you have taken care to lock your doors and all, but you now have linked your computer with telephone systems that are around the world, you're wide open, and only technology solutions will help you there.

We're really focused heavily on the technical solutions. The physical administrative things are reasonably well understood, although as demonstrated by others in this hearing, not necessarily well practiced.

I want to say something about the issue of sensitive information. I was at the hearing here about 4 years ago when the issue first came over, unclassified sensitive information, and I heard all the rumblings about, What do we mean by sensitive? Well, this stuff is sensitive but that isn't sensitive. And I thought at the time, maybe instead of saying sensitive we should call it important, unclassified/important. If it's important to someone for some period of time, then it should be treated as sensitive and it needs to be protected. If it's not important to anyone, then you have to wonder why do we have it—except there is information we want to give out to everyone that doesn't need any kind of protection.

But the NSTAC report that Herb is going to talk about talks about some of the issues that, where hackers can, in fact, do bad things to the phone system. And, of course, yesterday was a perfect

illustration of the kind of problem that can happen, and never mind that it wasn't done by a hacker.

There is another issue that I remember from my days at the Pentagon. It is the perception of the problem. We suspect that bad things can happen and therefore we do not use our information systems nearly as well as we could. In the military, in the WWMCCS—Worldwide Military Command and Control System—only 10 percent of the data in that system is Top Secret, and yet the system is run as a Top Secret system-high system, with everyone cleared to that level because we perceive there's a problem and we're afraid something might happen. We separate our accounting and our payroll and our personnel systems because we're afraid that if we link them together some sensitive information might be lost. So, we're actually hurting ourselves not only by making information vulnerable, but we're not using the systems as effectively as we could, simply because we're afraid of other things that may go wrong.

I had the opportunity starting about 2 years ago to join a panel of experts, industry and academia, taking a broad look at the computer security problem. This was a group put together by the National Research Council. It was sponsored by DARPA. But we quickly expanded our realm to what's the problem in the government and in the commercial sector, because many of the problems are the same and the solutions need to be able to be used by all.

In my written testimony I talk about the various recommendations. I strongly recommend this report as a—the best compendium of the problem and what to try to do about it since the Willis Ware report of 1970, which in itself is still a valid report. There were two major things that came out of the report and an awful lot of very good suggestions. One of them was that we need to put together what the report came to call the Generally Accepted System Security Principles—the GSSP. This was an attempt to take all the little checklists and gatherings of information about what the problem was and bring them together in one cohesive whole. There's a lot of work going on, a lot of things that can be brought together. They need to be there, not just for the Federal Government, not just for General Motors, but for the "mom and pop" grocery store. What should they worry about as they worry about sensitive information?

The GSSP was a major recommendation. The second one was the Information Security Foundation. The panel labored at great length with the issue of how do we get on with making these systems more available to the government and to industry. And we concluded at the time, not trivially, that neither NSA nor NIST were up to the job as they are currently constituted. That even if they did the job perfectly, by law and by attitude if not desire, they can't solve the problem for the commercial world. They may be—NSA is probably going to be able to do a fine job for the national security world. NIST could do a better job for the civilian government world. But neither of them are going to solve the problem for the commercial world.

And so we came to the conclusion that what was needed was an organization, private sector, able to work closely with the government to establish the GSSP and to establish mechanisms by which

evaluations of security-related products could happen. A lot of vendors like the idea of just let me give an assertion that this system is good enough. Vendor assertion it's called. The government can't accept that. You need to have an outside opinion. The Europeans have established mechanisms by which they have commercially licensed evaluation facilities that do this kind of activity. We need more of that. The government isn't going to be able to do these evaluations itself, and we need to find some ways like the British have to do a better job at this.

In the midst of all this there is a growing problem of individual agencies and commercial organizations establishing their own evaluation mechanisms and their own accreditation mechanisms. I know of at least a half a dozen government agencies that are striking out on their own. NSA hasn't produced enough in their evaluated products list. NIST hasn't really done anything to help this. And so these agencies are saying, "I've got to solve this problem. I'll do it myself." What's going to happen is there's going to be 5, 25, 50 different criteria for evaluating systems within the next 3 to 5 years.

Various of the vendors are upset that there is an NSA criteria and a European criteria and a pending NIST criteria. I have stated to them, "We're going to look back in a few years that this is the Golden Age when there were only 2 or 3 criteria. Soon there will be 15, 50 of them and there will be real significant confusion". That's a major problem that is rapidly coming upon us.

The NRC report received rave reviews back in December. They decided to call a follow-on meeting in May and there were a large number of people, 70 or so folks there. It was interesting, those of us on the panel thought the ISF was an idea that—well, that's great. It'll go on the shelf. We were gratified to hear that there were at least 3 organizations at that May meeting that were interested in making an ISF happen. This is intriguing. There are a lot of problems with it, as those who wish to do it are now grappling. At the June meeting of the Computer Systems Security and Privacy Advisory Board, an impossible name, we discussed the ISF and the question came up from the panel members, Why can't NIST do this? Why did the panel come to the conclusion that NIST is not up to this job?

Well, we went down through the list of the reasons that we saw up to now and there was much discussion, including some that happened after the meeting, that—and there was some interesting insight which I thought would be useful for your considerations today.

We came up with 3 factors that, if there were to be a shift in the positions of various organizations, maybe NIST could do it. And we came to the realization that if NIST could do it, if we could do this somehow within the structure of the government instead of having to set up a private organization with all the funding and personnel and conflict of interest and "how do you talk to the government" issues associated with it, that something significant could happen, if, in fact, NIST could do this.

With the factors that we detected, and I sort of felt like, you know, there were several rocks that were pressed against each other and wouldn't move, and then suddenly there was a shift. One

of them is that if the definition of NSA's role in evaluating systems and NIST's role could somehow be clearly defined so that they could operate without having to trip over each other all of the time, and the idea that was put forth—and I don't know whether this is really possible, but I think it's something that really needs to be considered, is that NSA shift their interest from the whole spectrum—I'm going to use orange book terms now, C–2 to A–1, C–2 being the bottom and A–1 being the top. If NSA were to shift their focus to the higher end of trust, which is what the national security community really needs anyway, and what their—well, what they are best acclimated to do, and if they were to relinquish the responsibility for evaluating C–2 and B–1, low-end-type systems, to NIST, that's what the commercial world and what the civilian agencies and the national security agencies that deal with unclassified information need. If we could define that NSA's role was at the higher end and NIST's role was at the lower end, then that would get them out of some of this logjam that they're in.

The second factor that was important to follow this is that NIST has not wanted to do evaluations since my first discussions with them back in 1980 on this topic. But there seems to be a shift to, say, under this National Voluntary Laboratory Accreditation Program—NVLAP—that if the evaluations could actually be done under the auspices of NVLAP using FIPS guidelines that would come from NIST that this may be an acceptable position for NIST and something that the industry could work with.

The third factor, of course, in this, an NSA shift in mind-set, a NIST shift in mind-set, we need an industry shift in mind-set to actually accept these things. If this was an approach that we could do, if industry would accept it, then, in fact, those three things might actually cause a significant change. I'm concerned that unless something like this shift occurs that we're not going to have that kind of a change.

The advantages, of course, over a private organization—I'm now arguing in some sense against what we recommended in the report. I mean NIST already exists. It already has at least some funds and could get more. It has some staff. It needs more. But it also has the ability to interact with users and vendors of systems with the U.S. Government agencies and with the international community. I mean it already has all of those. And, if we set up a private organization and try to empower it with this somehow, I can see us here 5 or 15 years from now wondering whatever happened to it.

A major point in this is that we are facing a crossroads right now. We have a suggestion made by a group of folks that seems to make sense to a lot of people. There's a lot of folks out there who want to make an ISF happen of some sort. It's either going to happen as a private organization in which the government is going to have to have interaction, or it's going to happen with NIST and NSA working together to make it happen, or we're going to find ourselves with multiple evaluations. I mean, if one or the other of those first don't succeed, we're going to find ourselves with each agency and each large organization in the commercial world doing their own evaluations to their own criteria, and we'll see very little progress.

I had a set of recommendations in my testimony and I wanted to summarize them. First, on the ISF, I suggest you watch it closely. It's hard to watch it closely because it's moving real fast, but—and that you encourage NSA and NIST in thinking about the shifting in their roles to find a way that they're not bumping up against each other all the time, but in fact can both make progress.

It is my belief, having been on the NRC panel and having watched the debates happen, that if NIST could do this job, if we could find a way for NIST to do C–2 and B–1 criteria development and the NVLAP program to do the evaluations, that that's better than a private sector initiative. That's my own personal opinion. But, if NIST does this, I would like to encourage you to have them do it. If they don't, let me encourage you to encourage a private sector initiative. Because we've got to do something. We can't have the chaos just going on.

Once it's established, whatever it is, the government is going to have to work with it. If it's a private sector initiative or if it's something done by NIST and NSA, we're going to—you're going to have to keep encouraging people to participate in it.

The NRC panel had some things to say about cryptography. It was a difficult topic because we had a broad range. As Marjory Blumenthal will say, the NRC goes to great length to get a spectrum of people. So that if it says anything at all, it's a good consensus. The NRC panel was upset about the DES situation and the fact that there's export control on DES, and what we said was we believe there should be a high level panel that contains both government and industry representatives, properly cleared to hear all sides of the subject, that can decide whether or not it really makes sense for the data encryption standard to be subject to export control any further.

I concur completely in that recommendation. I would like to go further, though. What we need is an exportable, publicly available private key and public key encryption algorithms. We need them now in this country. We keep talking to NIST and NSA, and they keep saying, "We're going to produce one pretty soon. We're going to produce one pretty soon." It can be DES, the private key version, but it doesn't have to be. If people are so worried about DES that they want to define something else, let them do it. But please do it. Don't just keep promising it forever.

The same with public key. It doesn't have to be RSA, but if it isn't, it has to be something that provides protection both for confidentiality and integrity. And, if we had had these 5 years ago, I believe we would have a significantly available set of products with encryption as a basic premise within them, built in.

As long as we don't have exportable cryptographic algorithms, we're not going to have those products. We're going to have a few specialized things that people will have to jerry-rig to use. Only when we get exportable versions of these algorithms, whatever they are, will we be able to see the kinds of privacy protection and the kinds of data protection of sensitive information that in fact we really deserve.

Mr. GLICKMAN. Can we ask you to kind of finish up?

Mr. WALKER. Sure. I'm almost done.

Mr. GLICKMAN. OK.

Mr. WALKER. On the issue of export of trusted systems, the NRC panel said don't use the orange book levels for export control. The present idea of a B–3 and above system is one that's arbitrary a number of years ago. There is no technical basis for it and it's preventing industry from building the best systems that they can, and that's a serious problem. I would encourage you to keep them from doing that.

In my testimony I make some discussions about sensitive information handling and how we ought to label things. The Canadians have a system they've had for about 5 years now that labels sensitive information A, B, and C. Simple structure. We've heard on the Advisory Board about the struggles of the government agencies with trying to do this. There are 27 agencies involved in the law enforcement area that are tripping over themselves trying to come up with ways to protect sensitive—to label and protect sensitive information. I think we need a framework for doing that. I suggest the Canadian one is a good idea.

And my last comment was simply to encourage the visits that OMB, NIST, and NSA are having with government agencies, and I think it's, in fact, doing a great deal of good at raising to high levels of management the nature of the computer security problem.

Thank you for the opportunity, and I'll be glad to answer questions.

Mr. GLICKMAN. Thank you.

[The prepared statement of Mr. Walker follows:]

TESTIMONY

BY

STEPHEN T. WALKER
PRESIDENT
TRUSTED INFORMATION SYSTEMS, INC.

FOR

SUBCOMMITTEE ON TECHNOLOGY AND COMPETITIVENESS
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
U.S. HOUSE OF REPRESENTATIVES

JUNE 27, 1991

I am pleased to testify at this hearing on the status of computer security in the Federal Government. My focus today is on the findings and recommendations of the National Research Council (NRC) report *Computers at Risk*, a report of the panel on which I was a member, and observations that I have on the overall status of computer security in the Federal Government from my perspective as a long-term participant in this field in both Government and the private sector and from my new position as a member of the Computer Systems Security and Privacy Advisory Board established by the Computer Security Act of 1987. My comments are my own opinions and do not necessarily represent the opinions of the National Research Council, the NRC panel of which I was a member, or the Advisory Board.

In my testimony, I will discuss the nature of the computer security problem, summarize the findings and recommendations of the NRC panel report, describe some of the activities that have taken place since the report was published last December, and make recommendations on actions which this Subcommittee might consider taking in the future to accelerate the inclusion of computer security in Federal programs.

WHAT IS THE PROBLEM?

Like so many other issues today, computer security is first and foremost a management problem. If management cares about protecting its sensitive information, it will be protected; if not, it won't. This is true for large corporations, for "Mom and Pop" grocery stores, and for agencies of the Federal Government. The improvements in awareness of the computer security issues and quality of information security protection within the Federal Government are directly attributable to the diligence and perseverance of this Subcommittee and its predecessors.

Computer security involves physical, procedural, personnel, and administrative measures, all of which must be balanced to provide adequate protection at an affordable cost. Every

security measure costs something, some very little, others prohibitively much, and no single measure or combination of measures will provide perfect security.

One must be able to identify what is important (sensitive) in order to know what to protect. One must be able to identify what is important by stamping words like "IMPORTANT" on the document or file, so that others will know how to treat it. I would like to propose that we drop the "unclassified/sensitive" terminology and adopt "unclassified/IMPORTANT" to emphasize that if information is important to someone, even if only for a short time, it deserves to be protected. I will say more on this later.

Computer security is "lastly" a technical problem. I say "lastly" because one cannot substitute technology for the other protection measures. If one does not have adequate physical, procedural, personnel, and administrative security measures, no amount of technology can help. Attempting to substitute technology for prudent management procedures is wasteful and dangerous. On the other hand, once adequate procedural measures are in place and one begins to employ advanced technology for information processing, technical security solutions must be added to the physical and procedural measures already in place. No amount of physical, procedural, or personnel measures can protect against a hacker breaking into a local area net of workstations linked to an international complex of wide area nets. Today, any link beyond your local computer should be assumed to be connected to the rest of the world because it probably is.

The National Security Telecommunications Advisory Committee (NSTAC) Network Security Task Force report that Herb Benington will describe during this hearing is a disturbing view of what can happen to our public switched telephone network if organized adversaries attempt to disrupt service. The problems outlined in that report are symptomatic of the problems faced by all such networks from the stock exchange to large commercial networks to FTS2000 and Congressional electronic mail systems.

As long as computer systems, whether they are personal computers or mainframes, can be physically isolated and protected from external access (just as with papers locked in file cabinets), the computer security problem can be limited to a physical and procedural level. As soon as we link computer systems together in any way, a wide spectrum of vulnerabilities arise and, depending upon the sensitivity of the information, the threats can be very substantial.

If information, whether stored on a computer or not, is important to someone for some period of time, then it should be considered sensitive and afforded appropriate protection. Agricultural crop reports are highly sensitive until they are released and then they become public information. Agencies that maintain proprietary information on commercial products either in existence or under development must protect the information of each company from its competitors. Organizations that maintain personal information concerning one's health or financial status have similar problems. Organizations, be they Government agencies or

corporations, that deal with future planning, budgets, new initiatives, cutbacks, all must be concerned with the disclosure, modification, or destruction of that information.
These issues are not new. Government and business have coped with them throughout history but as computers and particularly computer networks have entered the scene, the volume of information has increased, the desire to share portions of the information with others has increased, and the problems of understanding how to control that sharing have proliferated, often out of control.

Hackers on computer networks are serving as harbingers of what is to come. Our networks are so complex and diverse that what may look like a simple telephone link may expose one's information to worldwide threats.

In addition to the actual threats posed, there are the limitations that we place on ourselves through the "perception" of a problem. Many corporate executives have said, "I don't use electronic mail for anything important because I don't know who can read it." We build duplicate systems and fail to connect important users to our systems because we are not confident that important information can be adequately protected. In the military, the Worldwide Military Command and Control System runs at TOP SECRET with all personnel so cleared even though less than ten percent of the data is TOP SECRET. In the civilian government and business, we use isolated systems for accounting, payroll, finance, and other sensitive planning functions. We are so used to this situation that we often don't recognize how much we are limiting our ability to use information systems or how much it is costing us.

Simply stated, if we could only avoid putting important (sensitive) information on our computers or if we could avoid sharing information with users on other systems, our computer security problems could be limited to traditional physical and procedural concerns. As soon as we link our systems containing important (sensitive) information, we introduce a complex set of vulnerabilities that cannot be avoided.

COMPUTERS AT RISK

In the spring of 1989, the National Research Council organized a group of experts in the computer security field from academia and industry to conduct an 18 month broad look at the status of computer security. The study was funded by the Defense Advanced Research Projects Agency, but the topics considered included the full needs of the Government and the private sector. The *Computers at Risk* report was published in December 1990 and has become a best seller. It has been recognized by many as the first major work in many years to identify the problems of modern computer security for the Government and the commercial sector and suggest comprehensive and practical measures to make major improvements in the availability of computer security solutions. This report ranks along with the original Willis Ware Defense Science Board Report of 1970 in describing the nature of the problem and alerting us both to the concerns and the solutions which may be available.

The *Computers at Risk* report identifies many of the problems inherent in this complex field and makes specific recommendations on what to do about them. It contains six major recommendations which cover the spectrum.

In its first recommendation, the panel states, "there is a basic set of security related principles for the design, use, and management of systems that are of such broad applicability and effectiveness that they ought to be part of any system with significant operational requirements." The panel recommends that these basic principles be brought together in what they call the Generally Accepted System Security Principles (GSSP). The concept, which relates to the Generally Accepted Accounting Principles that have guided the financial community for many years, is to identify basic security issues that organizations ranging from Government agencies, large corporations, and small independent businesses should take in to account as they develop sensitive information handling capabilities. There are many activities currently underway within Government and the commercial sector to identify principles such as those envisioned for the GSSP. The goal of this recommendation is to bring together the results of these activities in a comprehensive document which could be used by individuals and organizations to recognize the breadth of their information security problems and determine what steps are needed in their own particular situations.

The second recommendation specifies a number of short-term actions which both computer vendors and users can take today to yield immediate benefits. The third recommendation concerns the establishment of a system incident repository and education and training programs to promote public awareness of the computer security problem.

The fourth recommendation is specific to export control issues with respect to both cryptography and trusted systems. The panel recommends, "the administration appoint an arbitration group consisting of appropriately cleared individuals from industry and the Department of Commerce as well as the Department of Defense to impartially evaluate if there are indeed valid reasons at this time for limiting the export of DES [Data Encryption Standard]." The panel also recommends, "Orange Book ratings not be used as export control criteria." The fifth recommendation supports a comprehensive research program to resolve the major technical issues involved in the computer security field.

In its final and most important recommendation, the panel makes a strong case for establishment of a new organization to "nurture the development, commercialization, and proper use of trust technology." This organization, referred to as the Information Security Foundation (ISF), would carry out many of the preceding recommendations, in particular the establishment of the GSSP. The ISF is envisioned to be a private, nonprofit organization with close affiliation to the Government. The panel spent a great deal of time analyzing the present situation in Government to determine if there was any way the Government itself could carry out this function and, after much deliberation, the panel concluded that something significantly different than the present NSA/NIST structure was needed if we were to succeed in significantly improving the availability of computer security solutions for the Government and commercial sector.

The panel recognized that there would be significant complications in establishing a new organization to perform the functions envisioned for the Information Security Foundation. The difficulties of creating a nonprofit corporation, obtaining near- and long-term funding, establishing a credible management structure and technical staff, and defining relationships with the U.S. Government, in particular NSA, NIST, the European governments, as well as user groups and vendor groups were all viewed as almost insurmountable. It was also recognized that there would be difficulties with the new organization competing with existing organizations which either do or could do at least a portion of the functions envisioned for the ISF. The general conclusion was that no existing organization, either Government or private sector, as presently established, could perform all of the functions envisioned for the ISF and thus the panel recommended that a new organization be established.

ACTIVITIES SINCE *COMPUTERS AT RISK*

In discussions that have occurred since the publication of the NRC report, the actual functions of the ISF and its relationship with existing organizations have received a great deal of attention. If the ISF is to establish and maintain the GSSP and evaluate products, it would necessarily compete with many existing organizations both for technical staff and in many direct activities. From this analysis, the notion that the ISF would be more successful as an "enabling" organization rather than a "doing" organization has emerged. If the ISF could facilitate the establishment of the GSSP and endorse specific organizations to perform evaluations of products rather than performing the evaluations itself, the competition for technical staff would be reduced and the activities of existing organizations could be enhanced through ISF endorsement. This "enabling" concept has gained fairly wide acceptance as a basis for how the ISF should function.

While this discussion of the ISF has proceeded, many Government agencies and commercial organizations are setting up their own capabilities or hiring outside help to accredit their sensitive information handling systems. There are at least a half dozen Government organizations actively pursuing such activities with many more watching how these go. Once these accrediting organizations establish their criteria for evaluation of systems for their own use, those people who now complain about the confusion of having NSA and European criteria and the potential emergence of additional NIST criteria, may look back on these times as the golden days when there were only two or three criteria instead of the fifteen or fifty criteria that we may have within the next five years.

As a follow-on activity to the publication of the *Computers at Risk* report, the National Research Council sponsored a meeting in May to discuss the findings of the report and to see what if anything could be done to foster the endorsement of its recommendations. At this meeting, three groups expressed interest in establishing an Information Security Foundation. The meeting had the flavor of the ultimate New England Town Meeting. Everyone spoke, but there was no one in charge to make a decision on how to proceed. At the conclusion of the meeting, it was agreed that a subset of the people there would meet in June to discuss potential functions for the ISF and how it should be organized.

At the June meeting of the Computer Systems Security and Privacy Advisory Board, there was a discussion of the Information Security Foundation and the question "Why doesn't NIST do this?" was again raised by the members of the Board. The advantages of having NIST perform this function, the fact that NIST is a Government entity, that its charter is currently almost adequate, that it has at least limited funding sources and staff already in place, that it has the ability to deal with vendors, users, agencies of the U.S. Government, and the Europeans, all argue strongly in its favor. Unfortunately, even with these advantages in place, without a change in the current environment both inside and outside NIST, the NRC panel's conclusion that the ISF functions could not be performed by NIST, remains.

Much discussion among Board members and others followed concerning what it would take for NIST to be able to have a more direct role in performing the ISF functions. Three factors emerged. The first was the need for a clear separation of functions between NSA and NIST. An example of one workable relationship would be for NSA to focus on the evaluation of systems at the higher levels of trust (B2 and above) while NIST concentrated on lower levels of trust (C2 and B1). The second factor was that the role of evaluating the lower level systems needed to be handled by an activity that was related to but independent from NIST. An example of a potentially workable approach was the use of the National Voluntary Laboratory Accreditation Program (NVLAP) to sponsor the actual product assessments against Federal Information Processing Standard (FIPS) Evaluation Criteria that NIST would promulgate. The third factor that was deemed essential for NIST to play a more direct role was that industry be willing to cooperate with and endorse such evaluations.

At the conclusion of the discussions at the Advisory Board meeting, there was reason to hope that new developments in all three of these areas could occur, each dependent on the other.

Thus today, we find ourselves at a significant crossroads in the computer security arena, one that will impact the ability of the Government and commercial organizations to protect sensitive information in fundamental ways. On one hand, we have several activities looking to create an Information Security Foundation as a private, nonprofit organization. One or more of these activities may find sufficient support to create such a capability and to accomplish what the NRC panel report recommended. On the other hand, through a shift in Government and industry perceptions, it may be possible for NIST to perform many of these same activities recommended by the NRC panel. If neither alternative occurs, it is virtually certain that the proliferation of multiple accreditation activities by Government agencies and commercial organizations will create far more confusion in the next few years than anything we have observed to date.

RECOMMENDATIONS

Information Security Foundation

It is my recommendation that this Subcommittee should stay closely attuned to the developments of both the ISF evolution and the potential for increased Government activities in this area.

The need for action in all areas of the NRC panel recommendations and the confusion over the growing number of independent evaluation and accreditation efforts warrants careful scrutiny by everyone. This Subcommittee is perhaps the only place in Government with oversight of the complete spectrum of activities. Your continued interest will have a strong, positive influence on how this process proceeds.

Given the complexities of establishing a new organization and assuming that the changes in the Government approach discussed at the Advisory Board meeting have some likelihood in occurring, I personally favor the Government approach to that of establishing a new private sector organization. I recommend that the Subcommittee encourage NIST and others in the Government to proceed along these lines. If a Government approach does not materialize in the near-term, the Subcommittee should be prepared to support private sector Information Security Foundation developments. It is very important that Congressional support be given to whichever approach emerges so as to assure widespread Government concurrence.

Export Control of Cryptography

I would like to comment on the recommendations of the NRC panel on export control. The continuing lack of publicly available, exportable cryptographic capabilities is perhaps the most serious impediment to the protection of important (sensitive) information in the United States commercial and Government activities. I fully concur in the NRC panel recommendation that a National Security Council level arbitration group consisting of individuals from industry and Government knowledgeable about the national security issues and the negative impact that the lack of cryptographic solutions is having on protecting sensitive information within the United States should be established.

The immediate need for publicly available, exportable private key and public key encryption algorithms cannot be over stressed. The apparently endless debate over suitable encryption capabilities for unclassified/IMPORTANT information continues to subject large quantities of commercial and Government sensitive information to substantial risk of loss or modification and causes the United States to fall further behind in technologies that we used to lead. The private key algorithm need not be the Data Encryption Standard, but if it is not, many will wonder why not. The public key algorithm need not be RSA, but some public key capability is needed now for providing both integrity and confidentiality protection. If the Government cannot decide on the use of DES and RSA as exportable, publicly available algorithms,

alternative algorithms must be approved very soon. I recommend that this Subcommittee press with all available energy for exportable, publicly available encryption algorithms now.

Export Control of Trusted Systems

On the issue of export control of trusted systems, I wish to restate what I emphasized last year in my testimony. The current policy of drawing the line in the middle of the Orange Book criteria layers is an arbitrary policy which is seriously hurting the ability of the United States to protect its own sensitive information and to get high quality computer systems. I fully concur in the recommendations of the NRC panel that Orange Book criteria should not be used as a basis for establishing export control measures. Trusted systems for running on special purpose or high performance computers should be considered for restricted export on the basis of the special purpose of the computer and not the existence of a trusted system.

I recommend that this Subcommittee encourage revisions of the present export regulations to eliminate trusted system criteria as a basis for case-by-case export review.

Sensitive Information Labeling

Among the deliberations of the Computer System Security and Privacy Advisory Board, there has been considerable discussion of the issue of labeling sensitive information. Since this Subcommittee is particularly interested in the protection of unclassified/IMPORTANT (sensitive) information, this should be a topic of considerable interest. The Advisory Board has heard from a number of executive branch organizations that are struggling to come up with bilateral agreements for commonly accepted labeling mechanisms for sensitive information. The law enforcement community, some 27 plus agencies, described their efforts to protect information about informants where loss of critical information could effect the lives of individuals.

The present trend is to establish a series of bilateral agreements between agencies governing how information will be handled. The number of these bilateral agreements is growing rapidly, and it is becoming more and more difficult for people to comprehend how to label information let alone what protection to afford it. In the middle of this confusion, we heard a presentation on a straightforward Canadian Government unclassified/sensitive labeling initiative that has been law for about five years and is transforming the way they deal with sensitive information labeling. They have three levels of labeling for unclassified/IMPORTANT information: PROTECTED A, B, or C, with C being the most important (sensitive).

Having observed the confusion among various U.S. agencies in this area, I became convinced that a simple framework such as the Canadian approach would greatly assist individual agencies as they establish agreements among themselves for protecting their unclassified/IMPORTANT (sensitive) information. The framework need not be complex; its adoption need not be costly. The guidance should be that in the future as agencies develop

important (sensitive) information labels, they should use this framework. There is no need for extra money to retrofit old systems. In five, ten, or fifteen years, we will find ourselves with most of our important (sensitive) information already labeled in simple categories which will make agreements among agencies much easier to establish and enforce.

It is interesting to note the parallels between the Canadian PROTECTED information structure and the traditional classified information structure. People say that the national security community has a major advantage because it already has a labeling system in place and that civilian organizations have trouble defining what they mean by sensitive information. In reality, the definitions of CONFIDENTIAL, SECRET, and TOP SECRET are exceedingly vague and ambiguous. What has happened is that there are three levels of classified information that have been used over a period of years and have gained common labeling and handling procedures among agencies handling classified information. If we are serious about protecting unclassified/IMPORTANT (sensitive) information, we should create a simple framework to identify degrees of important (sensitive) information which will, over time, allow agencies to establish reciprocal protection agreements in a straightforward manner. I recommend that this Subcommittee investigate the possibilities of such a framework and, if necessary, prepare legislation to establish such a framework Government-wide.

OMB, NIST, NSA Visits to Government Agencies

I have one final comment relative to my observations on the Advisory Board. We have heard recently about the agency visits that OMB, NIST, and NSA are performing in a "second phase" of the activities prescribed in the Computer Security Act of 1987. It is my observation that these agency visits are having the significant positive impact of raising the level of awareness of senior management in a constructive way to the vulnerabilities to which their information systems may be susceptible. I recommend that this Subcommittee encourage OMB, NIST, and NSA to continue these visits on a periodic basis to reinforce the concern of Congress and the Administration that computer security is an important concern in the Federal Government.

I appreciate the opportunity to testify before this Subcommittee and welcome any questions you may have.

Mr. GLICKMAN. Mr. Benington, a pleasure to have you.

Mr. BENINGTON. Thank you, Mr. Chairman, members of the committee. Today, I'm going to talk about activities on telecommunications network security that are conducted under the auspices of the National Security Telecommunications Advisory Committee, NSTAC.

NSTAC is a Presidential advisory committee consisting of about 25 CEOs of three kinds of companies; all of the major telecommunications companies; major companies that provide equipment to service telecommunications; and system integration companies, such as our own, which ties these together with other data processing systems. NSTAC is the Federal Government's principal mechanism to work with the U.S. telecommunications industry in one important area, and that is, matters affecting national security and emergency preparedness. What gets called NS/EP. In other words, NSTAC is not there to address the whole range of telecommunications issues that have to be taken up by the Federal Government, but concentrates on NS/EP, and it has been doing that since 1982.

In early 1990, the government was concerned about potential disruptions of NS/EP communications because of software manipulation of the network. As you pointed out in your earlier remarks, software is becoming an increasingly dominant element in the telecommunications system. A task force was established to look into this. I was chairman of that task force. A copy of the task force report is included, and I hope you include it in the written record of this meeting.

The task force concluded that intrusions into the public switch network over the past several years have confirmed that hackers have significant capabilities to penetrate key switching and signaling system elements. However, it's important to recognize that no hacker-related loss of services has affected NS/EP and the network. The task force concluded that the primary responsibility for network security lies with individual service providers. However—and I quote here—"Until there is confidence that strong comprehensive security programs are in place, the telecommunications industry should assume that a motivated and resourceful adversary in one concerted manipulation of network software could degrade at least portions of the public switch network and monitor or disrupt telecommunications serving NS/EP users."

Now, in saying this we did not mean that we considered it likely that a major disruption of NS/EP would occur or could occur. But rather, we felt that because there was potentially a very significant threat there, and because we had seen vulnerabilities, and because we felt there were great uncertainties about the risk, that we thought that software vulnerabilities should receive very high priority.

The task force provided service providers with a checklist of steps that when followed would substantially enhance the security of their own network. And I might point out that in this checklist we emphasize something that Mr. Walker just has, and that is, that the key, the first essential key to good security is management attention and management priority to make sure that what can be currently done is being done and is being disciplined. We found that a number of these steps had been followed by the industry. We

felt that the creation of the task force increased the impetus within industry. And, when I briefed the Chief Executive Officers, I was very pleased that their reaction to our findings was quite visible to them and that they were giving high priority to such steps.

The NSTAC at its 12th meeting, in December 1990, approved the task force recommendations and directed a follow-on task force to proceed in four areas: security information exchange, information about the threat, government research and development, and industrywide standards. I want to concentrate particularly on the establishment of the Network Security Information Exchange.

The task force has established a Network Security Information Exchange where 8 NSTAC companies are providing experts in network operations and computer security. The NSIE has 4 roles. First, the NSIE exchanges information, some of it quite proprietary, sensitive or classified, on threats, incidents, vulnerabilities, remedies, and risks concerning software manipulation. Second, the NSIE will periodically provide an overall assessment of the security of the public switch network, including trends, successes, and potential new threats. Third, if a significant attack should take place on the public switch network software or if a potential attack appears imminent, the NSIE will convene a group of experts to foster a concerted real-time response by affected companies. Finally, the NSIE should provide us experience about the value of information exchange and provide the basis for more permanent recommendations to the NSTAC at its meeting next June, a year from now.

In parallel with task force activities, the manager of the National Communications System called together a Federal Government NSIE to work in concert with the NSTAC NSIE. This NSIE consists of Federal employees who are subject matters from intelligence, information protection, and law enforcement agencies. Its charter closely parallels that of the NSTAC NSIE. We believe that closely coordinated industry and government NSIE activities will improve the flow of information to industry and keep the government in touch with ongoing efforts in industry to enhance network security.

The first meeting of these two NSIEs was held earlier this week, and we believe that 3 or 4 meetings should provide a basis for follow-on recommendations.

Now, to support the real-time function of protecting against significant attacks on network software, the task force and the government agreed that a joint industry-government National Coordination Center can play a strong role. The National Coordination Center, which exists today and was established in 1985, is concerned with the restoration and reconstitution of NS/EP telecommunications services or facilities. It operates under the manager of the National Communications System to provide for the rapid exchange of information and to expedite responses. The NCC has already assumed the role in the joint NSTAC/NCS approach to real-time software, and, as a matter of fact, last night, yesterday afternoon I was in contact with the NCC to follow the developments that were taking place in the Washington area, what was being done to handle them, what was the nature of the problem, the related activities in California, and I discovered that the NCC was very much up to speed, because at the same time in talking to Bell

Atlantic I found that when I got the information in greater detail that it supported that which was made available to the government.

So, in summary, before the NSTAC began addressing the risks of software manipulation, individual companies were alert and taking corrective action. The establishment of the Task Force on Network Security and the support of senior company management has given further impetus to these efforts. We believe the main burden of providing strong security clearly rests with the individual companies, but the NSTAC believes that cooperative efforts between the government and industry in areas such as information exchange, standards and R&D can further help to strengthen security.

That concludes my prepared remarks. Thank you very much, Mr. Chairman.

[The prepared statement of Mr. Benington follows:]

Testimony

of

Herbert Benington

Chairman

Network Security Task Force

National Security Telecommunications Advisory Committee

at Hearings on

Computer Security

Before the

Subcommittee on Technology and Competitiveness

House Committee on Science, Space, and Technology

June 27, 1991

Mr. Chairman and Members of the Committee:

I will talk today about activities on telecommunications network security conducted under auspices of the National Security Telecommunications Advisory Committee, or NSTAC. The NSTAC is a Presidential Advisory Committee that serves as the Federal Government's principal mechanism to work with the U.S. telecommunications industry in matters affecting national security and emergency preparedness (NS/EP). The industry's NSTAC and the Government's National Communications System (NCS) have been working together since 1982 to assure that the telecommmunications required to support NS/EP are available when needed.

Since NSTAC establishment, a number of NSTAC task forces have addressed various aspects of security of US telecommmunications. In early 1990, in response to Government concerns about potential disruption of NS/EP telecommunications through network software manipulation, an NSTAC task force evaluated the vulnerability of the current public switched network (PSN) to intrusions that might deny telecommunications service to NS/EP users or extract NS/EP-significant information.

The task force concluded that intrusions into the PSN over the past several years confirm "hackers" have significant capabilities to

penetrate key switching and signalling system elements. However no hacker-related loss of NS/EP services has occurred in a network.

The task force concluded the primary responsibility for network software security lies with individual service providers, and "until there is confidence that strong, comprehensive security programs are in place, the telecommunications industry should assume that a motivated and resourceful adversary, in one concerted manipulation of network software, could degrade at least portions of the PSN and monitor or disrupt the telecommunications serving NS/EP users."* This does not mean that we consider it likely that major disruption will or can occur. Rather, because of current uncertainties about the risk, we think reducing software vulnerabilities should receive high priority.

The task force provided service providers with a checklist of steps that, when followed, would substantially enhance the security of their own networks. A number of these steps have already been implemented by various industry companies, as a result of increasing focus on network security in recent years. Industry response was given further impetus by creation of the task force, and briefings to NSTAC

---

* Report of the Network Security Task Force, November 1990, National Communications System, Arlington, VA, Executive Summary page i. A copy is attached to this testimony.

Chief Executive Officers about the task force's conclusions provided still further impetus to elevate priority of network security in individual companies.

Finally, the task force concluded a broader crossflow of security information among U.S. telecommunications companies and with government agencies having an interest in network software security will assist carriers/suppliers to improve their network security.

The NSTAC at its twelfth meeting (December 1990) approved the task force recommendations and directed a follow-on task force to proceed in the following four areas:

1) Identify a mechanism and provide an implementation plan for security information exchange concerning risks and remedies

2) Recommend steps to Government agencies that will improve the flow of Government information about threat to industry

3) Recommend to the Government research and development needed for commercially applicable security tools, and

4) Evaluate existing industry-wide standards activities for network security and make recommendations.

The NSTAC charged the task force to work closely with, and in support of, a complementary body --- the Government Network Security Subgroup (GNSS), directed by the National Security Council, and consisting of representation of governmental agencies concerned with network security.

In order to address the first two areas, the task force has established a Network Security Information Exchange -- NSIE. In this exchange, eight NSTAC companies are providing subject-matter experts in network operations and computer security. The NSIE has four roles:

First, exchange information -- some of it quite proprietary and sensitive -- on threats, inciduents, vulnerabilities, remedies and risks concerning software manipulation of the PSN.

Second, periodically provide overall assessments of the security of the public switched network including trends, successes, and potential new threats.

Third, if a significant attack should take place on the PSN, or if a potential one appears imminent, convene the group of experts to foster a concerted response by affected companies.

Finally, gain experience in such a information exchange to provide the basis for more permanent actions by NSTAC -- and the Government -- a year from now at NSTAC's fourteenth meeting.

In parallel with the task force activities, the Manager, NCS, called together a Federal Government NSIE to work in concert with the NSTAC NSIE. The Government NSIE consists primarily of Federal employee subject-matter experts from intelligence, information protection, and law enforcement agencies. Its charter closely parallels that of the NSTAC NSIE. It is expected that closely coordinated industry and Government NSIE activities will improve the flow of threat information to industry and keep the Government in touch with ongoing efforts in industry to enhance network security.

The first meeting of the two NSIEs, held jointly, took place only yesterday and the day before (on June 25th and 26th); the task force believes the first 3 or 4 meetings will begin to provide a basis for recommendations.

To support the "real time" function of protecting against significant attacks on network software, the task force and GNSS agreed that the joint industry-Government National Coordinating Center (NCC), can play a strong role. The NCC's mission is to assist in the initiation, coordination, restoration and reconstitution of NS/EP telecommunications services or facilities. Established in 1985, it operates under the Manager, NCS, to provide for the rapid exchange of information and expedite NS/EP telecommunications responses. The NCC has already assumed its role in the joint NSTAC/NCS approach to real time situations.

Regarding R&D and standards, the 3rd and 4th areas to address, the task force has preliminarily identified steps to improve NS/EP telecommunications network security in which the Government may have contributions to offer.

In summary:

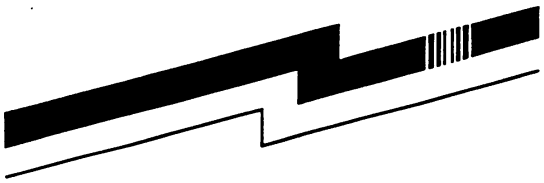
Before NSTAC began addressing the risks of software manipulation of public telecommunications, the individual companies were aware of the threat and were taking corrective action.

The establishment of an NSTAC task force on Network Security and the support of senior company management has given further impetus to these efforts.

The main burden of providing strong security rests with individual companies.

But NSTAC believes that cooperative efforts between the government and industry in the areas of information exchange, standards, and R&D can further help strengthen security.

That concludes my prepared remarks and I will be pleased to answer your questions.



Network Security
Task Force
Report

Report of the Network Security Task Force

November 1990

Report of the Network Security Task Force

November 1990

EXECUTIVE SUMMARY

The Network Security Task Force was established in response to Government concerns about potential disruption of National Security and Emergency Preparedness (NS/EP) telecommunications through network software manipulation.

A significant number of intrusions into the public switched network over the past several years confirm that "hackers" have capabilities to attack the networks and that some networks -- including network elements and operations systems -- are vulnerable to hostile penetration. Service vendors and equipment manufacturers have generally recognized this risk and improvements are underway. Nevertheless, until there is confidence that strong, comprehensive security programs are in place, the industry should assume that *a motivated and resourceful adversary, in one concerted manipulation of network software, could degrade at least portions of the PSN and monitor or disrupt the telecommunications serving NS/EP users.*

Although the burden of protecting the public switched network falls primarily on service vendors and equipment manufacturers, the task force recommends the National Security Telecommunications Advisory Committee (NSTAC) take the following actions:

1) A follow-on task force should be established that addresses means to reduce the vulnerability of the current public switched network to significant degradations of NS/EP capabilities. The task force should work closely with and in support of the Government Network Security Subgroup. In particular, the task force should:

   - Identify a mechanism and provide an implementation plan for security information exchange concerning risks and remedies
   - Recommend steps to Government agencies that will improve the flow of their intelligence information to industry
   - Recommend to the Government research and development needed for commercially applicable security tools
   - Evaluate existing industry-wide standards activities for network security and make recommendations

   The task force should finish its work in sufficient time for review by the NSTAC at its fourteenth meeting in the summer of 1992.

2) The Funding and Regulatory Working Group should address long-term funding, legal and regulatory issues.

TABLE OF CONTENTS

SECTION 1

INTRODUCTION

1.1 BACKGROUND AND PURPOSE

In early 1990 the Office of the Manager, National Communications System (OMNCS) addressed concerns that were being debated in the national security community about the security of common carrier networks. Aware of the heavy dependence of National Security and Emergency Preparedness (NS/EP) telecommunications on common carriers, the OMNCS moved to clarify, through cooperation between industry and Government, the nature and seriousness of these concerns.

The Industry Executive Subcommittee (IES), at its 21 February 1990 meeting, acted on a Government request to initiate a task force to address the network security concerns. At IES request, the National Security Telecommunications Advisory Committee (NSTAC), at its 29 March 1990 meeting, validated the formation of the Network Security Task Force. The task force has met during a period of seven months in 1990.

The purpose of the current documentation is to report:

- The activities, findings and conclusions of the Network Security Task Force to date, and
- The task force recommendations for follow-on actions.

The IES receives the report in written and oral form at its 7 November 1990 meeting.

1.2 PROBLEM DEFINITION AND SCOPE OF NSTAC ACTION

The IES responded to the Government request in February 1990 by assembling a task force and charging it "to scope the network security issue and to determine whether it is appropriate for NSTAC addressal." The network security issues of concern to members of the Government national security community were collected and coordinated in a meeting of NCS representatives from multiple agencies. A summary of these concerns was presented to the task force at its second meeting, in April.

Following dialogue with OMNCS personnel in early meetings, the industry representatives agreed the scope of concerns the task force would address are as follows:

General Area: Potential threat and vulnerability of the current public switched network and associated operations systems to software manipulation that results in:

- Denial of service to NS/EP users - primary
- Extraction of NS/EP significant information - secondary

Issue: Could a motivated and resourceful adversary, in one concerted event, take down the public switched network

- Solely through manipulation of network software, and
- With predictability?

1.3 APPROACH TAKEN

The first few meetings of the task force highlighted a difference of opinion/perception about the severity of the threat and vulnerabilities. Across the full range of participating companies' statements, initial expressions about the gravity of the situation, i.e. the potential consequences of recent intrusions into network software, varied broadly. Unable to rapidly arrive at consensus on the issue, the task force agreed to take further steps and:

- o Assess and characterize the threat
- o Identify types of manipulation and their likelihood
- o Evaluate potential impact on NS/EP capabilities, and
- o Suggest measures to reduce any vulnerability identified.

With the approval of the IES in May, the task force formed a panel to address potential threats and vulnerabilities. The panel's task was to assess the threats to current public telecommunications networks and the specific vulnerabilities of these networks to network element software manipulation. Composed of subject matter experts from NSTAC member companies, the panel provided outstanding help to analyze and correlate specific evidence and historical events and quantify the threat, to the extent possible.

A series of five panel meetings ensued, extending from May to August. Sensitive information was discussed, with accompanying strong commitment to confidentiality by individual attendees. An oral report by the panel chairman was given to the task force, for its consideration, in August 1990.

Following the report of the panel, the task force explored potential areas of future action that had become evident and measures that might reduce vulnerabilities. In the process of identifying these potential areas for

action, the task force identified actions that were appropriate for industry to undertake by itself and also actions that could be undertaken in coordination with the Government.

1.4 ORGANIZATION OF THE REPORT

Section 2 of this report summarizes the findings and conclusions of the task force. Within section 2:

Section 2.1 addresses the findings and conclusions of the task force about the threats to the public switched network, its vulnerabilities to the threat addressed, and the resultant risks.

Section 2.2 addresses what the industry members can do on their own to address the vulnerabilities --- in many cases individual industry members have already proceeded with these activities.

Section 2.3 addresses potential actions that could be carried out in the future. Some can be carried out by industry members themselves (e.g. continuing to improve their own networks' security). Certain others could be carried out by industry members together (establishing industry-wide network security standards). Still others (broadening network security information exchange) could be carried out in alternative forms. Some issues are identified that must be addressed, jointly with the Government, in undertaking such a broadening action.

Section 3 contains the recommendations to the NSTAC based on the above task force findings and conclusions.

Appendices A and B list the members of the Network Security Task Force and the Panel on Threats and Vulnerabilities, respectively.

SECTION 2

FINDINGS AND CONCLUSIONS

The task force deliberations have resulted in findings and conclusions in three areas: (1) the threats, vulnerabilities and risks in the area of network software manipulation; (2) industry actions that individual companies can take to reduce current risks of damage; and (3) potential actions that industry, or Government and industry jointly, can take to reduce current risks.

2.1 THREATS, VULNERABILITIES AND RISKS

Regarding the current and recent threat, the task force has reviewed specific information on the evolving capabilities of "hackers" who appear to be targeting the public switched network. In this document, the public switched network includes all public telecommunications service offerings that could affect NS/EP. The term "hackers" refers to computer criminals who intrude into computers illegally or without authorization. These individuals have technical and operational capabilities to penetrate public switched networks. The "hackers" network and share information with each other.

Regarding existing vulnerabilities, the task force has reviewed information on specific penetrations of networks by "hackers" in the past several years. These penetrations have attacked Operational Support Systems and key switching and signalling system elements. In some cases, computer criminals have repeatedly explored some PSN network elements.

The task force concludes:

- There have been software security vulnerabilities in the public switched network and some of these could impact some NS/EP capabilities. Although most security "holes" are "fixed" when discovered, others continue to be identified. Even when fixes are made, not everyone concerned becomes aware of them, and subsequent changes may "undo" the fix. Further, as technology evolves, new security "holes" appear.

- While the PSN is robust with physical redundancy and diversity, there is evidence that there is a new threat to the PSN in the form of computer criminals or intruders who penetrate the various systems of the PSN. The threat to software security is international; penetrations originate in some cases from overseas.

  The individual "hacker" is very capable, even when working on his own. Well-funded adversaries capable of organizing a community of "hackers" will have the capability to launch even more sophisticated attacks. Having the time and resources, such an adversary could build databases and plan and test a widespread attack on the PSN.

- Unless network security is strengthened, a motivated and resourceful adversary could penetrate portions of the public switched network and probably monitor or disrupt telecommunications serving NS/EP users.

The task force reviewed many technical, operational, economic, market and institutional factors that characterize and drive the evolving PSN, and the impact these factors have in creating new vulnerabilities. In a network as complex, heterogenous, and software-driven as the PSN, a high degree of security is technically difficult to achieve. Many features that make the current network excellent with respect to performance, function, and cost make the achievement of high security much more difficult. To over-simplify: open, accessible, customer-driven networks are vulnerable to penetration and software manipulation.

However, the task force also reviewed, in some detail, the steps being taken today to strengthen the network. These involve a mix of technical controls and monitors, personnel practices, operational constraints, and, most important, management commitment. With these measures, security can be significantly strengthened today. In addition, security can be further strengthened by developing a consistent long-term approach, a network security architecture. The task force concludes:

- Strong security in the PSN depends primarily on the actions of individual service vendors and equipment manufacturers that incorporate security features. Security must be wedded to the unique management and administration of each company. Strong security can be achieved with here-and-now measures that have minimal impact on operational costs or network performance.

The task force has been working closely with the Government regarding their perspective of software vulnerabilities of the public switched network. Under the leadership of the Manager of the National Communications System, a Government Network Security Working Group has been established including agencies concerned with telecommunications policy and operation, law enforcement, and national security. It is clear that the Government is very concerned about potential vulnerabilities and attaches a high priority to better understanding this problem in the near future. It recognizes that close cooperation with the NSTAC is essential to meeting its objectives. The task force concludes:

- The Government desires a close working relationship and strong communications among the NSTAC, the NCS, and other Government agencies regarding potential PSN software vulnerabilities and steps to counter them. This relationship should address information exchange, incident reporting and recovery, actions underway in the industry, law enforcement, technical standards, and the potential of Government INFOSEC and COMSEC research and development to focus more closely on PSN security requirements.

Finally, the task force concludes:

- The current risk, which is a function of vulnerabilities and threat, is highly uncertain. Several aspects of the threat are difficult to ascertain: the potential degree of collusion and hostility of "hackers" is not known; the role of foreign "hackers" is undetermined; the support from adversary nations/groups is not quantified; and the deterrent power of law enforcement is just emerging. Consequently, a total threat assessment has not been attempted. In addition, vulnerabilities must be regarded as uncertain: the priority and effectiveness of recent security measures taken by industry are not known; incident risk has been inadequately evaluated; there is a lack of a total system view of security vulnerability; and the capability to respond quickly to an enhanced threat is unclear.

  If the risk is in fact high, it is likely that a body of adversaries could undertake a coordinated attack that would severely degrade the public switched networks' performance capabilities, inducing prolonged nationwide outages. Physical redundancy will not assist in countering this threat.

  If the risk is in fact low, it is much less likely that we will see significant NS/EP service degradation, although the possibility still exists. It is more likely that we would continue to see what we have seen in the past. To date we have not seen the kind of attack that significantly degrades the PSN's NS/EP performance capabilities.

  However, it is imperative that prevailing impressions are eliminated among industry company personnel that "hacker" capabilities are limited to toll fraud. Until there is confidence that strong, comprehensive security programs are in place, the industry should assume that a motivated and resourceful adversary, in one concerted manipulation of network software, could degrade at least portions of the public switched network and monitor or disrupt the telecommunications serving NS/EP users.

2.2 INDUSTRY ACTIONS TO REDUCE RISKS

The task force identified a number of both near-term and long-term "rational and prudent steps" that individual industry members could take to reduce current vulnerabilities and blunt the existing threat. It should be noted that a number of these steps have been or are being implemented by various companies within the industry.

Eight actions were identified to enhance security in the near-term (Actions A through H). Three further actions (I through K) were identified that will enhance security over the long-term. The actions and steps to achieve them are described in some detail below.

2.2.1 Near-Term Actions

Actions A through H can be undertaken immediately by any individual member company of the telecommunications industry for near-term improvement of its network software security. They represent a prudent approach to enhance the protection of each company's own networks and customers.

Action A: Conduct intensive security evaluations/audits*.

For each company the underpinning for further actions to reduce risk is an initial network software security evaluation/audit, together with continuing follow-on audits. Each company needs to have, internally, the skills to carry out such audits, and to work with vendors on problem areas that come to light. *Most company audits have been carried out with traditional audit groups whose skills and perspectives are different from those required for this kind of audit.* Those conducting these evaluation and audit activities must be capable of looking for intentional wrongdoing, through the application of anomaly detection.

It is clear that companies are unlikely to be in an equal state of network security. Further, companies vary in sophistication in judging their own security. Those regarding themselves as well protected may in fact be more vulnerable than those who are cognizant of a number of problem areas. The task force concludes:

- There is a need for each company to conduct a company-wide intensive and thorough security evaluation/audit. Experience has shown that cursory, or less than complete, security reviews (as described below) may give a company a false sense of network security. The three-level review recommended here is intended to minimize the probability of such an occurrence. A number of the actions subsequently listed will be a direct outgrowth of the findings of such an audit.

*The words "evaluation/audit" are used to convey both that: 1) this is intended to be more than a traditional audit; and 2) the rigor and formality of traditional audits are required. The task force noted that traditional audit groups are not likely to have the requisite skills or perspective to conduct these evaluations/audits by themselves. The challenge for each company will be to obtain people with the necessary technical security expertise to participate in conducting these audits. It is expected that each company will need to enlist the aid of appropriate system developers and vendors.

- Company policy review. As with any comprehensive audit, the process should begin by collecting and examining for completeness and adequacy any and all company policies, practices, procedures or other guidelines addressing the security of the company's assets and properties (physical and intellectual). These policies should be reviewed and judged against generally accepted industry standards, and against the practices (to the degree known) of other similar companies. Also, in a more absolute sense, they should be reviewed and judged for adequacy in the face of the known and documented threat to the network and its attendant operations systems from today's computer criminals. Because of the appropriately long lead times and formalities associated with establishing policy in most companies, experience has shown that the official written material regarding network security has not always kept pace with advances in technology or with the changing nature of the external threat. Inadequacies or incompleteness in these areas should be corrected.

While this is a necessary first step in a complete and comprehensive audit, it is by no means a sufficient step. The next two steps must also be completed, if the audit is to be effective.

- Implementation review. Field implementation of the company's policies, practices and procedures should be reviewed next. It is well known that field implementation of a set of policies, procedures and guidelines can differ significantly from the written word. If the prior step has uncovered inadequacies in the company's policies, procedures or practices, this step should still be conducted without delay. It will be valuable to determine just what de facto security practices are in place, and what awareness of security issues and attitudes towards them the field staff has. The results of this step will also be important input to defining or correcting company policies, practices and procedures.

- Site/system review. The final step in the audit process is the most important, the most time-consuming and the most difficult. This step involves detailed audits, including physical site inspections, of security for all of a company's computer-driven assets. In the past, security reviews that have basically stopped with the first two steps have resulted in an overly optimistic view of a company's security posture.

The company will have to take inventory of all of its mechanized, computer-driven systems. Once the inventory is complete, the systems should be categorized roughly as follows. (The audits of systems should proceed through the categories listed in the order given. Those types of systems listed first are the most critical to review.)

1. All systems that are directly involved in the real-time process of completing customers' calls. These are the company's Network Elements. The list of such systems would include all circuit and packet switches, digital cross-connect systems and

real-time network-accessible database systems (such as "Service Control Points" or "Network Control Points").

2. All systems that directly interface with the Network Elements for the express purpose of updating, maintaining or otherwise managing the data elements or programs within the Network Elements. These would include all memory administration systems, service management systems and software generic maintenance systems.

3. All systems that contain sensitive network data or that are involved in critical service-affecting functions. This would include systems that are critical to the establishment of a customer's service (often referred to as "provisioning" systems).

4. All systems that contain sensitive customer data.

Within categories 2 through 4, all Unix® based systems should be reviewed first, followed by VAX/VMS based systems since these operating systems appear to be favored targets of computer criminals.

Each system audit should begin by identifying all vendor or developer provided security features and by explicitly determining which of those features have been purchased or activated by the using company. In addition, all add-on security capabilities should be identified.

Physical site inspections and security reviews should focus on whether or not these security features are being used and how effectively they are being used.

- Site inspections should, for example, determine whether logons and passwords are being shared or not and whether or not they are being properly protected (e.g., not posted on terminals or bulletin boards).

- Particular attention should be given to dial access and access control mechanisms. Password laxity and dial access mechanisms are often the most visible signs of system vulnerabilities.

- Another extremely important area to examine is that of system defaults. Most systems are shipped with startup, or default, accounts, passwords and permissions. It is extremely important to change these default values before the system is put online. A review of the vendor-provided defaults and whether or not they have been changed is a key part of these audits.

- Trash management should be reviewed since trash has been exploited extensively in the past by hackers.

Specific details of this level of security audit will differ for each company and each system. The intent of this step, however, is the

same across companies and systems: to ascertain the actual field implementation of security features and capabilities and to identify any unnecessary vulnerabilities through physical inspection.

Action B: Assure dial access control.

Experience has indicated that very useful and necessary dial access capabilities are a prime point of criminal intrusion into software systems. In fact, one of the very powerful and attractive features of automated, software-driven systems is that they are remotely accessible over the public switched network. Rational and prudent steps can be taken to reduce the probability of this very useful capability being subverted.

- o Eliminate unnecessary ports. All unnecessary dial access ports identified as a result of the audits described above should be eliminated. Previous audits have indicated that old or no longer needed ports are sometimes not deactivated. This step will improve security by reducing the number of possible entry points.

- o Improve dial access procedures. In many instances, improved dial access procedures can improve security. These improved procedures are particularly useful when "occasional" outside (i.e., non-company) personnel must gain access to a system. This can occur when a switch manufacturer, for example, needs access to install a program patch or to test a suspected problem.

  Improved procedures can include manual port activation and automatic de-activation at call completion. Other procedural improvements may also be warranted. These might include restricted dial access permissions and second party access verification. Yet another procedure improvement would be to use "trap and trace" recording procedures on particularly sensitive but hard to control dial access ports. These procedures would create a real-time log of port use.

- o Use security-oriented dial access technologies. Perhaps the most effective action is to undertake the use of security-oriented dial access technologies. While some of these also have vulnerabilities and should not be viewed as panaceas, they can increase overall security. These techniques include:

  - dial-back modems

  - validation of the incoming calling number against an authorization database, and

  - use of dial-in passwords.

  Another available defense is

  - the use of encryption modems at both ends of the dial access connection.

Advanced security capabilities identified in Action E below can also be applied to dial-access ports.

Action C: Use existing security features.

As indicated above, one of the most frequent sources of system vulnerabilities is the simple failure to effectively use existing security features of today's systems. These "use failures" should be identified in the audits discussed above. The task force concludes:

- **A variety of employee education and "feature use" action plans can and should be developed and implemented to ensure that existing security features are effectively used on an ongoing basis.**

Action D: Require elimination of security "holes".

Most systems seem to have a number of security "loopholes." Either intentionally installed in the system for the convenience of system developers or unintentional software "bugs", these holes create access opportunities for the computer criminal. Well-known but unclosed holes or software bugs in the Unix® operating system were used by Robert Morris in creating and propagating his now infamous "Internet worm".

The intentionally created holes (consisting of undocumented system "defaults", or programmer-created "back-door" entry points into certain subsystems) must be identified and removed by the system developers or vendors. They are virtually impossible for the user organization to discover and eliminate. The unintentional holes (generally software "bugs" or undesirable side-effects of desirable and necessary features) are even harder to find. The task force finds:

- **The most effective technique currently known for rooting out these holes is to do a thorough technical "how did they do it" analysis of known system intrusions. This usually requires the expertise of technical security specialists working with knowledgeable systems developers and expert users.**

Identifying the holes, while necessary, is obviously not sufficient. The task force concludes:

- **Positive action must be taken to expeditiously close all discovered holes, with urgent attention being paid to those that are discovered because they have been exploited by computer criminals. Identified holes can usually most effectively be closed by the system developer. But this means that the existence of the hole must be communicated to the developer and that the user must require that the hole be closed. In the interim, it is incumbent on the using company to devise and apply interim corrective measures.**

Action E: Deploy new security technologies

New technologies exist that can significantly improve the security of existing systems. These new technologies can often be appliqued onto the existing systems without major modification to the systems. It is generally felt within the security community that the most effective security mechanisms are those that are carefully architected into a system; however, the security of existing systems can be improved by applique techniques. In fact, some of the newer techniques appear to be particularly adapted to use as a "fence" to "surround" existing systems.

The particular technologies that are most effective and desirable is a topic of much discussion and some disagreement among security experts. However, the following technologies are worth investigating and considering for implementation:

(1) Biometric identity authentication techniques. These include speech verification, hand geometry, retinal blood vessel patterns and fingerprints.

(2) Token-based systems. These generally take the form of small hand-held devices carried by the user that generate a one-time password when activated by a personal identification number (PIN). They also include "smart" cards coupled with authenticators/encryptors located at the originating end of the connection.

(3) Third party authenticators/encryptors. The prototypical system in this case is called Kerberos and was developed at MIT as part of project Athena. In short, the Kerberos approach uses an independent "trusted" (or secure) computer system as a broker between a user and a target system. The Kerberos "broker" knows the password of the user and once it authenticates the user it provides the user with a "token" (an encrypted character string), which will allow the user to access the target system.

These are by no means the only worthwhile technologies to pursue. The task force concludes:

- A variety of new technologies should be explored and deployed as quickly as possible in order to improve existing system security and to enrich the total security environment presenting a variety of defenses to would-be intruders.

Action F: Control proprietary information.

Often computer criminals discover how to break into systems by stealing and reading system and user documentation. The task force concludes:

- o Industry members should review their proprietary information protection practices and should institute appropriate and effective controls. All proprietary or sensitive information on paper should be shredded or otherwise disposed of; comparable care should be used in disposing of magnetic media, microfiche, printer ribbons, etc. bearing sensitive information. In no case should sensitive documentation be disposed of by throwing it in the trash bins outside of company offices.

Action G: Improve security staff skills.

Today's computer criminals have sophisticated software skills. Understanding their crimes, their techniques and how to thwart them requires equally sophisticated and knowledgeable security staffs. The task force concludes:

- o Industry should evaluate the current skill base of their professional security staffs and take action to supplement that skill base where appropriate. Consideration should be given to emphasizing computer crime prevention skills in security departments along with the more traditional crime prevention skills.

Action H: Establish security awareness programs.

Many companies institute employee security awareness programs from time to time, usually in response to specific incidents. The task force concludes:

- o Awareness programs should become a regular and ongoing part of employee information programs. In the final analysis, much of the security of a company's assets will be dependent on awareness and actions of its employees.

2.2.2 Long-Term Actions.

The task force and panel believe that industry members should undertake the following three long-term actions to improve the overall security of their telecommunications networks.

Action I: Develop and implement a network security "architecture".

The task force observed that current telecommunications network vulnerabilities are in part due to the fact that the existing networks have evolved as a collection or conglomeration of individual systems each with its own security architecture. There is, in fact, no consciously designed company network-wide security architecture. In this context, architecture is used to mean concrete, measurable security requirements, and a physical

systems plan for implementing these requirements. Such an architecture would specify the points in a network that require a given type and level of security, and identify feasible implementation alternatives. The task force concludes:

- Industry members with network responsibilities should each develop a total network security architecture and implement it. Such an architecture, in order to be implemented, must be an economically feasible approach targeted at protecting the network from real and quantifiable threats.

In section 2.3, the task force's conclusions are set forth about the need for the industry to develop a consistent set of network security standards. The task force also concludes:

- In developing the company's security architecture and plan, each company should assure that its security architecture is consistent with industry-wide standards as they emerge, and

- The architecture should incorporate effective security technologies that are not overly reliant on user willingness to cooperate or the user's memory. While protection that is sufficient to counter the threat is required, too much of today's security technology is too dependent on onerous user actions.

Action J: Demand, build and purchase secure systems.

Early in the deliberations of the task force, it was noted that suppliers of network elements and systems are motivated primarily by the expressed needs of their customers. The task force concludes:

- If the security of systems is to be improved over the long run, then the acquirers of those systems must demand, build and purchase only systems with appropriate levels of security. This implies that these system "customers" must be able to define their security requirements to their suppliers and must be in a position to objectively analyze the security adequacy of both offered and delivered products.

Action K: Establish effective incident response strategy.

As a result of its investigation of historical incidents, the task force concludes:

- The industry, possibly in coordination with Government, must have a unified and effective plan for responding to software security incidents.

Consistent with such a nationwide response plan,

- Each industry member (service provider and equipment manufacturer alike) must have its own corporate response plan.

These response plans should effectively treat both the immediate response to an incident and the appropriate recovery strategies and tactics. The establishment of such plans is totally consistent with today's NS/EP posture within the industry and in general involves only, one hopes, straightforward extensions to existing plans.

2.3 POTENTIAL GOVERNMENT/INDUSTRY FUTURE ACTIONS

The task force identified a number of actions that could be undertaken in the future either by industry companies themselves without Government sponsorship or by NSTAC in joint action with the Government.

Steps that can be taken by individual industry companies, and in some cases have already been undertaken, have been identified above. The focus of the current section is on potential future actions, e.g., those not yet undertaken. These include actions by individual companies themselves, by individual companies with each other, and/or by companies in coordination with the US Government. The task force concludes:

- The primary actions needed are that individual members of the telecommunications industry take whatever rational and prudent steps are indicated to secure their own networks, to the extent that these steps have not yet been accomplished. An important start would be the actions/steps listed above in Section 2.2.

- The most important potential follow-on action for NSTAC to address is implementing improved exchange of software-related information on threats to, vulnerabilities of, and incidents in the public switched network.

2.3.1 Security Information Exchange (SIE).

The task force addressed the potential advantages of providing a cross-flow of security information among U.S. companies and agencies that have an interest in network software security. Parties to network security information exchanges could include service vendors, equipment manufacturers, and Government agencies (e.g. network users, network supporters, technical experts, law enforcement agencies, and intelligence agencies.)

In order to define objectives, identify issues, and learn about security information exchange from the experience of others, the task force reviewed the following: (1) the current role of the National Coordinating Center and potential extensions; (2) the Bellcore Security Information Exchange Program for its nine sponsors; (3) the activities of the Government Network Security Working Group, including their Threat/Intelligence Subgroup and their Technical Subgroup, a presentation on a concept for a Network Security Focal Point, and the evolving Terms of Reference for the working group; and (4) potential objectives of, actions of, and restraints on public network operating companies regarding security information exchange. It appeared to the task force that value could be added toward the security of the telecommunications industry by providing a security information

exchange not only among local exchange carriers as provided by Bellcore but also among the broader community of U.S. carriers and suppliers, possibly with the Government in a supportive role.

However, the task force identified issue areas that remain to be addressed in order to identify the most appropriate form of network security information exchange. Examples of areas that need further deliberation are listed below:

1) What would be the priority of each of various objectives to be supported by information exchange? Candidate objectives to be prioritized are:

   Reduction of PSN vulnerabilities

   Alerts provided in near-real-time to contain vulnerability and foster recovery

   Increasing visibility to Government and US industry of trends in threats, vulnerabilities, and risks

   Support to law enforcement and increased deterrence to lawbreakers

   Detection of and response to a new threat

2) What kinds of information would, or could, be exchanged? Candidate kinds of information include:

   Security vulnerabilities, including poor operating practices, security "holes"

   Security remedies

   Incidents (Subissues: Which ones would be reported? How quickly? Under what conditions would they be reported? Would anonymity be a requisite?)

   Recovery needs, actions, plans

   Threats, such as provided by law enforcement agencies, network operators, and/or intelligence agencies

3) What would be needed to make security information exchange successful? Candidates include:

   Removal or reduction of legal barriers, real or perceived

   Security and anonymity of information exchanged

   Experienced analytical capability provided at a central exchange point

   Time, and trust among participants

4) Is there a role for Government in a security information exchange program? Candidate roles include information supplier, information user, and observer.

Regarding roles of the Government, the task force finds the following specific sub-issues to be pertinent:

Would the exchange mechanism be involved in determining whether hostile software manipulation was likely to cause specific NS/EP problems?

Would the exchange mechanism be involved in determining whether Government NS/EP user problems being experienced were being caused by hostile software manipulation?

Could the Government play a useful role in detailed vulnerability studies including scenarios, threat modeling, funded support of industry analytical efforts, identification of NS/EP priorities, conduct of national level exercises, etc.?

What Government intelligence and counter-intelligence efforts could be expanded to specifically address public switched network vulnerability to software manipulation?

What could be the role of the NCC in security information exchange?

As a result of the described investigations and deliberations about information exchange, the task force concludes the following:

- Significantly increased exchange, between PSN service vendors and equipment manufacturers, of software related information on threats, vulnerabilities, and remedies could significantly help to reduce vulnerabilities of the public switched network. Initially, emphasis should be placed on measures that will reduce vulnerability rather than provide near-real-time alerts, assist prosecution of computer criminals, or provide trend information.

- Issues remain to be addressed in order to develop a program that would foster the appropriate security information exchange. For example, from industry's point-of-view, what are be the principal objectives of improved security information exchange and what factors would need to be addressed to meet these objectives? In a joint activity between industry and Government, what Government objectives, industry objectives, and mutual objectives should be pursued? Also, prior to establishing such an exchange, clarification of legal and regulatory constraints is needed.

2.3.2 Legal and Regulatory Ramifications to SIE

The task force found that there are a number of legal and regulatory ramifications that must be identified prior to establishing broader coordination or sharing of information about network security incidents.

The impacts of laws and regulations such as the Privacy Act, the Modified Final Judgement, and anti-trust regulation need clarification. In particular, clarification is needed regarding the nature of the information that can be collected and the handling of information that might later become involved in law enforcement actions. Legal experts of potential participants in such an information exchange do not always agree on the ramifications of the above laws and regulations.

Constraints on the sharing of information must be addressed early. Example questions that have been raised and still need to be addressed are:

> Are there any regulatory impediments that restrict telecommunications service providers from exchanging data among themselves regarding intrusion into the network? Might the type or source of the data be key regarding its shareability, i.e. generic break-in information, information about holes in the network, warnings about suspected intrusions or intruders, information that was obtained in the course of business, information obtained through network monitoring activities such as wire-tapping, or information obtained through the monitoring of bulletin boards?
>
> Under what conditions can telecommunications service providers obtain and use information from the network to protect themselves or others from the activities of computer criminals? What evidence is necessary to obtain cease and desist or arrest warrants to stop network intrusions? What evidence is necessary to be able to indict and successfully prosecute network intruders? What constitutes a network intrusion? Must a perpetrator actually do harm to the network or illegally copy, sell or destroy software in order to be successfully prosecuted?
>
> Which federal agencies and departments are responsible for apprehension and prosecution of computer crimes? Governmental responsibility seems to be fragmented. The monetary impact of software losses is difficult to quantify, but law enforcement uses monetary loss thresholds as an artificial barrier before any investigative action is taken. Additionally, local law enforcement officials are generally ill-equipped to deal with the computer crimes. Often when such crimes are proven, penalties are not commensurate with the potential damage that could have been caused. Penalties range from seizure of equipment and files, to probation, to short terms in institutions.
>
> To what extent can law enforcement personnel share information with telecommunications companies? What legal and regulatory constraints are there on the flow of information from local and Federal personnel to private industry telecommunications personnel?
>
> Will the use of information in law enforcement procedures such as grand jury deliberations unduly hamper the dissemination/ coordination/use of such information by industry, even if industry has been the source of the information?

The task force was unable in the time available to address all the legal and regulatory ramifications of common carrier network security information exchange. However, the task force believes:

- The NSTAC's Funding and Regulatory Working Group (FRWG) can work with Government to address the legal and regulatory issues and identify why they are important. Government could work to clarify the situation and NSTAC can review and advise on the clarification.

2.3.3 Industry Criteria and Standards

The development of industry-wide criteria and standards is a potential future action among industry companies. The telecommunications infrastructure comprises hundreds of local exchange and interexchange carriers. Each switching node may be supported by several operations support systems. The protection of network elements and their operations systems, or their secure interconnection, is not covered by accepted industry-wide security standards.

The networks themselves have been designed historically in an environment of trust. Once a craftsperson passes an entrance security check and remotely enters one system, access to another system is typically not blocked. Therefore, if an intruder penetrates defenses at any point of entry, few internal barriers or challenges are raised. Penetration of any "weak link" in the "chain" of network nodes can permit broad access within the network, even from a remote dial-up location.

An adversary can gain access to a system by exploiting a weakness in the security screen or by masquerading as an "authorized" user. Once in the system, he can manipulate system software and network elements.

The trend toward automation is driven by business and economic factors. Further automation of the IEC and LEC interconnection systems (e.g., SS7 signalling systems) is planned. However, in the belief of the task force, two actions can contain the potential damage caused by the present and emerging threat:

1) Insist on installing robust security options on each network element procured by each network provider, and

2) Insist that each employee operate and maintain the security element in a fashion consistent with its intended use.

These two items merely reflect prudent business practices.

Industry-wide security criteria and standards become increasingly important as automated interoperability of networks proliferates. It is not envisioned that the task force would develop new industry standards to address network security shortcomings. The task force should review the current and developing industry standards that support or enhance network security, and determine what network security issues remain. The task force should describe these remaining network security issues in detail and

present them to the appropriate standards organizations for inclusion in their developmental activities.

2.3.4 Research and Development and Technology.

The task force believes that, in future research and development, ways to enhance the network security of the public switched network need to be addressed. Current Government sponsored security research is generally not commercially applicable, is restricted in its use, and is not application-oriented (in particular, intrusion detection research). Coordinated, synergistic work efforts are needed among the National Security Agency (NSA), the National Institute of Standards and Technology (NIST), industry, and possibly academia. Possible approaches to assist in redirecting Government research to commercially applicable security mechanisms are as follows:

- A follow-on task force, involving security research experts, could define problems, provide examples, explore approaches, and provide recommendations.
- A joint industry/Government security research advisory board could provide the industry view to NSA/NIST on an ongoing basis, provide Government research results to industry, and review relevant academic accomplishments.
- Specific action panels with participation from industry and Government could be constituted, for example, to develop a "commercial Orange Book"; intrusion detection devices for carrier networks; and encryption devices that are commercially applicable.

SECTION 3

RECOMMENDATIONS ON FUTURE NSTAC ACTIONS

The task force has concluded that major responsibility for network software security lies with individual service providers. In its report the task force has provided guidance for these service providers that, when followed, will substantially enhance the security of their own networks. Beyond this, it appears that a broader information flow among carriers and suppliers nationwide will assist the carriers/suppliers to improve their network security. Therefore, the task force recommends two follow-on activities:

1) A follow-on task force should be established that addresses means to reduce the vulnerability of the current public switched network and associated operations systems to software manipulation that results in denial of service to NS/EP users, and extraction of NS/EP significant information. The task force should work closely with and in support of the Government Network Security Subgroup that is addressing related issues. In particular,

   - The task force should focus primarily on the identification and development of a mechanism for establishing a security information exchange that will enhance public switched network security. The task force should prepare a detailed implementation plan for establishing a security information exchange. Potential players in such an information exchange could include service vendors, equipment manufacturers, and government agencies.

   - The task force should consider mechanisms that will enable Government agencies to give to industry intelligence information that impacts the security of the network. As part of this process, the task force will define the information that industry needs and how this may be fed into the security information exchange.

   - The follow-on NSTAC task force should examine, in a joint effort with the Government, what network security areas need further research and development relative to the public switched networks, in order to facilitate the development of commercially applicable security tools. As part of this process, the task force should: (1) identify and prioritize needs of the PSN for technical developments; (2) meet with the Government and present an industry view of what is needed to be developed; (3) determine what is already being addressed by the Government; (4) make recommendations on what Government/industry should focus on in the future.

   - The task force should investigate existing industry-wide standards activities for network security, determine if shortfalls exist, and make recommendations as appropriate.

Task force evaluation of the network security issue, coordination of this evaluation with Government representatives, and recommendations to the NSTAC should be completed in sufficient time for review by the Operations Working Group (OWG) and the Industry Executive Subcommittee (IES) prior to the NSTAC's fourteenth meeting in the summer of 1992. As the task force makes progress it should report specific results and recommendations to the OWG, IES, and NSTAC.

2) The Funding and Regulatory Working Group should address long-term funding, legal and regulatory clarifications and potential improvements that could enhance public network software security beyond the level attainable by industry and Government actions in the near term. The FRWG should address section 2.3.2 of this report; the follow-on task force will continue to work in consultation with the FRWG and cite specific areas of concern, particularly with regard to issues that relate to security information exchange.

APPENDIX A

Network Security Task Force Membership

AT&T	Mr. Dave Bush/Mr. Jim Taggart
BELLCORE	Mr. Randy Schulz
CONTEL	Mr. Don Nowakoski
Ford Aerospace	Dr. George Dinolt
GE	Mr. Pat Glenn
GTE	Mr. John Cholewa
ITT	Mr. Joseph Gancie
MCI	Mr. Joseph Cassano
Motorola	Mr. Alexander Toth
NTI	Dr. Jack Edwards
Rockwell	Mr. Larry Manly
UNISYS	Mr. Herb Benington, Chair
UTI	Mr. Jay Nelson

APPENDIX B

Panel on Potential Threats and Vulnerabilities
Membership

AT&T	Mr. Dave Bush/Mr. Jim Taggart
BELLCORE	Mr. Barry Schwartz, Chair
CONTEL	Mr. Doug Guernsey
Ford Aerospace	Dr. George Dinolt
GTE	Mr. Jim Moake
MCI	Mr. Bruce Wells
NTI	Dr. Jack Edwards
UNISYS	Mr. J. Michael Williams
UTI	Mr. John Laclede

Mr. GLICKMAN. I want to thank you all for your testimony. All excellent testimony.

I want to go back for a minute to Mr. Schwartau's statement. On page two you talk about three points that need to be underscored and I want to see what all the witnesses say about them.

Number one—this is a very profound statement: "Government and commercial computers are so poorly protected today that they can be essentially considered defenseless. An electronic Pearl Harbor is waiting to happen."

Mr. Schwartau, that seems to imply that the information stored in all these systems—Social Security records, banking records, veterans' records—I'm now talking about the kind of information that affect people's daily lives every single day; 150, 200, 250 million Americans have their information in systems which can be opened up and invaded and destroyed or distorted without very much they can do about it.

Mr. SCHWARTAU. That's correct.

Mr. GLICKMAN. And you believe that's the case?

Mr. SCHWARTAU. That's absolutely correct. There is enough documentation to prove that. I even have here a set of U.S. Department of Justice records that go through a number of cases involving not only civilian, but military, penetrations, and those are the ones that we know about.

Mr. GLICKMAN. Mr. Walker, how would you characterize your view of his statement?

Mr. WALKER. That's a little strong. I think that most of these systems are, in fact, physically protected adequately. People aren't going to just walk in and steal the information. To the extent that their—communications are used though and that hackers can, in fact, get in through there, there is the serious problem. It's a problem that is bigger than I think—well, it certainly has been demonstrated to date. It can, if someone were to aggressively try to go after this information, they could get much of it. They could modify much of it. I think it would be detected that they did it. But they could, in fact, destroy a great deal of information.

Mr. GLICKMAN. So, the reason why it hasn't happened to date is why, we just don't have imaginative criminals or—

Mr. WALKER. There's nobody that it's worth going after this particular kind of information for yet. I mean we have—there's a vulnerability there but there isn't someone who's ready to go in and modify a Social Security record. What are they going to get for it?

Mr. GLICKMAN. But let's say that we had a situation like what happened at Revlon where you got a disgruntled former government employee gets hostage to the Social Security System, for example, and they want to terrorize it, and they had access over the years. If so, I suppose there's a real possibility of computer thieves demanding ransom or else a thief will take down a government computer system. Is that the kind of thing that could happen?

Mr. WALKER. That's happening more and more. That's happening more and more. In fact, the day before yesterday there was a case, I think in Houston, where an employee had put a trapdoor into a computer hoping he would quit and then they would hire him back at a big salary to take it out. And he's being, he was—I saw the pictures of him being led away in handcuffs.

I mean that kind of thing is, in fact, happening and will happen more and more.

Mr. GLICKMAN. Now, when you say a trapdoor, you mean there is some sort of software he put into the existing system that——

Mr. WALKER. Would either shut it down at some given time or would cause some failure or would cause some disclosure of information at a particular time. It's something in the future.

Mr. GLICKMAN [continuing]. And was he relying on the fact that only he would know how to fix it?

Mr. WALKER. That's right. It was buried in the software such that nobody else could find it. Fortunately, somebody else did find it and was able to disable it.

Those cases used to be rare in the Seventies and Eighties. They are more and more frequent now.

Mr. GLICKMAN. Mr. Benington, I wonder how you would respond.

Mr. BENINGTON. I think that it's a very strong overstatement of the situation. I cannot comment on government computers. I don't consider myself expert there. I can comment on the computers of the telecommunications industry.

First of all, let me point out—and I think Mr. Walker underscored this—that I believe that the operational experiences, the operational practices are available, that the technology is available, the policies are available, the success stories are available that show that you can protect complex networks of computer system and that you can have some appreciation of what risks still resides—and there will always be some risk residing. So I think you've got to ask yourself in the case of any particular set of computer systems to what extent has management understood the risks. And I agree with the basic conclusions of "Computers at Risk": to what extent has the management understood the risks, understood what steps can be taken and taken those steps.

Now, I know of no portion of the industry which has had greater experience with hackers than the telecommunications industry because hacking is getting access to telecommunications and, hopefully, you don't want to pay for your hacking, so the first thing you want to do is have some toll fraud so you can get some free communications domestically and overseas. So there has been a great deal of experience in the telecommunications industry. And, in our task force, and now starting in our Network Security Information Exchange, there are stories of that war taking place. And there have been penetrations. Some of them have come out in the press. In some cases companies have been quite brave and decided to take the hackers to court, to announce what the problems were, to show that they had been vulnerable and take steps. And some companies are taking very, very significant steps.

So I do believe that if you apply these practices, if you make security an objective, and I think many of the telecommunications companies have, and they are doing so increasingly, that you can very significantly reduce the risk.

Mr. GLICKMAN. Well, what happened yesterday doesn't give a lot of us confidence, much confidence that, in fact, when the unusual takes place that in fact the systems are very well protected. That is, I didn't gather anything in reading the paper yesterday that anybody screwed up particularly. It's just that the software got

ahead of us. Our mind-set was 20 years ago and the software was 20 years ahead of where our mind-set was, and that's your industry.

Mr. BENINGTON. Well, I think one has got to put yesterday's event in perspective. And I don't have enough data yet to do it, but I do know some aspects of it that I'd be glad to go into in more detail. Does yesterday's event signal a trend that the industry is becoming more vulnerable? I don't think it does at all. I think it was a very, very serious event. I think a lot of people were very discomfited by it. I don't deny that at all. We've had other events where fiber optic cables have been cut, and increasingly fiber optics is becoming as vital to the transmission of a lot of data reliably. We've had a similar event in common channel signaling that happened in January, a while back, which was significantly more significant than yesterday's event. It didn't take place in Washington.

But I don't see a trend at all. I think, in fact, I would like to make one comment about yesterday's event. You said that 20 years ago that hackers could whistle down the system and bring down the entire system, and that vulnerability related to what got called the blue box. That, in fact, you could go out and buy a box that would give you automatic whistling and you could have significant impact, the most obvious one being you get a lot of free phone conversations, as Touch-Tones came in. Now, the reason you could do that is that the signaling in the system of who you wanted to call was carried by the same circuit that you would talk over. And, as a matter of fact, the Washington Post had a very good description of that.

So, one of the reasons for trying to take the signaling away from the transmission circuit, so that when you and I talk we do it on one circuit, but if you want to place a call you go to a different box, it finds out whether there's a line available, if there is one, it sets up the call in a second, if there isn't one, it doesn't try to bother the whole system, it just says we can't do it. The reason that was done among other things was to get away from the security vulnerabilities of the blue box, of the whistlers.

Mr. GLICKMAN. I'm not saying that you haven't——

Mr. BENINGTON. And so this is a step. But, as in any step that we see in complex systems, there are failures. They happen in the aircraft industry, which is, to me, one of the most disciplined industries. They've happened in telecommunications, and I think one mustn't take that event out of perspective.

Mr. GLICKMAN. Let me—I just got a couple more and I'll move on because this is a very interesting subject. But one of the things that strikes me that both of you first—all of you talked about has to do with how the government perceives the threat to what you call information that average Americans need versus the threat to information that may affect our "national security." What seems to me underlies a lot of what we're talking about is the NSA does a super job of protecting national security secrets at the highest level. But there is kind of a perception in our government that everything else isn't that important to protect. I mean, you know, my aunt's Social Security records aren't important, the veteran's Veterans records aren't important, you know, the banking records aren't important. But the records vis-a-vis the Soviets are very im-

portant. So we're going to protect those and nobody else's. And it's kind of—and I think that one of the things you've talked about is there's got to be some rule of reason here, some mind-set, some different levels of protection, so that we don't get ourselves into the ball game of perpetually protecting some, maybe—I'm not demeaning the importance of the national security threat, but there are different levels of national security. After all, if somebody comes in, a disgruntled taxpayer, and electronically blows up the Internal Revenue Service, well that may make a lot of constituents happy for a short period of time. In fact, the Government of the United States would cease to be able to operate. It couldn't collect any money, and then it couldn't do a lot of the things that we do, that we need to do in order to pay bills and do that kind of stuff. That affects our national security very directly.

The other thing is, is that this question of the relationship between NIST and the NSA, and I've been in this for a long time because I'm on the Intelligence Committee as well, and I see what has happened with the National Security Agency justifiably trying to protect the national security side of the picture, jealously protecting its turf over this entire area and really not wanting to give up at all because they are not interested in the other side of the threat, which is the threat to average Americans every day. And I have seen NIST not really have the gumption or the credibility or the clout that's been given to them in this government to take this problem on.

And I guess, Mr. Walker, I'm kind of worried after hearing your testimony and seeing some of the things that need to be done. Until such time as the government really lets us believe that they want to solve this problem, it won't be solved. Because NIST will continue to have no credibility in the government and NSA will run the show because it's "national security." What do we do about that? Does Congress just have to come in and mandate it? Is that about the only way? And even then that doesn't necessarily work very well.

Any of you who want to respond to that.

Mr. WALKER. Well, I think the discussions that we were having two weeks ago at the Advisory Board were—I really sensed a shift there, where NSA because of the Computer Security Act restricting them to the national security area and because of the lack of resources to do the whole job they are beginning to think maybe we can focus on the high end. And, if NIST can find a way to get its gumption up, to find a way that it would not have to do evaluations itself, if this lab program would work, they could establish the FIPS criteria and cause these lower level systems to be evaluated.

Mr. GLICKMAN. But I guess my point—this may be a political question. If the Social Security System were invaded by an electronic bomb, and the checks were gone for 2 months, this government would turn its priorities inside out, I can tell you that right now, and the NSA would be sent out for a long vacation unless they cooperated in protecting these records. And maybe it will—it has to take, because I don't think it's going to happen. I think that it's very interesting, what you're talking about here. But I think

for the most part national security concerns will always dominate this issue unless we have some catastrophic event take place.

Mr. WALKER. Unfortunately, the solutions to this are long-term solutions. They take time. Industry has to build the products. The government has to figure out how to decide which ones are good. A catastrophic event of the sort that you talk about will raise the interest for a little while, but it won't provide the long-term solution. Yesterday's problem with the phone system won't provide a solution. We have to find a way to do it over the long term.

I think you people can help by encouraging NSA to focus on the area that they already have responsibility for and let NIST do its thing.

Mr. GLICKMAN. Okay. Just quickly, Mr. Walker, can you tell me how you feel the effectiveness of the Computer Security and Privacy Board is? How would you assess the effectiveness of the Board?

Mr. WALKER. Well, I'm very new to it. I am only an official member as of the last meeting. I've been there three times. And so, and these are my opinions, please. No one else's. Somebody will probably shoot me anyway.

I think that the Board has the capability to do some very effective things, to make some serious recommendations. I am concerned that what I've seen in the past, it's caught up in the Department of Commerce bureaucracy and it can't speak out. I'm not sure what you had in mind in saying this thing ought to be created. But it seems to me it ought to be able to get to you. It ought to be able to get to others. And I have the feeling—this is just an observation as a new member—it's not able to do that as effectively as it should.

Mr. GLICKMAN. Okay.

Mr. WALKER. It took, it took nine months for my membership to be approved through the system. And I realized at the March meeting that—I asked the question, has anyone else since it was originally constituted been approved, and no one had. Well, now that got fixed. In May, I was approved, as were other people.

Mr. GLICKMAN. Do you think if this committee, some of us wrote to relevant people asking that we get periodic input, do you think that would help?

Mr. WALKER. It couldn't hurt. Yes, it would help.

Mr. GLICKMAN. Okay. I would like to ask one final question. Mr. Schwartau, you talked about these HERF guns—high energy radio frequency guns. I mean, these look like actual ballistic devices?

Mr. SCHWARTAU. The designers of these could make them look pretty much like how they want. Essentially, a HERF gun is nothing more than a power amplifier, an oscillator and an antenna of some sort, and whether they're disguised or openly used looking like antennas, that's certainly——

Mr. GLICKMAN. They exist now?

Mr. SCHWARTAU. The capabilities exist.

Mr. GLICKMAN. The capabilities.

Mr. SCHWARTAU. And I just came from a show down in Florida where all of the equipment to plug one of these together sits on vendors' shelves.

Mr. GLICKMAN. Now, you say that these HERF guns, if we have the technological capability now to build a HERF gun, it could be

pointed at, let's say, the New York financial district, it could do serious damage to Wall Street, let's say?

Mr. SCHWARTAU. For Example, one of the worse problems that occurs in any electronic situation is what we call an intermittent problem. One that occurs occasionally. And one of the things that can be postulated would be, perhaps—a HERF gun is a fairly low power device, compared to what I call an EMP–T bomb—an electromagnetic pulse transformer bomb. If I had an adversary, perhaps, on Wall Street, another markets firm, securities firm, I might be so inclined to shoot this gun at their network installation and cause it to crash once an hour, whereby they would find their network constantly going down with little or no ability to initially identify the problem. And then even once they did identify the problem, to find me is a very, very difficult task.

Mr. GLICKMAN. The other gun, this electromagnetic——

Mr. SCHWARTAU. Electromagnetic pulse transformer.

Mr. GLICKMAN. That's much stronger?

Mr. SCHAWRTAU. Much stronger.

Mr. GLICKMAN. But the same——

Mr. SCHWARTAU. Same principle.

Mr. GLICKMAN. Same principle. Now, you say the Social Security System could be destroyed, rendering payments impossible. That is, any major system you could——

Mr. SCHWARTAU. Yes. Those were for illustrations only.

Mr. GLICKMAN. Airplanes? You could target it at an airplane in the sky?

Mr. SCHWARTAU. You need higher power for airplanes. But it has been postulated by some that the most efficient way to do it would be at the beginning of a runway or the end of a runway where the planes were at relatively low altitude.

Mr. GLICKMAN. Do you think—I hate to get involved in the issue of "gun control," and this is not a gun in the classic mode, Mr. Rohrabacher. But do you think that we ought to consider banning these kinds of devices?

Mr. SCHWARTAU. If you did you would be banning the microwave and communications industry from its existence.

Mr. GLICKMAN. Well, yes. [Laughter.]

I mean, well, what I had in mind—Mr. Benington?

Mr. BENINGTON. Yes. I can't comment on the specific threats that are being mentioned here. But, if the committee is interested in them, the Department of Defense is concerned with an electromagnetic pulse that comes from a nuclear blast——

Mr. GLICKMAN. Right.

Mr. BENINGTON [continuing]. And the equipment being able to operate. And a number of the telecommunications switches, commercial telecommunications switches, have been exposed to these electromagnetic pulses at various test installations. I don't want to give the details of the results, but I think you can get independent government assessments of what has happened and not happened under what would be a very extreme condition, where a high altitude nuclear weapon was detonated. And I'm not sure that you will end up with the anxiety that Mr. Schwartau has, but why don't you look at the classified information.

Mr. GLICKMAN. Okay. Thank you very much.

Mr. Lewis?

Mr. LEWIS. Thank you, Mr. Chairman. I think the testimony is very interesting. There is some element of disagreement, which is probably good. But I'm very much concerned about, for example, our national air system and air traffic control system. We have a glitch in New York and the whole Northeast is put out of business.

This again comes under national security, where any country that wanted to turn our system into havoc could very well do this by switching the system, as you say, with a HERF gun or maybe an electromagnetic transformer bomb, but that would do that.

Are we at a point at this time where, first of all, we have a number of agencies in the government that basically have assumed, some of them—others have been assigned—the security for certain areas, and there is quite a bit of overlap. And we also have problems out in the private sector, on Wall Street, in Chicago at the Board of Trade, places like this, where we have the same kind of problem.

Have we arrived at a point where we need some focal points, where we need—and in the government area we need one responsible person, or should we have—not person, but agency, or should we have two, one to take care of everything other than in the Defense Department? And are we looking at the same thing in the private sector?

You're on several boards, Mr. Walker, and advisory committees. You ought to be able to tell us that. Maybe we've got too many of those.

Mr. WALKER. That may be. I believe that we have two constituted now, NSA and NIST, but their relative strength and ability to perform aren't anywhere near equal. I am concerned that if we don't strengthen NIST in some way or create some—that a number of other organizations will be created. The Information Security Foundation, the reason it was suggested, the reason it's being followed up on is because the government isn't doing the job that would best be done by the government.

Now, NSA should not be doing the job for the commercial world or the civilian agencies. I think that's been well established. We need to find a way to strengthen NIST's role.

Mr. LEWIS. Might I interrupt you just for a moment there——

Mr. WALKER. Yes.

Mr. LEWIS [continuing]. And ask you, do you think Congress is part of the fault of this? I'm not going to take all of the blame. But do you think Congress is part of the problem?

Mr. WALKER. I would suggest that what you did in the Computer Security Act was a good thing, and it was a good start. But it is not enough. That, in fact—and that's why my recommendations are that you encourage in any way you can, and I don't know all the ways you can, but that this kind of cooperation happen. Now, just butting heads against each other isn't going to get us anywhere, and that's where we've been for quite a while.

Mr. GLICKMAN. Would you just yield for one second?

Mr. LEWIS. I certainly would.

Mr. GLICKMAN. As of today, would you still characterize NIST and NSA as butting heads against each other?

Mr. WALKER. There's a lot of cooperation. There's a lot of meetings. There's a lot of discussions. But we don't have a public key encryption algorithm. We don't have an exportable private key encryption algorithm. There are draft documents that the Advisory Board has been shown of ways in which the two are going to work together. It does seem to me it's taking forever, and this is part of where I say give somebody responsibility and hold them accountable for it. As long as two people have the responsibility, neither one of them can be blamed then and nothing happens. If you say, "NSA, do this; worry this area; NIST, do this; worry this area"—I am talking about now in the technical area of evaluating systems—a lot more progress would happen.

If we could somehow get some encryption capabilities that were generally available, exportable, it would make a great deal of difference. It would encourage industry to actually play seriously in this business. Industry is just watching now. They are saying, "NSA is drifting away; NIST isn't doing anything; what am I supposed to do? The Europeans are doing their thing. I can't stand all these different activities; bring them together."

If we don't fix this problem, which I think is—we are going to find ourselves with every individual agency going off and doing their own—because they have a responsibility to do it, and if we can't find a way to give them sound advice, they will do their own job and it will only get more confusing.

Mr. LEWIS. Thank you.

Mr. Schwartau, I think that your comment is a profound comment, but it is one that gets attention, that the chairman referred to, where we are so poorly protected on our computers.

But this does intrigue me a little bit, with these HERF guns and electronic magnetic transformer bombs and things like that. Do you think that we are looking at a real security problem from a Department of Defense issue with this? Because, from what you are saying, and as referred to by Mr. Benington with the nuclear blast, a concentrated effort could be made to disable all of your computers and not even be in the continental United States.

Mr. SCHWARTAU. In the extreme case, yes, but I am not specifically addressing DOD concerns. That is not—I have never been involved in the military community; my concerns have been from addressing the civilian agencies and the private sector and the impact of the loss of major computer systems on the economy and viewing that as a portion of our national security. I am not a defense expert at all.

Mr. LEWIS. No, but even outside the defense area we have had international problems with transferring accounts from one bank to another, but you could basically set up to do the same thing to disable the financial markets, if you wanted to, and create havoc in the country.

Mr. SCHWARTAU. It is possible to be done.

Mr. LEWIS. I would, Mr. Benington, like for you—on page 4 of your testimony, in your areas of exchange of information, the third one, where you say significant attacks take place on the PSN—if a significant attack should take place on the PSN or if a potential one appears imminent, convene a group of experts to foster a concerted response by affected companies. Could you elaborate a little

bit on that? It appears to me that this, again, could be after the fact, and what would be gained by an after-the-fact analysis? You already had substantial damage done. Could you elaborate a little?

Mr. BENINGTON. Yes, sir. The notion that I mentioned, this network security information exchange—and this is a panel of experts from eight major companies, and the notion is that if there were a threat of an attack or if there were indications that an attack might be under way, that then we would convene those experts in real time, within half an hour, with teleconferencing, and exchange information as to what each of them knew, and, for example—and this is very hypothetical, but we have, as you well know, three major interexchange carriers in this country, and they cover the entire country. They all use or are moving towards the kind of common channel signaling that I was discussing earlier, and that would be an attractive target if one wanted to go after it. It is quite heavily protected, we hope.

But if the common channel signaling of one of the three interexchange carriers was behaving strangely and we could alert the other two that this kind of behavior was taking place, and if the experts could talk about what the strangeness was, it could well be that we could nip the situation in the bud, or if something significant happened, that we could recover much more quickly because of coordinated actions as to how to handle this thing.

So if there is such a threat there of a concerted attack, we think that this group of experts could be very helpful, and we have now established the procedures so that they can be activated.

Mr. LEWIS. Thank you, sir.

Could you, Mr. Schwartau, tell me how you think that we could neutralize these electronic devices?

Mr. SCHWARTAU. There are known techniques. Most of the techniques——

Mr. LEWIS. How could you protect against them as well?

Mr. SCHWARTAU. These are all very well known. There are certain DOD and classified situations that are designed for the fallout, the magnetic fallout from a nuclear blast.

In the scenarios that have been postulated for, we will say, localized magnetic bombs, perhaps in the financial district or what-have-you, there are fairly effective shielding techniques to shield the E fields—the electric fields—or the magnetic fields from penetrating either entire structures or the computers themselves or the communications systems. These are fairly well known techniques.

Mr. LEWIS. I have some other questions, Mr. Chairman, but I am out of time, and I will work on them later on.

Mr. GLICKMAN. Thank you.

Mr. Rohrabacher.

Mr. ROHRABACHER. Yes, Mr. Chairman. First, I would like to remind you that HERF guns are outlawed only outlaws will have HERF guns.

Mr. GLICKMAN. Do you think if we had a seven-day waiting period [Laughter].

Mr. ROHRABACHER. Just after listening to the testimony, I think that we can be lucky that Colonel Khaddafi and some of the others of his ilk in the world don't understand that destroying information can be more damaging than putting a bomb in a dance club

and killing American servicemen, because they just—today, from what you are telling me, that the destruction of information through some sort of electronic machines or devices actually can be severely damaging to the lives of pensioners and people who rely—and just the way we do business in America, including how we fly our airplanes and everything.

So I—you know, I just was very fascinated about what you were saying. All three of you had very enlightening testimony, and I will have to admit that I am one of these fellows that, I have to call in my staff to help me with my own word processor to make sure I am all set up.

Also, I remember when I was at the White House that—I was a speech writer at the White House for seven years—there were particular machines that we were supposed to use when we were writing specific speeches, foreign policy speeches, where we could use—when we were just writing speeches for the Congress, we could use other machines, and——

Mr. GLICKMAN. Which machine was more protected?

Mr. ROHRABACHER. Excellent come-back.

Am I hearing what we are really talking about is, not having the Government necessarily buy a lot of equipment or hire unnecessarily a lot of other people, but what we are really talking about is having the Government get its act together and provide definitions and standards? Is that basically what we are talking about here, that because perhaps you are saying there is a conflict between NIST and NSA we haven't been able to set certain standards to come to certain definitions? If what we are really talking about is just providing these definitions and standards so that the private sector and other people can function—if you could all give me a little—your answer on that.

Mr. WALKER. If the standards existed and if there was a way to do the evaluations of them so that you could say to IRS or the FAA, or whatever, "This is the quality of this particular system versus that system"—the Government agencies and the commercial world are buying computer systems every day—if the standards existed and a way to evaluate them existed, industry would build them and users would buy them.

So there is not a matter of finding new money to buy massive new computer systems. You can really dramatically affect—and I think NSA, with their Orange Book and their evaluation process, has already had a dramatic effect. It needs to be stronger; it needs to be extended to the civilian government and the commercial world.

If you establish standards and an evaluation process, then industry will build to those and users will buy to them. So it is not a matter of spending a lot of extra money, it is a matter of being able to focus the money that you are spending.

Mr. SCHWARTAU. There is another issue besides purely the technical standards, and I think that is perhaps what you were addressing, and Mr. Walker pointed out the word "important" perhaps replacing some of the words, the Government catch phrases that we use of "sensitive but unclassified," and what does that mean?

There is a perceived duty on the part of the Government by many Americans that their information on them, some of the most

critical information on them, whether it is in the IRS, or the Social Security, or the Veterans' Administration, or in the Centers for Disease Control, or the Federal Reserve system, wherever it is, that there is some reasonable level of protection offered that information to keep their privacy intact, and with the kinds of technology that are available today very inexpensively to compromise that privacy, there needs to be some level of reclassification or additional classification with respect to privacy perhaps in distinction to security, which is what the Orange Book addresses, and this is much of what the Europeans in their current ITSEC movement are addressing, where it is not just a security issue but it is also an integrity and privacy issue.

Mr. ROHRABACHER. So in order to—we have to come up with definitions, the Government has to come up with definitions, that will make sure that we are talking about theft and vandalism, that we now are in this new age of electronics, and perhaps our definitions of "theft" and "vandalism" are not adequate.

Mr. SCHWARTAU. Well, according to, I believe it is U.S. Code 2314, there are certain judicial rulings that uphold that data or information is, in fact, a tangible asset and a goods. There are other judicial opinions on the same code that hold contrary opinions. So, yes, a portion of this entire effort needs to be what is information, and what is its intrinsic value on a security basis, and what is the fiduciary, moral, and legal responsibility on the part of the Government and society, the private sector, to protect that information.

Mr. BENINGTON. The task force that I am now heading is just starting to look into this, but there is a term in our charter that the NSTAC gave us that says "commercially applicable research and development," and what I would stress here is, if you want a standard to be commercially applicable—that is, to find a place in the commercial equipment that is produced and used in the commercial marketplace—then it is quite different than if you are unilaterally establishing a standard for the Federal Government for some particular objective, and I would point out, for example, that the open system interconnection standards—the so-called ISO standards which NIST played a very large role in representing the U.S. Government, but also the country, in developing those—have caught on and are catching on like wildfire in commercial equipment, and there, I think, the Government has played a very major role.

In contrast, some of the standards that were developed for computer security, where it was hoped, I believe, in something called the Computer Security Initiative, that they would be widely commercially applicable and therefore they would naturally protect the banking and the energy and the telecommunication industry, those standards, in fact, I think, have faltered significantly in terms of their commercial applicability, and so I think you have got to keep that in mind.

Mr. ROHRABACHER. Does someone have a list that says one, two, three, four, five, six, seven, maybe all the way down to 100 or whatever—maybe it is 1,000, for all I know—of specific definitions that need to be set and standards that need to be set on this?

Mr. BENINGTON. Sir, I think you would find there are that many standards bodies—that is a slight overstatement. Yes, there are

many, many such kinds of lists, and it is a very active area. I am not at all an expert in it.

Mr. ROHRABACHER. Well, I would just like to say that I have been fascinated by what we have been talking about today. Being a student of history, I know that many of the crucial problems in the past dealt with definitions of property rights, and we are talking about property rights here and also about how to make this society function, and whether you are going to have a narrow gauge railroad or a wide gauge railroad, and who is going to be responsible for protecting the bridges and making sure the bridges are capable of holding the railroad as it crosses the ravine, and these are all questions that our society had to face in the past, and now that we are reaching a higher level of sophistication and technology, we have got some more questions and we have got some more answers we have got to get, and thank you very much for helping me understand those.

Mr. MCMILLEN [presiding]. Mr. Gilchrest.

Mr. GILCHREST. Thank you, Mr. Chairman.

I missed the testimony because I was at another committee hearing, but I will read this all very carefully. I, like Mr. Rohrabacher, do not know much about computers, and I am kind of ashamed to say that, but I will try to fix that within the next few years.

I learned a few days ago of millions of dollars that are siphoned out of banks because of computer hacking, and, just to show you my expertise in computers, I said, "Well, why don't they unplug them at night?" So I have a lot of work to do to come up to speed on some of these issues.

I was also told by a gentleman that works for me that it is very easy to get into the computer in my office via a modem and a computer, and, boom, if you know the number, you can have access to everything, all of the information, which kind of unnerved me a little bit, and I also realized that the same number that goes to the computer is very similar to the number that goes to my office, so anybody with a little knowledge of Congress could just keep trying and they eventually would come up with it.

This is a very simplistic question, I suppose, but if that—is there a similar system to banks and other—could you find access in a similar manner to the IRS?

Mr. SCHWARTAU. There is a thing within the hacker community known as demon dialing, and what demon dialing essentially is, a small software program that runs modem that dials every 10,000 numbers within a specific exchange on a sequential basis and identifies whether the targeted phone number is either a voice line, a fax line, or another computer. It automatically then outputs all of the relevant information to that particular hacker and gives him a full list of computers and fax machines at the other end, and there are organized groups of this doing this all across the country for however many exchanges and area codes there are.

Mr. GILCHREST. Is there such a thing as—I guess there is.

In other words, even if it is an unlisted number?

Mr. SCHWARTAU. Yes.

Mr. GILCHREST. They have access to it?

Mr. SCHWARTAU. Yes.

Mr. WALKER. There was a hearing of a predecessor of this committee in 1984, I believe, and the movie "War Games" had just come out, and at the beginning of the movie "War Games" this kid in Seattle sets up exactly what Winn was talking about, and he went off and had—down to the arcade to play with his girlfriend while his computer went searching through various exchanges to find which ones responded, and then he would come in and it would give him a list: this number, to the best it could tell, was this kind of thing. He finally found one which, for reasons that don't make sense, was connected to a NORAD computer, and that's how the gist of the movie went on.

I suggest that one get that movie—it is still available in the video stores—because the beginning of it, the things that he is doing to hack computers are routinely available; anybody can do it.

Mr. GILCHREST. What is the name of that movie?

Mr. WALKER. "War Games."

Mr. GILCHREST. "War Games."

Mr. WALKER. Yes. In fact, at the hearing they showed parts of it, at the beginning of it, and it is still true. I mean not only still true, more true.

Mr. GILCHREST. If it is still true, is there a system that will block that?

Mr. WALKER. There are various things that one can do. For example, in many systems now, if somebody dials in, it takes the information as to who you are, and then it dials you back, so—and if it doesn't know who you are, it is not going to dial you back. I mean so that there are some routinely available techniques to do that, but, still, many, many computer systems have a way to have dial-in access from outside, and a lot of people don't realize the vulnerability that is there.

Mr. GILCHREST. I don't know if this was asked, but yesterday Washington's phone lines were down, for whatever reason. Could that possibly—could someone with a computer or the knowledge shut that system down? Is that possible?

Mr. BENINGTON. Well, I addressed that, and we hope it would not be the case. There is no doubt that hackers have had access to some parts of the phone system and that protective measures are being taken. There is a long list of protective measures that you can take.

I think Steve Walker would agree with me that that long list of measures, if properly taken, will provide a great deal of protection to a system. It has got to be monitored with discipline; the management has got to support it; that not always happens. So I couldn't say that something couldn't happen, because I would have to know what the management is doing and what steps they are taking to protect it and what risks they are willing to undergo.

But if you are aware of the problem and you give it some priority, without great expense, you can do a great deal to protect a system.

Mr. GILCHREST. I see.

And this demon dialing—not a very pleasant term—but in this demon dialing you hit an access to a computer, and then a computer figures out or tries to identify you. I would guess that the hackers know this and they know that they are going to try to be iden-

tified in a certain way. So is there a kind of—you know, in the old missile, anti-missile, anti-anti-missile——

Mr. WALKER. To every measure there is a countermeasure, yes. If I can effectively identify myself to this computer, then it will dial me back; no problem. Now you put extensive passwords and other capabilities in there so that, you know, it is hard to guess, and you don't let somebody do it more than three or four times a minute, or whatever, so that the time it takes is a long time. So there are measures. They all can be defeated if you try hard enough, but, in fact, people will get tired of trying before they succeed with many of them. It is an interesting play/counterplay business.

Mr. SCHWARTAU. There is a fairly good set of articles that U.S. Attorney William Cook from Chicago—and he has had a long history of successful prosecution of telecommunications fraud more than anything else—isn't it?—and he has a number of published articles on the subject, which are very, very telling, which may be valuable to you in the educational process.

Mr. GILCHREST. Thank you. Thank you, gentlemen. Thank you, Mr. Chairman.

Mr. MCMILLEN. Thank you.

I guess it is my turn to ask some questions.

You know, what is interesting about this whole issue, it is directly related to a subject that I have a lot of interest in, and that is economic intelligence, one of those buzz words that people don't like to talk about in this country, but it seems to be that quite a bit of it is going around in the world.

There is this Orwellian fear in America that somehow Government is going to be all over your lives and it is going to create problems in terms of privacy. I think it is a realistic fear, but I think, using a basketball analogy, if you will, it seems to me that we are always trying to find defenses for Michael Jordan. He has always got the newest move, the newest spin, pretty hard to do. The attackers have more capability in technology than oftentimes the defenders, and in this case the Government is the defenders, our businesses are defenders, and when you extrapolate and trend that out, that is a very disconcerting trend, because it means that unless your Government decides that it is going to go aggressively at the economic intelligence arena and have an offensive strategy, that we are going to be continually dealing with these kinds of intrusions in our businesses and our Government. It is very difficult. The best systems, the best management, are going to probably be efficient in dealing with this problem in toto, and so I would like to have you comment upon that a little bit, just in general about the—kind of the arms race, if you will, the hackers versus the enforcers. What can we do to assist in trying to make our forces more capable? And also the issue of economic intelligence and whether the United States should be more aggressive in those areas.

One of the things the administration doesn't like to talk about is certain national strategies, and this economic intelligence, as you know, is not a very popular word with the administration, but give us some of your thoughts on that.

Mr. BENINGTON. If I could start, I don't think that the hackers are as tall, if I may use another analogy, as possibly you make them.

When I briefed the task force report to the CEO's of the members of NSTAC, the major telecommunication companies and service and equipment providers, I told them some stories about generically how their systems had been penetrated, and also some Government experts had been telling them a story before me, and then I said to them, "The thing that is important to recognize is that in virtually all of these cases it was very poor security practices on your part that allowed the penetration to take place," and just to give you two examples, people take manuals for complex systems that they have, and they have model 26, and then model 27 comes along, so they throw the manual for model 26 into a dumpster, and then that night a hacker comes along and gets that manual and reads how the system works. Well, that is just horrible practice.

Another example is, vendors sell very complex switches, and they have password features so that you can only sign in if you use a password, but in order to get the system started there has to be what they call a default password, like, "One, two, three, four, five, six," and they turn the system on, and they use it for three years, and they never change the default password, and these brilliant hackers know that that was the default password, in part because they picked it up in a dumpster, that it was, and they try it, and it works.

So if you are not going to take steps, then you are very vulnerable, but there are steps that can be taken that give you a great deal of protection.

Mr. WALKER. To follow up on Herb's comments, in the economic intelligence area one of the things I was emphasizing earlier was the need for cryptographic mechanisms, and the crucial thing in there is the need for an exportable cryptographic mechanism. As long as we don't have that, manufacturers aren't going to put these into their products and industry and Government is going to continue to send its information over networks in the clear.

Mr. MCMILLEN. May I interrupt? There is some legislative—do you think that is something that the Congress should do? When I read your testimony, you thought that maybe Congress should address a cryptographic standard of sorts.

Mr. WALKER. You people have been asking for a public key algorithm for a long time, and NIST has been promising it for a long time, and it is still not here.

Mr. MCMILLEN. We may have to do it for them?

Mr. WALKER. Well, here's the problem. If—I mean to represent the other side here, if, in fact, we put out an encryption algorithm that could be widely used in industry and could protect industry and Government from industrial espionage of whatever sort, the risk is that other people will use it and it will make it harder for us to listen in on other people's communications, and right now the pendulum is completely on the side of, let's not let anything happen because the other guy might be able to do something better. As a result, we have a lot of the vulnerability that you were just talking about. Somehow, the pendulum has got to come back. I

don't care whether it is DES or any other algorithm; there has to be some algorithm that we can use.

Mr. McMILLEN. But if the standard is too high—I know NSA has this concern——

Mr. WALKER. Indeed. Don't make it so high.

Mr. McMILLEN [continuing]. And we export, you know, a high standard around the world, won't that certainly impair our ability to—

Mr. WALKER. Yes, but you can go to Europe and buy DES chips almost on the street. RSA public key cryptography, because there is no patent restrictions on it in Europe, is widely used. In fact, the Europeans are trying to export it to the United States. The horse is out of the barn. I mean that has already happened.

Now, we can continue to say, well, we don't want to see that happen any more because the longer we put it off, the better we are, but your industrial espionage, your economic espionage, problems are heightened dramatically by the lack of progress we have made in this area.

Mr. McMILLEN. Any final comments?

Mr. SCHWARTAU. Yes, absolutely.

We keep talking about—referring to hackers, and hackers are isolated, unorganized, basically, individuals that perhaps don't have any real motivation other than rebellion, technical rebellion, or they are on a search to find the ends of the operating system, which is the claims of some of them. I don't think that we have to worry as much about hackers as we do about organized groups who are much more well organized, well funded, and well motivated, who may have real reason to do penetrations of systems for either economic or industrial advantage.

But, on the other hand, when we talk about protecting them, we have to also accept the fact that there is a very large group out there who wants no protection whatsoever, and there are an awful lot of open systems advocates, primarily out of academia, who want to keep absolute total exchange of information absolutely free to anybody with a modem and dial-up, and they purposefully keep the passwords either nonexistent or very common to make the flow of information very easily. And, one of the unfortunate ramifications of that is that many of the academic systems are directly tied in to Government and military networks, so we are compounding the problem right there by some of those advocacies.

Mr. McMILLEN. I appreciate your comments on that issue and certainly appreciate your testimony and your answers to the questions that have been posed today, and, with that, we will move to our second panel and thank you, gentlemen.

The panelists are: Mr. Howard Rhile, Junior, Information Management and Technology Division, the General Accounting Office; the second panelist is Mr. Raymond Kammer, deputy director of the National Institute of Standards and Technology in Gaithersburg, Maryland.

Thank you, gentlemen, for coming today. Why don't we begin with Mr. Rhile.

STATEMENTS OF HOWARD G. RHILE, JR., INFORMATION MANAGEMENT AND TECHNOLOGY DIVISION, GENERAL ACCOUNTING OFFICE, WASHINGTON, DC, ACCOMPANIED BY ANTHONY N. SALVEMINI, SENIOR EVALUATOR; AND RAYMOND G. KAMMER, DEPUTY DIRECTOR, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, GAITHERSBURG, MD

Mr. RHILE. Thank you, Mr. Chairman.

I would like to introduce my colleague on my left, Mr. Tony Salvemini, who has done a lot of the work in the area that I am about to discuss, and I would also like to summarize my statement, if I may, and ask that the full statement be placed in the record.

Mr. MCMILLEN. With unanimous consent, your statement will be included in the record.

Mr. RHILE. Thank you, Mr. Chairman.

First of all, I would like to say that we are pleased to be here today to discuss our work in this area at the Department of Justice. As many of us know, the Department relies on computer systems to protect highly sensitive information, including the names of defendants, witnesses, informants, undercover agents, and the like, and our work over the past three years for the Subcommittee on Government Information, Justice, and Agriculture in the House Committee on Government Operations has identified many disturbing weaknesses in Justice's implementation of the Computer Security Act and the applicable regulations.

I might say that the weaknesses we identified are not mere inconveniences, as occurred yesterday with the telephone system; these weaknesses that we have identified have life and death implications for people whose identities might have been compromised as the result of inadequate control over this information. So we are talking about the ultimate security problem here, and let me just recap a little bit some of the problems that we did find.

In 1989, we found that although highly sensitive information would be contained in one of the Department's systems called Project Eagle, the Department had no security plans for this system nor had it conducted any risk analyses. This system, called Eagle, is composed of about 12,000 work stations at 200 sites nationwide processing information such as the names of defendants and witnesses.

The Department was going to wait until after the systems were installed and operational before performing a risk analysis or developing security plans. We took issue with this approach, and the Department agreed to prepare security plans and do these analyses. Our recent follow-up work, however, shows that, although some improvements have been made, there are still several locations where the risk analyses have not been completed even though the system has been installed, and the security plan is still not in its final form. That was 1989.

In 1990, we found that Justice was not ensuring that its highly sensitive computer systems were adequately protected. We found again many disturbing weaknesses that could compromise both the computer systems and the information that they process. These weaknesses, we felt, were caused by inadequate leadership, inadequate oversight by the Justice Management Division, which is a

headquarters unit of the Department of Justice that is responsible for developing and directing the computer security program of the Department.

We found, for example, that within its seven litigating organizations—these are the people who do the prosecuting and so forth—that contingency plans were not there to combat interruptions to the computer systems, or they had not been tested; they had a plan, but they never tested it; they don't know whether it works; and there was no mandatory computer security training, as required by the Act.

That same review, we also found several material weaknesses in physical and other security at the Department's main data center in Rockville. Justice processes a lot of classified, a lot of sensitive information at this facility and plans to process national security information.

We found, for example, that access to the data center was not properly controlled. An electronic card key device that records when employees enter and exit the facility didn't record, store, or generate any reports on activities of the card holders, so you couldn't reconstruct any events that may have occurred. Guards were not positioned to monitor survey—to monitor the activities in the center, and there were other major problems.

This year, just three months ago, we testified about another example of inadequate computer security at the Department. We reported the results of our investigation of last summer's security breach in Lexington, Kentucky, in which computer equipment excessed by the U.S. Attorney's Office was found to have highly sensitive information on it, including grand jury material, information regarding confidential informants. How this could happen, Mr. Chairman, is shocking in itself, but even more dangerous is the fact that it is still going on.

Several months after this incident, a different U.S. Attorney's Office cautioned Federal and local officials that again sensitive information might have been compromised, information again that has life or death implications.

We have to conclude, Mr. Chairman, that until Justice radically changes its approach to computer security one just can't trust that sensitive data will be safely secured. These problems that we have identified in Kentucky and elsewhere are systemic, they are not isolated incidents, and they require dedicated and focused Department-wide attention to bring about changes that are needed.

Now our reports and our testimony in the past has contained a number of recommendations to the Attorney General to fix these problems. In March of this year, the Department acknowledged the need for improved computer security and identified a number of efforts under way to address the computer security problems. These actions included a more proactive leadership role on the Department—on the part of the Department's security staff, a major security upgrade of the Department's data center, increased security awareness training, and more aggressive oversight by the Department of the preparation and the utilization of contingency plans.

Later, in April, the Attorney General also directed that the Department conduct immediate reviews of the security programs of the various agencies, and then last month the Assistant Attorney

General for Administration directed component heads to provide him with their plans to ensure that all Justice employees receive mandatory computer security awareness training by November of this year.

So I think it is apparent that the Department of Justice has recognized the importance of computer security and is beginning to take some steps necessary for improvement, but the Department has a long way to go, and we don't know yet how effective these actions will be. Continued oversight by this committee, by the Congress, and others, and by Justice's top management will be required to maintain these improvements and to achieve them.

That summarizes my statement, Mr. Chairman. I would be happy to respond to any questions.

[The statement of Mr. Rhile follows:]

United States General Accounting Office

GAO

Testimony

For Release
on Delivery
Expected at
9:30 p.m. EDT
Thursday
June 27, 1991

Computer Security Weaknesses at the Department of Justice

Statement of
Howard G. Rhile
Director, General Government Information Systems
Information Management and Technology Division

Before the
Subcommittee on Technology and Competitiveness
Committee on Science, Space, and Technology
House of Representatives

B-233809

Mr. Chairman and Members of the Subcommittee:

We are pleased to be here today to discuss our work in the area of computer security at the Department of Justice. The Department relies on computer systems to process highly sensitive information, including the names of defendants, witnesses, informants, and undercover law enforcement officials. The dependence on computer systems to process sensitive information presents considerable risk. If the systems and/or Justice employees fail to protect this information from unauthorized access and disclosure, individuals could be harmed and public trust eroded.

Our work over the past 3 years for the Subcommittee on Government Information, Justice, and Agriculture, House Committee on Government Operations, identified many disturbing weaknesses in Justice's implementation of the Computer Security Act of 1987 and applicable regulations. The weaknesses we identified have life-and-death implications for individuals whose identities may have been compromised because of inadequate control over sensitive information contained in the Department's computer systems.

As you know, the Computer Security Act of 1987 requires federal agencies to develop security plans for computer systems that they designate as containing sensitive information, and to establish

mandatory computer security training to make employees aware of their specific responsibilities and how to fulfill them. The Federal Information Resources Management Regulation (41 C.F.R. part 201-7) and Office of Management and Budget policies further direct agencies to protect access to and operation of computer systems by requiring that agencies (1) conduct risk analyses to identify areas of vulnerability, and (2) prepare and test contingency plans.

The fact remains, Mr. Chairman, that the Department of Justice has not been ensuring that its highly sensitive computer systems are protected. Recognizing its vulnerability and the need to improve its computer security status, the Department is now taking more of a leadership role. In recent months, the Department has taken a number of actions designed to address its computer security deficiencies.

SENSITIVE COMPUTER SYSTEMS FOUND VULNERABLE

In 1989 we found that, although highly sensitive information will be contained in the Project EAGLE systems, Justice had not developed security plans or conducted risk analyses for these systems.[1] The EAGLE network is composed of integrated systems

---

[1]Justice Automation: Security Risk Analyses and Plans for Project EAGLE Not Yet Prepared (GAO/IMTEC-89-65, Sept. 19, 1989). EAGLE stands for Enhanced Automation for the Government Legal Environment.

with 12,000 workstations in 200 sites nationwide processing sensitive information, such as the names of defendants and witnesses. Justice was going to wait until after the Project EAGLE systems were installed and operational before performing the required risk analyses or developing security plans. After we took issue with this approach, however, Justice officials agreed to prepare the security analyses and security plans prior to the installation and operation of the EAGLE systems. Our recent preliminary followup work shows that some improvements have been made. Nevertheless, risk analyses are still not being completed before installation of the systems in some locations and all vulnerabilities identified by risk analyses that have been done are not being corrected expeditiously. Moreover, Justice is still finalizing its security plan for the EAGLE systems.

In 1990 we found that Justice was not ensuring that its highly sensitive computer systems were adequately protected. We identified many disturbing weaknesses in existing security that could severely compromise both the computer systems and the sensitive information they process. We reported that these weaknesses reflected inadequate leadership and oversight by the Justice Management Division, which is responsible for developing and directing the Department's computer security programs. Within Justice's seven litigating organizations, for example, we found that contingency plans necessary to combat service

interruptions to the computer systems used to process sensitive information either had not been prepared or were not tested.[2] Further, no mandatory computer security training was being provided to employees.[3]

During this review, we also found several material weaknesses in physical and other operational security at Justice's main data center. Justice processes sensitive information at this facility, and plans to process classified information. Our review disclosed, for example, that access to the data center was not properly controlled. An electronic card-key device that records when employees enter and exit did not record, store, or generate reports on activities of cardholders; therefore, center officials could not reconstruct these events if they needed to investigate a security breach. Further, guards were not positioned to visually survey activities in the center, and video monitors, where used, lacked recording mechanisms to store and replay information should it be needed. At present, Justice is in the process of making major security upgrades to its data center.

---

[2]Justice's litigating organizations include 94 U.S. Attorney's Offices and six divisions--Antitrust, Civil, Civil Rights, Criminal, Land and Natural Resources, and Tax.

[3]Justice Automation: Tighter Computer Security Needed (GAO/IMTEC-90-69, July 30, 1990).

Just 3 months ago we testified about yet another example of inadequate computer security at the Department of Justice.[4] We reported the results of our investigation of last summer's security breach in Lexington, Kentucky, in which computer equipment excessed by the U.S. Attorney's Office was later found to contain highly sensitive data, including grand jury material and information regarding confidential informants. How this could happen is shocking in itself, but even more dangerous was Justice's ongoing vulnerability. As recently as this past February, a different U.S. Attorney's Office cautioned federal and local officials that, again, sensitive data that could potentially identify agents and witnesses might have been compromised.

Mr. Chairman, the highly sensitive nature of our Kentucky investigation's findings precludes us from being able to fully describe in open session all of the details of what we uncovered. I can say, however, that we found patterns of neglect and inattention nationwide that have resulted in Justice's compromising sensitive information that could result in the possible loss of life of individuals whose identities may have been disclosed.

---

[4]Justice's Weak ADP Security Compromises Sensitive Data (Public Version) (GAO/T-IMTEC-91-6, Mar. 21, 1991).

DECISIVE ACTION LONG OVERDUE

Our investigations since 1989 lead to the unmistakable conclusion that until Justice radically changes its approach to computer security, one cannot trust that sensitive data will be safely secured at the Department. The problems brought to light by the Kentucky incident and our other investigations are systemic--and they require dedicated, focused, Departmentwide attention to bring about the changes that must be made. Such attention must be sustained.

Our reports contained recommendations to the Attorney General to (1) ensure that the computer security weaknesses we found were properly corrected, (2) strengthen the Justice Management Division's leadership and oversight of departmental computer security programs, and (3) report the computer security deficiencies as a material internal control weakness under the Federal Managers' Financial Integrity Act. We further recommended that the Office of Management and Budget designate computer security at the Department of Justice as a high-risk area.

JUSTICE'S ACTIONS: A BEGINNING

In March of this year, the Department acknowledged the need for improved computer security, and identified efforts either planned or underway to address the agency's computer security deficiencies. These actions include (1) a more proactive leadership role on the part of the Department's security staff in the Justice Management Division, (2) a major security upgrade of the Department's data center, (3) increased security awareness training, and (4) more aggressive oversight of the preparation and utilization of contingency plans. In addition, in April 1991, the Attorney General directed the heads of Department components to conduct immediate reviews of their security programs. And last month, the Assistant Attorney General for Administration directed component heads to provide him with their plans to ensure that all Justice employees receive mandatory computer security awareness training by November 1, 1991.

It is apparent that the Department of Justice has recognized the importance of computer security, and is beginning to take the steps necessary for improvement. However, Mr. Chairman, we do not yet know how effective the Department's actions will be. Continuing oversight by the Congress and Justice's top management will be required to sustain needed improvement.

- - - - -

Mr. Chairman, this concludes my prepared statement. I would be pleased to answer any questions that you or members of the Subcommittee may have at this time.

Mr. McMillen. Thank you very much.

We will turn now to Mr. Kammer.

Mr. Kammer. I am Ray Kammer.

I will cover three topics today: awareness and education efforts, international issues related to computer security, and the development of a family of data protection standards.

Awareness and education are still inadequate nationally and in the Federal Government. I think it is pretty clear we need a more organized collection of data to improve public awareness of system threats and risks, and we need more education about secure systems, and we need more training in security practices and in ethics.

One of the things that we have been trying to do in the Government is upgrade the attention that is paid by agencies to security. And in aid of that, led by Jim MacRae of OMB, whose testimony was put in the record, we have conducted a series now of 13 visits to major agencies. We started with agencies that had higher ratings of problems with respect to computer security, and out of those visits we have noticed that there are some common needs that have been expressed by the agencies, and among them are protection of electronic data, digital signature capabilities, and contingency planning and risk management techniques, and indeed we are factoring these agency needs into our program planning.

We have also continued to support computer emergency response programs as a tool for raising awareness and helping security managers throughout Government to respond to threats and risks and failures. In aid of that, we have established our own response capability designed to field calls on a 24-hour basis to ensure that Federal agency users with computer security problems are put in contact with computer security assistance when they need it.

We have also devoted a lot of effort over the past year to international activities. One of the important efforts was contributing to the work of international—of ISO, the International Organization for Standardization, and, in particular, Standing Committee 27, which is focused on information technology security techniques.

Also during the past year, we have reviewed two versions of the Information Technology Security Evaluation Criteria, usually called ITSEC. These were developed by the Governments of the United Kingdom, Germany, France, and the Netherlands, and ITSEC is an effort on their part to harmonize the different security criteria of the countries into a single document with the potential to become a European Community standard.

In formulating our position on ITSEC, we worked with NSA, with other Federal agencies, and with U.S. industry. We felt that the ITSEC document was incomplete in many respects, especially because it tended to focus on the correctness and effectiveness of the evaluation process more than on the sets of security functions that were needed by the user. We really aren't sure that a system developed and evaluated against the ITSEC would inherently help improve the security posture of its users.

Some changes have been made to the ITSEC as a result of our discussions. The four nations plan to begin using the ITSEC as the basis for their product evaluations. We will continue to cooperate with them to gain an understanding of the evaluation process, and

toward that end we have a cooperative project under way with DARPA, DARPA being the developers of a U.S. trusted system called TMach, which just means "Trusted Mach." The Commission of the European Communities is also cooperating in the U.K. and German Governments. Our intent is to use the ITSEC to evaluate TMach, which we know the characteristics of pretty well, and see if that evaluation process yields a sensible answer. The intent here is to try and avoid multiple testing requirements that would be expensive for users and vendors.

I would like to talk a little bit now about new trusted systems technology. We all feel that a new standard is needed on trusted systems technology, and trusted computer systems developed to meet the current TCSEC requirements for confidentiality or classified information don't really meet the protection needs of unclassified systems which tend to have greater connectivity, which means they are not physically isolated, and, in fact, to use them, you probably want to be able to dial from remote locations, and frequently value integrity requirements over confidentiality. People don't mind if the information is disclosed, but they would have big problems if the information were changed. NIST and NSA have agreed to work together on developing this new Federal standard.

Testing for conformance to the new standard is an issue that we must consider. NIST operates the Voluntary Laboratory Accreditation Program which accredits various kinds of organizations to conduct standardized conformance tests. In our testing activities, we want to work towards reciprocity with other organizations conducting testing, and I should point out that the European Governments—and presumably the EC as a whole will also be—are strongly in favor of government-controlled third-party testing.

A case must be built by us for the usefulness and validity of manufacturer-conducted testing for computer security products, especially those intended for non-high-risk environments. In the United States, it would be a considerable economic disadvantage if the testing weren't possible to be done by the vendors as opposed to being done by the Government, which is what will be expected in Europe.

I would like to talk a little bit now about data protection standards. Last year, we initiated a revision of FIPS 140. This is a standard for using the data encryption standard in telecommunications networks. We have had excellent cooperation from Government and industry organizations in developing a revised standard and in reviewing it. We are analyzing the comments that we received, and we expect to move forward on the revised FIPS 140 for general security requirements for cryptographic modules.

I know you are very interested in our progress in developing a Federal digital signature standard based on the principles of public key cryptography. I am pleased to tell you that we are working out the final arrangements on the plan's standard, and we hope to announce later this summer our selection of a digital signature standard based on a variant of the ElGamal signature technique. Our efforts in this area have been slow; they have been difficult; and they have been complex. We have evaluated a number of alternative digital signature techniques and considered a variety of factors in this review, among them the level of security that is provided, the

ease of implementation in both hardware and software, the ease of export from the United States, the applicability of patents, and the level of efficiency in both the signature and verification functions that the technique performs.

In selecting a digital signature technique method, we followed the mandate contained in section 2 of the Computer Security Act, which told us to develop standards and guidelines that assure the cost-effective security and privacy of sensitive information in Federal systems. We placed primary emphasis on selecting the technology that best assures the appropriate security of Federal information. We were also concerned with selecting the technique with the most desirable operating and use characteristics.

In terms of operating characteristics, the digital signature technique provides for—that we selected, provides for a less computationally intensive signing function than it does verification function, and this matches up well with what we expect to be the Federal use pattern. The signing function is expected to be performed in a relatively computationally modest environment, perhaps with a smart card, whereas the verification process can be conducted in an environment that is computationally rich, such as on a mainframe computer or super-mini.

With respect to use characteristics, the digital signature technique is expected to be available on a royalty-free basis in the public interest worldwide. This should result in broader use by both Government and the private sector and bring economic benefits to both sectors. Broadest possible use in the Federal Government will be encouraged by an agreement that we have received from the Department of Defense that this digital signature technique may be used to sign unclassified data processed by Warner Amendment Systems and also for selected classified applications.

We will be able to release the actual algorithm for public review and comment as soon as we have submitted our application to the U.S. Patent Office for a patent, which is being written up now. This should take about another month and a half, and then over the next year, once we have filed the U.S. patent, we can release the algorithm publicly, and we have a grace period of 12 months to make decisions on which, if any, foreign patent protection we should seek. As I stated, we intend to make the technique available worldwide on a royalty-free basis in the public interest.

A hashing function, which will be necessary for use of digital signature, has not yet been specified by us for use. We have reviewed various candidate hashing functions. However, we are not satisfied with any of the functions that we have studied thus far. We will provide a hashing function that is complementary to the standard.

I would like to speak to two issues that have been speculated about with respect to our efforts in this area. I would like to say, first of all, there is no trapdoor that has been designed into this standard nor does anybody in the U.S. Government know of any characteristic that is inherent in the ElGamal signature method that would make it accessible.

Another issue raised is the lack of a public key exchange capability that would come into play in the securing of your first digital signature, if you will, getting the first one associated with you. It is my analysis that if we don't require some form of proof of identity

at that first step, such as is done for getting a driver's license or a passport, that all the rest of the security is kind of an illusion, and you need at least to have people show up once physically and prove who they are, which is something that you don't do when you use a public key exchange methodology for issuing the first key. The level of security that will be required or the level of proof of identity is a decision to be made by the users of the system. In the private sector, they can specify whatever level they want. I am interested in seeing what levels the people like the IRS and the Social Security Administration and the Veterans' Administration will want for proof of identity, but that is a decision for them to make, not for NIST.

With respect to the NIST-NSA technical working group, it has been a very productive, very fruitful relationship. A lot of the reasons why we have not made progress at the speed that we wished to have been technical. This is a very difficult set of problems. Many of the things that people seem so casual about saying work wonderfully, we discovered, don't work wonderfully, some of them don't do what they are said to do, and it took us a long time to work our way through that. NSA has been tremendously helpful in this process.

Thank you for your interest, your support.

[The prepared statement of Mr. Kammer follows:]

UNITED STATES
DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS
AND TECHNOLOGY

U.S. DEPARTMENT OF COMMERCE

STATEMENT OF RAYMOND G. KAMMER, DEPUTY DIRECTOR

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

BEFORE THE SUBCOMMITTEE ON TECHNOLOGY AND COMPETITIVENESS

OF THE COMMITTEE ON SCIENCE, SPACE AND TECHNOLOGY

ON COMPUTER SECURITY IMPLEMENTATION

HOUSE OF REPRESENTATIVES

JUNE 27, 1991

Mr. Chairman and Members of the Committee:

Thank you for inviting the National Institute of Standards and Technology to speak about its computer security programs. We share your interest in strengthening computer and communications security, and we continue to give high priority attention to implementing the Computer Security Act of 1987. We are working on many fronts, developing both the technology and the standards that will be needed in the long term, and addressing the short term needs for better management controls and awareness.

This progress report on our activities focuses on three principal topics: awareness and education efforts; international issues related to computer security; and the development of a family of data protection standards.

Awareness and Education

Awareness and education are still inadequate nationally and in the Federal Government. We need more organized collection of data to improve public awareness of system threats and risks, more education about secure systems, and training in security practices and ethics.

Agency Visits

We contributed to an important education and data collection effort organized by the Office of Management and Budget to visit agencies to discuss computer security with senior officials and to review agency requirements for guidance and assistance. OMB will report to you in detail on these visits. However, I want to confirm that the visits have been productive and have given us better insights into agency needs. Some of the common needs expressed by the agencies include protection of electronic data interchange transactions, digital signature capabilities, and contingency planning and risk management techniques. We are factoring these agency needs into our internal program planning.

Computer Emergency Response Teams (CERT)

We continued to support computer emergency response programs as a tool for raising awareness and helping security managers throughout government to respond to threats, risks and failures. We played a principal role in the establishment and operation of a cooperative group of computer security incident response activities, known as the CERT System. This group shares information on computer security incidents, system vulnerabilities, and related information. NIST serves as the secretariat of the group and works to expand membership both within and outside of government. We have established our own response capability designed to field calls on a 24-hour basis and ensure that federal agency users with computer security problems are put in contact with computer security assistance when they need it.

Assistance to Educators

This year, we assumed the sponsorship of a national educators forum. This forum gives us an opportunity to promote the development of consistent and effective training programs based on good practices for computer security.

Other Outreach Activities

NIST has greatly expanded the capability and content of its Computer Security Bulletin Board System to better serve the information needs of the federal government. The bulletin board now supports several simultaneous users and contains several hundred bulletins and files on a wide range of computer security topics. It also contains all alerts and bulletins issued by the CERT System.

We have started issuing our own bulletins both in paper form and on the bulletin board to provide timely advice to users on specific topics of significant interest. Some of the topics covered were the Data Encryption Standard and related standards, the use of trusted systems technology, and prevention of virus attacks.

An electronic mail "forum" that we are establishing for computer security managers throughout the government will provide still another way to get help. The forum will enable direct contact among NIST and federal computer security managers on a daily basis.

International Activities and Trusted Systems

We devoted a lot of effort over the past year to international activities. We have actively supported the development of international standards for computer security to foster fair competition in international markets. Both users and vendors are negatively affected by the lack of computer security standards for computer systems that can be purchased and used worldwide. We have contributed to the work of International Organization for Standardization (ISO) Standing Committee 27 (SC27), Information Technology Security Techniques. Issues being addressed in SC27 include standards for security evaluation criteria and for security services, guidelines and techniques.

Security evaluation criteria are standards against which computer and network systems can be evaluated with respect to security characteristics. Different approaches and different goals have resulted in the development of various evaluation criteria systems.

During the past year we reviewed two versions of the Information Technology Security Evaluation Criteria (ITSEC) which were developed by the governments of the United Kingdom, Germany, France and the Netherlands. This document attempted to harmonize the different security criteria of the four countries into a single document with the potential to become a European Community

standard. The four nations developed the ITSEC to provide a basis for reciprocity in the evaluation of security-related products between EC member nations. European products are excluded from the evaluation process conducted by the National Security Agency (NSA) under the Trusted Computer System Evaluation Criteria (TCSEC), known as the "Orange Book."

In formulating our position on the ITSEC, we worked with NSA, other federal agencies, and US industry. We felt that the ITSEC document was incomplete in many respects, especially because it tended to focus on the correctness and effectiveness of the evaluation process more than on the sets of security functions needed by users. We were not sure that a system developed and evaluated against the ITSEC would inherently help improve the security posture of its users. However, in discussing this position with the Europeans, we stressed our willingness to work together on the evolution of international security criteria, including the development of an international approach for testing products and systems.

Some changes have been made to the ITSEC as a result of our discussions. The four nations plan to begin using the ITSEC as the basis for their product evaluations. We will continue to cooperate with them to gain an understanding of the evaluation process. Toward that end, we have a cooperative project underway with Defense Advanced Research Projects Agency (DARPA), the

developers of a U.S. trusted system (Trusted Mach (TMach)), the Commission of the European Communities (CEC), and the UK and German governments to evaluate TMach using the ITSEC. We expect to learn about their evaluation process and how a compatible U.S. evaluation process might be established. Our goal is to avoid multiple testing requirements that will be expensive for users and vendors.

Other International Activities

During 1990 and 1991, NIST has held a series of informal meetings with officials of the CEC's Directorate General XIII. These meetings have been designed to gain NIST a more influential role in participating with the CEC and member nations on computer security projects of mutual interest. NIST and CEC officials drafted a Memorandum of Understanding on EC/US Information Security Cooperation. This draft MOU has been circulated informally among the member nations' senior information security officials. After informal approvals, we plan to go forward through the appropriate channels to get formal approvals.

We have also met with information security officials of the UK, Germany, and France to work on mutual cooperation, document harmonization, and framing of joint projects. There is a spirit of openness and willingness to work with NIST shown in these meetings. This appears to be the direct result of NIST

participation in the review of the ITSEC and the work on the CEC MOU. As a result, a significant amount of information sharing has taken place, along with informal involvement in various projects.

In addition, we met with information security officials of the governments of Canada, Sweden, and Australia. Canada has already published its draft Trusted Computer Product Evaluation Criteria document, which covers some of the middle ground between the TCSEC and the ITSEC in the areas of security functionality specification and assurance.

New Trusted Systems Technology Standard

A new federal standard is needed on trusted systems technology. Trusted computer systems developed to meet TCSEC requirements for confidentiality of classified information do not fully meet the protection needs of unclassified systems, which tend to have greater connectivity and frequently stress integrity requirements over confidentiality.

NIST and NSA have agreed to work together on developing this new federal standard that would be used to specify computer security requirements for federal procurements. This new standard will address computer protection requirements in the rapidly evolving open system environment, including distributed applications such

as Electronic Data Interchange (EDI). We expect to draw on the current TCSEC, the Europeans' ITSEC, the Canadian criteria, and other relevant documents to help create a basis for international harmonization of security specifications and assurance techniques.

Testing for conformance to the new standard is an issue that we must consider. NIST operates the Voluntary Laboratory Accreditation Program (NVLAP), which accredits various kinds of organizations to conduct standardized conformance tests. Computer products with security capabilities could also be tested under such a program. We want to consider a range of assessment methods for the new standard, including the current process and manufacturer conducted testing as well. This approach, of course, will have to be carefully instituted and controlled.

In our testing activities, we want to work toward reciprocity with other organizations conducting testing. I should point out that European governments are strongly in favor of government-controlled third-party product testing. A case must be built for the usefulness and validity of manufacturer-conducted testing for computer security products not intended for high-risk environments.

Open Systems Interconnection (OSI) security standards

We continued to support the development of standards for security of Open Systems Interconnection (OSI) networks. This is a high priority need for Federal agencies as they implement the Government Open Systems Interconnection Profile (GOSIP) standard. We are working toward international standards that will meet government needs for the security of sensitive, unclassified data transmitted through OSI networks.

Family of Data Protection Standards

NIST has identified requirements for a family of data protection standards to control access to computer systems and to protect data integrity and confidentiality. Last year we initiated the revision of FIPS 140, a standard for using the Data Encryption Standard in telecommunications networks. FIPS 140 was outdated, and needed revision to allow for the use of new cryptographic techniques. We have had excellent cooperation from government and industry organizations in developing a revised standard and in reviewing it. We are analyzing the comments that we received, and expect to move forward on the revised FIPS 140 for General Security Requirements for Cryptographic Modules.

Digital Signature Standard

I know that you are interested in our progress in developing a federal digital signature standard based upon the principles of public-key cryptography. I am pleased to tell you that we are working out the final arrangements on the planned standard, and hope to announce later this summer our selection of a digital signature standard based on a variant of the ElGamal signature technique.

Our efforts in this area have been slow, difficult, and complex. We evaluated a number of alternative digital signature techniques, and considered a variety of factors in this review: the level of security provided, the ease of implementation in both hardware and software, the ease of export from the U.S., the applicability of patents and the level of efficiency in both the signature and verification functions that the technique performs.

In selecting digital signature technique method, we followed the mandate contained in section 2 of the Computer Security Act of 1987 to develop standards and guidelines that ". . . assure the cost-effective security and privacy of sensitive information in Federal systems." We placed primary emphasis on selecting the technology that best assures the appropriate security of Federal information. We were also concerned with selecting the technique with the most desirable operating and use characteristics.

In terms of operating characteristics, the digital signature technique provides for a less computational-intensive signing function than verification function. This matches up well with anticipated Federal uses of the standard. The signing function is expected to be performed in a relatively computationally modest environment such as with smart cards. The verification process, however, is expected to be implemented in a computationally rich environment such as on mainframe systems or super-minicomputers.

With respect to use characteristics, the digital signature technique is expected to be available on a royalty-free basis in the public interest world-wide. This should result in broader use by both government and the private sector, and bring economic benefits to both sectors.

A few details related to the selection of this technique remain to be worked out. The government is applying to the U.S. Patent Office for a patent, and will also seek foreign protection as appropriate. As I stated, we intend to make the technique available world-wide on a royalty-free basis in the public interest.

A hashing function has not been specified by NIST for use with the digital signature standard. NIST has been reviewing various

candidate hashing functions; however, we are not satisfied with any of the functions we have studied thus far. We will provide a hashing function that is complementary to the standard.

I want to speak to two issues that have been raised in the public debate over digital signature techniques. One is the allegation that a "trap door", a method for the surreptitious defeat of the security of this system, has been built into the technique that we are selecting. I state categorically that no trap door has been designed into this standard nor does the U.S. Government know of any which is inherent in the ElGamal signature method that is the foundation of our technique.

Another issue raised is the lack of public key exchange capabilities. I believe that, to aviod capricious activity, Public Key Exchange under control of a certifying authority is required for government applications. THe details of such a process will be developed for government/industry use.

NIST/NSA Technical Working Group

Aspects of digital signature standard were discussed by the NIST/NSA Technical Working Group, established under the NIST/NSA Memorandum of Understanding. The Working Group also discussed issues envolving the applicability of the digital signature algorithm to the classified community, cryptographic key

management techniques, and the hashing function to be used in conjunction with the digital signature standard. Progress on these items has taken place; however, as with the digital signature standard, non-technical issues such as patents and exportability require examination, and this can be a lengthy process. We have found that working with NSA is productive. The Technical Working Group provides an essential mechanism by which NIST and NSA can conduct the technical discussions and exchange contemplated by the Computer Security Act and also allows us to address important issues drawing upon NSA's expertise.

Conclusion

We have had a productive year, and have contributed to many more activities than I can cover in this statement. Improving computer security is both a technical problem and a social problem. We are addressing both and cooperating with government, industry, and international organizations that are also trying to find solutions to the problems.

We thank you for your past interest and support. I hope that I have addressed the questions that you had, and I invite other questions or comments.

RAYMOND G. KAMMER

Deputy Director
National Institute of Standards and Technology (NIST)
(Formerly National Bureau of Standards (NBS)
United States Department of Commerce

Ray Kammer is Deputy Director of NIST and at present is Acting Director of the National Measurement Laboratory. NIST is the Nation's central laboratory for measurement and standards research in support of U.S. industrial needs.

A graduate of the University of Maryland, Kammer joined NIST in 1969 as a technical program analyst. Over the following decade he served the agency and the U.S. Department of Commerce in a succession of offices concerned with budgetary and program analysis; planning; and personnel management. In 1980, Kammer was appointed Deputy Director of NIST.

In addition, Kammer has served as chairman of several important evaluation committees for the Department of Commerce, including reviews of satellite systems for weather monitoring and the U.S. LANDSAT program, and the next generation of weather radars used by the U.S. government. He has just completed the first source evaluation process for the Advanced Technology Program.

His awards include both the Gold and Silver medals of the Department of Commerce, the William A. Jump Award for Exceptional Achievement in Public Administration, the Federal Government Meritorious Executive Award, and the Roger W. Jones Award for Executive Leadership.

February 1991

Executive Summary

Computer systems are coming of age. As computer systems become more prevalent, sophisticated, embedded in physical processes, and interconnected, society becomes more vulnerable to poor system design, accidents that disable systems, and attacks on computer systems. Without more responsible design and use, system disruptions will increase, with harmful consequences for society. They will also result in lost opportunities from the failure to put computer and communications systems to their best use.

Many factors support this assessment, including the proliferation of computer systems into ever more applications, especially applications involving networking; the changing nature of the technology base; the increase in computer system expertise within the population, which increases the potential for system abuse; the increasingly global environment for business and research; and the global reach and interconnection of computer networks, which multiply system vulnerabilities. Also relevant are new efforts in Europe to promote and even mandate more trustworthy computer systems; European countries are strengthening their involvement in this arena, while the United States seems caught in a policy quagmire. Although recent and highly publicized abuses of computer systems may seem exceptional today, each illustrates potential problems that may be undetected and that are expected to become more common and even more disruptive. The nature and the magnitude of computer system problems are changing dramatically.

The nation is on the threshold of achieving a powerful information infrastructure that promises many benefits. But without adequate safeguards, we risk intrusions into personal privacy (given the grow-

ing electronic storage of personal information) and potential disasters that can cause economic and even human losses. For example, new vulnerabilities are emerging as computers become more common as components of medical and transportation equipment or more interconnected as components of domestic and international financial systems. Many disasters may result from intentional attacks on systems, which can be prevented, detected, or recovered from through better security. *The nation needs computer technology that supports substantially increased safety, reliability, and, in particular, security.*

Security refers to protection against unwanted disclosure, modification, or destruction of data in a system and also to the safeguarding of systems themselves. Security, safety, and reliability together are elements of system trustworthiness—which inspires the confidence that a system will do what it is expected to do.

In many ways the problem of making computer and communications systems more secure is a technical problem. Unlike a file cabinet, a computer system can help to protect itself; there exists technology to build a variety of safeguards into computer systems. As a result, software, hardware, and system development presents opportunities for increasing security. Yet known techniques are not being used, and development of better techniques is lagging in the United States. From a technical perspective, making computer system technology more secure and trustworthy involves assessing what is at risk, articulating objectives and requirements for systems, researching and developing technology to satisfy system requirements, and providing for independent evaluation of the key features (to assess functionality) and their strength (to provide assurance). All of these activities interact.

Attaining increased security, in addition to being a technical matter is also a management and social problem: what is built and sold depends on how systems are designed, purchased, and used. In today's market, demand for trustworthy systems is limited and is concentrated in the defense community and industries, such as banking, that have very high levels of need for security. That today's commercial systems provide only limited safeguards reflects limited awareness among developers, managers, and the general population of the threats, vulnerabilities, and possible safeguards. Most consumers have no real-world understanding of these concepts and cannot choose products wisely or make sound decisions about how to use them. Practical security specialists and professional societies have emerged and have begun to affect security practice from inside organizations, but their impact is constrained by lack of both management

awareness and public awareness of security risks and options. Even when consumers do try to protect their own systems, they may be connected via networks to others with weaker safeguards—like a polluting factory in a densely populated area, one person's laxness in managing a computer system can affect many. As long as demand remains at best inconsistent, vendors have few incentives to make system products more secure, and there is little evidence of the kind of fundamental new system development necessary to make systems highly trustworthy. The market does not work well enough to raise the security of computer systems at a rate fast enough to match the apparent growth in threats to systems.

The U.S. government has been involved in developing technology for computer and communications security for some time. Its efforts have related largely to preserving national security and, in particular, to meeting one major security requirement, confidentiality (preserving data secrecy). But these programs have paid little attention to the other two major computer security requirements, integrity (guarding against improper data modification or destruction) and availability (enabling timely use of systems and the data they hold). These requirements are important to government system users, and they are particularly and increasingly important to users of commercial systems. Needed is guidance that is more wide-ranging and flexible than that offered by the so-called Orange Book published by the National Security Agency, and it should be guidance that stimulates the production of more robust, trustworthy systems at all levels of protection.

Overall, the government's efforts have been hamstrung by internecine conflict and underfunding of efforts aimed at civilian environments. These problems currently appear to be exacerbated, at precisely the time that decisive and concerted action is needed. A coherent strategy must be established now, given the time, resources, planning, and coordination required to achieve adequate system security and trustworthiness. The reorganization of and perceived withdrawal from relevant computer security-related activities at the National Security Agency and the repeated appropriations of minimal funding for relevant activities at the National Institute of Standards and Technology are strong indications of a weak U.S. posture in this area. A weak posture is especially troubling today, because of the momentum that is building overseas for a new set of criteria and associated system evaluation schemes and standards. Influencing what can be sold or may be required in overseas markets, these developments and the U.S. response will affect the competitiveness of U.S. vendors and the

options available to users of commercial computer systems worldwide. They will also affect the levels of general safety and security experienced by the public.

This report characterizes the computer security problem and advances recommendations for containing it (Chapter 1). It examines concepts of and requirements for computer security (Chapter 2), the technology necessary to achieve system security and trustworthiness, and associated development issues (Chapter 3), programming methodology (Chapter 4), the design and use of criteria for secure computer system development and evaluation of computer system security relative to a set of criteria (Chapter 5), and problems constraining the market for trustworthy systems (Chapter 6). *The System Security Study Committee concluded that several steps must be taken to achieve greater computer system security and trustworthiness, and that the best approach to implementing necessary actions is to establish a new organization, referred to in the report as the Information Security Foundation (ISF).* The concept of the ISF and the roles and limitations of organizations that currently have significant responsibilities in the computer security arena are discussed together (Chapter 7). Topics and tactics for research to enable needed technology development are outlined (Chapter 8). Supporting the individual chapters are appendixes that provide further details on selected technical and conceptual points.

The committee urges that its recommendations be considered together as integral to a coherent national effort to encourage the widespread development and deployment of security features in computer systems, increase public awareness of the risks that accompany the benefits of computer systems, and promote responsible use and management of computer systems. Toward the end of increasing the levels of security in new and existing computer and communications systems, the committee developed recommendations in six areas. These are outlined below and developed further in the full report.

1. Promulgation of a comprehensive set of Generally Accepted System Security Principles, referred to as GSSP, which would provide a clear articulation of essential security features, assurances, and practices. The committee believes that there is a basic set of security-related principles for the design, use, and management of systems that are of such broad applicability and effectiveness that they ought to be a part of any system with significant operational requirements. This set will grow with research and experience in new areas of concern, such as integrity and availability, and can also grow beyond the specifics of security to deal with other related aspects of system trust, such as safety. GSSP should enunciate and codify

these principles. Successful GSSP would establish a set of expectations about and requirements for good practice that would be well understood by system development and security professionals, accepted by government, and recognized by managers and the public as protecting organizational and individual interests against security breaches and associated lapses in the protection of privacy. GSSP, which can be built on existing material (e.g., the Orange Book), would provide a basis for resolving differences between U.S. and other national and transnational criteria for trustworthy systems and for shaping inputs to international security and safety standards discussions.

2. A set of short-term actions for system vendors and users that build on readily available capabilities and would yield immediate benefits, including (for users) formation of security policy frameworks and emergency response teams, and (for vendors) universal implementation of specific minimal acceptable protections for discretionary and mandatory control of access to computing resources, broader use of modern software development methodology, implementation of security standards and participation in their further development, and procedures to prevent or anticipate the consequences of inadvisable actions by users (e.g., systems should be shipped with security features turned on, so that explicit action is needed to disable them).

3. Establishment of a system-incident data repository and appropriate education and training programs to promote public awareness.

4. Clarification of export control criteria and procedures for secure or trusted systems and review for possible relaxation of controls on the export of implementations of the Data Encryption Standard (DES).

5. Funding and directions for a comprehensive program of research.

6. Establishment of a new organization to nurture the development, commercialization, and proper use of trust technology, referred to as the Information Security Foundation, or ISF. The committee concludes that existing organizations active in the security arena have made important contributions but are not able to make the multifaceted and large-scale efforts that are needed to truly advance the market and the field. The proposed ISF would be a private, not-for-profit organization. It would be responsible for implementing much of what the committee has recommended, benefiting from the inherent

synergies: ISF should develop GSSP, develop flexible evaluation techniques to assess compliance with GSSP, conduct research related to GSSP and evaluation, develop and maintain an incident-tracking system, provide education and training services, broker and enhance communications between commercial and national security interests, and participate in international standardization and harmonization efforts for commercial security practice. In doing these things it would have to coordinate its activities with agencies and other organizations significantly involved in computer security. The ISF would need the highest level of governmental support; the strongest expression of such support would be a congressional charter.

Although the System Security Study Committee focused on computer and communications security, its recommendations would also support efforts to enhance other aspects of systems such as reliability and safety. It does not make sense to address these problems separately. Many of the methods and techniques that make systems more secure make them more trustworthy in general. The committee has framed several of its recommendations so as to recognize the more general objective of making systems more trustworthy, and specifically to accommodate safety as well as security. The committee believes it is time to consider all of these issues together, to benefit from economies in developing multipurpose safeguards, and to minimize any trade-offs.

With this report, the committee underscores the need to launch now a process that will unfold over a period of years, and that, by limiting the incidence and impact of disruptions, will help society to make the most of computer and communications systems.

Mr. GLICKMAN (presiding). Thank you.

I was out of the hearing a little bit—I apologize—so I may ask redundant questions.

Mr. Rhile, last year the GAO completed a report showing that only 38 percent of the planned controls identified in their computer security plan had been implemented at 10 agencies. I have a copy of that GAO report right here. These agencies were not serious about implementing the provisions of the Act to improve the way they manage computer and network security. I believe that is also evident from your testimony regarding the Department of Justice. Therefore, I would like to request the GAO to complete a phase two of that audit, and I will be sending over a request shortly. You have implemented—you have got the first part of it. I want to see what is happening now. So you will be getting that request.

These agencies have had an additional year to implement the planned security controls. If they still have not implemented these controls, I will work with the Committee on Government Operations to restrict systems acquisitions until the agency management implements these controls. This is very serious. You have brought up one case study that is very serious indeed, and a different kind of seriousness than some of the things we have been talking about in the first hearing, but I would hope that you would do that, and I would also hope that you would—I don't believe the Justice Department was one of the agencies in this first report. Was it?

Mr. RHILE. Yes, it was, Mr. Chairman, I believe.

Mr. SALVEMINI. Yes, it was.

Mr. RHILE. Yes, it was, Mr. Chairman.

Mr. GLICKMAN. Okay. All right. Well, I just want to make sure that that additional thing is there.

Now I am aware that Mr. Gilchrest was going to ask some questions about the Lexington, Kentucky, incident that maybe would present other aspects of this issue, and I would ask you to be ready for a series of written questions propounded by the subcommittee that will be sent in reference to that as well.

Mr. RHILE. We would be happy to respond, Mr. Chairman.

Mr. GLICKMAN. I am concerned about the Justice Department incident, and reflecting upon your audit work at Justice, Mr. Rhile, what is your opinion of Mr. Walker's statement, who testified in the first panel, where he said, "If management cares about protecting its sensitive information, it will be protected. If not, it won't work"?

Mr. RHILE. Yes. I think that care is the first step. "Commitment" is the word I would use. Management must be committed to protecting its sensitive information, and even that is not enough. "Commitment" is a word that is difficult to measure, and sift, and so forth. I would say action. If you are committed, then you need action, and this action needs to be done. These are the kinds of things that we hadn't found at Justice. We didn't find action.

So I agree with Mr. Walker's statement, but I would extend it to that degree.

Mr. GLICKMAN. What was not in place—procedures, guidance to the field activities, training—that led someone in the U.S. Attor-

ney's Office to sell used computers that contained sensitive information? Or was it just stupidity?

Mr. RHILE. It is difficult to describe that, but I can do it. It is—I was going to say, it is easier to say what was in place; it is a shorter list.

Training—security awareness training—there was no training done down there of the folks who are operating these computers; they were not aware. And technical training is another area. People were not aware of the things that you can do with a magnetic disk. Procedures—there were no real procedures for the disposal of used equipment. There were no periodic reviews by the Department of Justice of the security practices at these places, and, I might add, it is not just Lexington. No risk assessments to identify the vulnerabilities, the threats, and to develop some procedures to control against these. These—all these things were not there, Mr. Chairman.

Mr. GLICKMAN. As of today, where do you—you know, you have indicated in your statement that Justice has made some improvements, the Eagle system.

Mr. RHILE. Yes.

Mr. GLICKMAN. Where are they today and from what your review——

Mr. RHILE. They have begun a number of actions. They have—I think I would characterize it this way: a number of actions are under way, and many have just begun. I think I would put it that way. They have, for example, developed some policies on surplusing equipment which did not exist before, established some mandatory security awareness training, which is currently—which is about a month old. They have added some additional staff to the Justice Management Division to review compliance with security procedures.

One thing that Justice hasn't done until last week was to identify all equipment that had been surplused and determine whether or not there is the possibility of sensitive information being placed on that, or being surplused along with the equipment. That was begun last week.

So there's a number of things that have started, but we are nowhere near there yet. For example, in security training we don't have a full panoply of security training. We have security awareness training, but what we don't have is training for—at different levels of management, you know, what are management's responsibilities to—in the area of computer security. We don't have technical training that is mandatory for people like, say, security managers, people whose job it is to conduct security.

Mr. GLICKMAN. Let me ask you this hypothetical. Now you mentioned in this Lexington thing that there were some things you would prefer not to talk about.

Mr. RHILE. Yes.

Mr. GLICKMAN. You know, that makes me think, well, maybe—could organized crime, let's say, be able to invade systems in the Department of Justice and find names in the Witness Protection Program or other relevant information? I mean it leads me to believe that the accessibility to sensitive information in the Department of Justice is more open than it should be.

Mr. RHILE. That is correct. It is much more open, and what we are really talking about is—the Lexington incident was in the area of surplusing of equipment—you know, what procedures do you follow to properly surplus your equipment—but we are talking about other functions besides surplusing.

To answer your other question, I would think that it would be well within the realm of possibility.

Mr. GLICKMAN. Yes. I mean you haven't—we are not saying that that has, in fact, happened.

Mr. RHILE. Yes.

Mr. GLICKMAN. I am just saying that, you know, it is very hard to—if you are in an agency like Justice, to say, "Oh, well, we are going to super-protect these systems and we are not going to super-protect these systems," and I think that is—there obviously are systems with more critical information than other systems.

Mr. RHILE. Correct.

Mr. GLICKMAN. It is a very grave concern, and it is an example of an agency that affects people's daily lives on a law enforcement basis, and they haven't had good management in terms of setting up their systems, and they haven't taken it very seriously, and I am—I would hope that if you go ahead and do phase two of this thing, we continue to bird-dog the Department of Justice, and I intend to talk to my colleagues.

I am also on the Judiciary Committee. Congressman Hughes, Congressman Schumer, Congressman Brooks—you know, these people need to know that all of our efforts in fighting crime—and right now, as we speak, the Senate is working on a crime bill. It would be the height of irony indeed if the information base in the Department of Justice was like a sieve and you could just come in and pull it all out because nobody set up basic management techniques to keep that information secure.

Mr. RHILE. Yes, I would like to comment on that, Mr. Chairman. I don't think we are talking about a sieve in the sense that, you know, one can walk in off the street, but I think what we are talking about are a set of procedures, a set of internal controls, that have holes in them, and these holes must be plugged. I also understand that Mr. Brooks is holding a hearing as we speak, part of—right now, to discuss, among other things, the Department of Justice's ADP management, including computer security.

Mr. GLICKMAN. Mr. Kammer, you may want to repeat some of the things you said in your statement, but, you know, NIST has promised us in the past that a public key cryptographic standard would be published by the end of September of last year. To date, it hasn't been standard. It is interesting that the algorithm is announced today. What is the target date for publication for comment? Why does this all take so long?

Mr. KAMMER. Well, first of all, it is a tough problem technically, and, despite what people say about there's all these wonderful things available in the private sector, I mentioned that I won't have a hashing function even when I do publish, which I hope to do in about a month and a half.

I have the algorithm ready; we have written a patent disclosure; we are filing it with the Patent Office. But none of the other systems will work without a satisfactory hashing function. So I'm not

sure, despite people's presumption that they have these wonderful working systems in this area, that they do. It is a technical problem that we—we think we now have in hand, but it was difficult.

There's also some very complex intellectual property problems. As you are probably aware, all of the candidates that are generally discussed were funded by the U.S. Government for their development, and, through a variety of appropriate means, legal means, many of them have come into the control of companies who now want to charge royalties for the use of those, and as we began to think that through, we began to think that it wasn't necessarily in the Government's interest to have a relatively expensive solution, and was there some solution we could find that wouldn't run afoul of those kinds of intellectual property issues, and we worked on that for quite a while too, but successfully.

Mr. GLICKMAN. Do you have a target date for the hashing algorithm?

Mr. KAMMER. I'm shooting for October.

Mr. GLICKMAN. I'm sorry—for——

Mr. KAMMER. October of this year. I will have the algorithm out for discussion in, as I say, about 90 days—45 days, I'm sorry—45 days, and that will probably still be under discussion when we put the hashing algorithm out—the hashing function.

Mr. GLICKMAN. We talked a little bit about this computer security and privacy board. It took a letter from this subcommittee and some pressure to even get the three members appointed. What was the problem of getting people appointed to the board? How is the board doing? You heard Mr. Walker basically indicate that the board doesn't seem to have what Congress contemplated it would have.

Mr. KAMMER. Well, in terms of the appointments, the people involved, including the gentleman who was here, knew that they had been nominated for some time, and they had indeed been going to board meetings in expectation of imminent approval. Why the approvals take so long I don't know. It isn't unique to this area. The clearance process is pretty obscure to me, and I don't have a real good answer for you. We nag, and after a while it happens, but it isn't—isn't a very straightforward process.

With respect to the functioning of the board itself, its intended purpose of representing the points of view of the users and the venders, and I think it does a relatively good job of representing the vendors and of representing consultants who would like to advise users. I don't feel that we get as good a feedback on the needs of the users, if you will, as we should, but they certainly feel free to let their opinions be known.

Mr. GLICKMAN. Let me just go through three questions.

Have you evaluated the NRC report?

Mr. KAMMER. Yes, I have.

Mr. GLICKMAN. Are there recommendations that you are planning to implement?

Mr. KAMMER. Well, if I could make sort of a contextual comment on it, it is an opinion document; there isn't any data in it. It is sort of a polemic by people that feel intensely, and some of the things are, I think, clearly the case. I don't think most people would dispute the fact that we need to put a higher priority on security.

Some of the opinions that they state are contradicted by facts, you know, that are not presented by them; it is just simply a point of view they wanted to argue.

All in all, I don't find it a terrifically useful document.

Mr. GLICKMAN. Have you responded in writing to it?

Mr. KAMMER. No, I haven't really felt a need to.

Mr. GLICKMAN. Recommendation two of the report outlines actions that can be taken now by the agency, such as shipping, installing systems with the security features turned on. Has NIST taken any action to advise or encourage the agencies to implement these suggestions?

Mr. KAMMER. Well, that's a technologically interesting idea. Putting the power pack with the computer while you transport it could be a might pricey. I actually feel more comfortable doing a security check at the point of installation and, indeed, post-installation by the security—by the computer operator rather than the installer. My personal philosophy is that the operator of the system is responsible for the security, not the guy that delivered it. It is not a recommendation that I would sign on to cheerfully.

Mr. GLICKMAN. Have you implemented a program to work with universities, colleges, high schools, and trade schools to include security as part of training on computers?

Mr. KAMMER. Well, this year we assumed not quite that far. I'd like to go that far. I think the issue of ethics and sort of inculcating in our society a different set of values about security and data starts there. But we did assume sponsorship of the National Educators Forum this year, and this Forum gives us an opportunity to promote the kinds of ideas that you're talking about. It's a first step but it'll be years in the making.

Mr. GLICKMAN. The question I asked you before is one that—perhaps, staff can talk to you afterwards. They weren't actually talk—the question was virtually having it turned on, like electrically on, was not the point of my question. Designing the package so that it would be much more ready to use instantaneously.

Mr. KAMMER. Well, the digital signature confers that kind of protection. It's entirely possible for the originator of software or hardware to digitally seal, and this functionality of integrity that we all talk about, which is very important, probably a lot more important than confidentiality for most purposes for the kind of security you want in the civil arena, would allow you to then know if there had been any alteration. You would have a positive assurance with a very, very, very high degree of certainty that it had not been meddled with. Or if it had, you would know that too, and you would be able to contact the originator and say, "Look. This wasn't delivered as you sent it." That's a relatively straightforward thing that I think will become—I doubt in a few years if you'll be able to buy a software package that doesn't have that.

Mr. GLICKMAN. I would say, kind of to close this hearing, one is to reinforce to Mr. Rhile, the subcommittee will be asking you and the full committee, too, to move ahead.

Mr. RHILE. I understand, Mr. Chairman.

Mr. GLICKMAN. Number two is that I was impressed by the initial witnesses. As you know, Mr. Kammer, and this is not to be personally critical of you, but I still believe this issue has a low priori-

ty in the government. Even reading OMB's statement, it looks pretty pathetic to me. And, as Mr. Rohrabacher says, the threats, the ultimate threats to the United States are far more directed at stopping the information flow in this country and all that that means, more than the military threats in terms of an actual invasion. And I just, I still detect no real interest. And I also detect this bureaucratic conflagration between NSA and the rest of the Government of the United States. It's still a very troubling thing to me in terms of trying to outline what is important, and I think that word was good. "Sensitive" may not be the right word. The word may be "important." And what the American people think is important may be different than what the planners of the National Security Agency or the defense establishment thinks are important, and I think that we need to deal with that issue from a philosophical context as well, because a lot of very important things are being jeopardized by not having computer security systems up and in place. It's important to the lives of most Americans.

And the private sector is working, moving ahead. I mean the banking system, as you know, is moving ahead on this thing, and I could end up seeing a lot of confusing equipment and standards out there that may not adequately protect us and may also place the United States of America in a secondary or tertiary position to what other countries are in.

So, these are just comments that I continue to have and continue to feel, and I'm glad that the GAO has been involved in this thing. I think you've all done a good job, but we're going to expect you to continue to work on it. And I know that NIST is working under difficult circumstances, budgetary circumstances where you don't often get the resources that you need from this Congress as well. But we're going to continue to "bird dog" this issue. I'm not going to let it go, and neither is this committee going to let it go as well.

So we thank you very much for coming today, and you will expect appropriate follow-up from us as well.

[The prepared statement plus answers to questions asked of Mr. MacRae follows:]

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

STATEMENT OF JAMES B. MACRAE
ACTING ADMINISTRATOR
OFFICE OF INFORMATION AND REGULATORY AFFAIRS
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE SUBCOMMITTEE ON
TECHNOLOGY AND COMPETITIVENESS
OF THE COMMITTEE ON SCIENCE, SPACE AND TECHNOLOGY
OF THE HOUSE OF REPRESENTATIVES OF THE UNITED STATES
ON IMPLEMENTATION OF THE COMPUTER SECURITY ACT OF 1987
JUNE 27, 1991

I am pleased to have the opportunity to describe the Office of Management and Budget's (OMB's) continuing efforts to oversee the implementation of the Computer Security Act of 1987, and to discuss specifically our work with Federal agencies in helping to improve their computer security.

The Computer Security Act

Last year when I testified before the Subcommittee on Science, Space, and Technology, I said that we would continue to emphasize security awareness and training, and that we would begin visiting senior officials at the Departments and agencies to focus attention on the security risks inherent in their computer systems. I also noted that, while planning is an important management tool, it only has value to the extent that it actually improves the security of our systems. Therefore, I made a commitment to emphasize implementation of agency plans. Finally,

I promised to come back this year to provide an update of how we are doing.

As I said last year, we view the purpose of the Computer Security Act to assure the cost-effective security of Federal computer systems. Furthermore, the Act provides the framework within which Federal agencies can work to assure the confidentiality, integrity, and availability of information contained in Federal computer systems. In this context, confidentiality means protecting information stored on Federal systems from unauthorized disclosure. Integrity means protecting Federal information from unauthorized or inadvertent modification. Availability means that information stored in Federal systems is available when it is needed.

The essence of good security is the understanding of threats and ways to mitigate them. Part of the wisdom of the Computer Security Act is its emphasis on broadening awareness of the need for computer security. And we are beginning to see some results. For example, the General Services Administration will soon offer secure data transmission under the FTS2000 contract. Once operational, this service will satisfy most Federal agencies' requirements for long-distance data encryption.

Recent security incidence, such as the sale of used computers without the erasure of data they contained, reaffirm the view

that our systems are probably more vulnerable to losses caused by uninformed or inadvertent behavior than to outside attacks by individuals wishing to obtain or destroy Federal information. To provide the level of security demanded by our dependence on Federal systems, prudence dictates that we continue our efforts to make all Federal employees aware of operational risks and proper security procedures as well as to work to defend our systems against deliberate attack.

Agency Visits

Today I would like to talk about the visits that we, NIST and NSA are making to agency senior officials. Our goals for the agency visits have been two-fold:

- to heighten computer security awareness among senior agency managers in the short term, and

- to change Federal agencies' behavior so as to improve the security of their systems in the longer term.

Our approach is based on the belief that computer security is primarily a management problem, and only secondarily a technical problem. By this I mean that the principal risk stems from how Federal computer systems are used, not from our inability to secure them by adding technical security features.

Each agency security visit begins with a staff discussion of the agency's computer security program and culminates in a meeting with the senior official designated under the Paperwork Reduction Act, usually an assistant secretary. We also ask senior managers from 2 or 3 key program areas to participate in the meeting. These are the managers who actually run the business of the agency on a day-to-day basis, not the technical cadre who operate its computer systems. We ask them to discuss the security of the critical systems they depend on to run their daily business. If these senior managers are satisfied with their computer security, we ask for justification. If these senior managers are not satisfied with their systems' security, we ask what corrective actions they have planned. We then discuss the agency's overall computer security program with the agency senior official. Finally, we discuss specific incidents and vulnerabilities the agency may have identified, and direct managers to the appropriate technical assistance. We tend to keep the discussion away from technical details, although we are accompanied by NIST and NSA experts who are available when technical issues arise.

To date, we have visited 13 agencies. Our first visits were to agencies where computer security was identified as a high risk area or a "material weakness" under the Federal Manager's Financial Integrity Act. We wanted to put those agencies in touch with appropriate technical experts as soon as possible. We subsequently began visiting the other agencies, starting with the

larger ones. It is worth noting the high level of interest in all of the visited agencies, as evidenced by the fact that every one of these meetings with senior managers has run over its planned two-hour schedule. I have attached a list of the agencies we have visited to this statement.

Observations From Agency Visits

While we are far from finished with our visits, we can identify some common elements that cut across the agencies we have visited:

- First, like the Computer Security Act itself, the visits have clearly raised the visibility of computer security as an issue with senior managers and within their agencies.

- Second, many of the agency program managers we met have made considerable effort assessing the security of their automated systems, as well as their internal controls, with the goal of ensuring that their systems were doing what they were supposed to, and nothing more.

- Third, one concern we are hearing from program managers is the question of data availability if a primary computer system is disabled. To focus technical attention on preparedness for computer disaster recovery, we asked

agencies, in OMB Bulletin 91-10, "Information Resources Management Plans," to describe the current status of their contingency and back-up planning. We are also working with GSA and the Council of Federal Data Center Directors to identify the most cost-effective alternatives for satisfying agency back-up requirements.

- Fourth, it is worth noting that we have seen cases where agencies do not use computer technology because of their inability to assure adequate security. For example, several agencies told us that they do not send out laptops to remote locations or let employees dial into their mainframes because of the security risk.

Generally speaking, we are finding that Federal managers are aware of the basic control issues relating to computer security and the primary risks and vulnerabilities in their own systems. Although it is premature to draw more definitive conclusions at this time, we will share a more complete report with the Subcommittee after we have visited more agencies.

I understand that NIST will be describing their perception of the visits in later testimony.

Computer Security Planning

While the agency visits have been our most visible activities of the past year, we have not forgotten the need for viable security planning in new computer systems. In OMB Bulletin No. 90-08, "Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information," we issued improved guidance for agency preparation of computer security plans. We also asked agencies to continue preparing security plans for new or changed systems that contain sensitive information and to seek independent advice and comment on those plans. And, as I said last year, we focused their efforts on implementation of their plans.

In OMB Bulletin No. 91-10, "Information Resources Management (IRM) Plans," we asked agencies to include summaries of their computer security activities in their IRM plans. In particular, agencies are to provide measures of their planning and implementation activities, such as the number of plans reviewed and implemented. They are also to describe improvements in the security of their most sensitive systems, the status of their awareness and training programs, and their actions to assure that plans are implemented. We are now receiving those reports, which will be published later this year as part of the Five Year Plan for Information Resources Management. As I noted earlier, we

also asked agencies to report to us on their emergency, backup, and contingency plans in the bulletin.

Other Computer Security Activities

In addition to continuing our agency visits and the ongoing agency security planning and awareness work, we have several other initiatives underway to further improve Federal computer security.

- **NIST's Computer Security Budget:** The 1992 President's budget request proposes an over 40% increase in NIST's computer security activities.

- **Revision of Computer Security Appendix in OMB Circular No. A-130:** On March 4, 1991 OMB published a notice in the Federal Register announcing our plans to revise Circular No. A-130, which is OMB's guidance to Federal agencies on the management of their information resources. We intend to revise the appendix dedicated to computer security, and to incorporate what we learn on the visits.

- **Federal Manager's Financial Integrity Act "High Risk" Areas:** The National Computer System Security and Privacy Advisory Board, on May 17, 1991, recommended that we require that an agency's lack of compliance with the Computer Security

requirements of OMB Circulars A-130 and A-123 be defined as "material internal control weaknesses." So defined, these computer security weaknesses would then be reported to the President and the Congress under the Financial Managers Financial Integrity Act. We agree with the Advisory Board's recommendation and plan to give agencies such guidance. One benefit of this plan is that it will use the already existing FMFIA reporting mechanism to report computer security problems, and thus bring high-level attention to these problems quickly. After reporting a material weakness, agencies are also responsible to provide progress reports in their annual statement of assurance. As I mentioned earlier, several agencies have already identified computer security as a material weakness and have begun corrective action. We will continue to work with the Advisory Board and the Inspectors General over the next few months to develop our guidance.

- Electronic Data Interchange: OMB is currently sponsoring a government-wide effort to explore and expand Federal use of Electronic Data Interchange or "EDI." This initiative to move the government from paper-based transactions to electronic transactions has major implications for the way the government does business. Using EDI, each piece of electronic "business" must be authorized and authenticated electronically, as well as secured, while being transferred,

processed, and stored. We are currently leading a multi-agency task force including NIST, the Departments of Defense, Veterans Affairs, and Treasury, the GSA, and others to share experiences and develop Federal EDI solutions. Earlier this year, the EDI task force adopted a pilot project of the Department of Veterans Affairs, which I mentioned in my testimony last year. This project is one of the first to convert Federal purchase orders into electronic format, and is thus raising many of the security issues involved in the electronic transfer of business information between a Federal agency and its commercial suppliers.

In summary, the past year has seen increasing activity and progress in implementing the Computer Security Act. Thus far, we have generally been pleased that the agencies we have visited have been working on computer security with the high level of attention that is appropriate, given their dependence on their computer systems. I can assure you, Mr. Chairman, that we will continue to devote sustained attention to this area, and we appreciate the continuing support of this Subcommittee in these efforts.

I would be pleased to answer any questions that you may have.

Statement of James B. MacRae
Attachment

Agency Visits
(as of 6/27/91)

Visits Completed

Department of Education

Department of the Treasury

Federal Emergency Management Agency

Department of Commerce

Department of Health and Human Services

Agency for International Development

Department of Justice

Department of State

National Aeronautics and Space Administration

General Services Administration

National Archives and Records Administration

Department of Energy

Department of Housing and Urban Development

Visits Initiated

Nuclear Regulatory Commission

Department of Transportation

Department of Agriculture

Federal Communications Commission

Environmental Protection Agency

Department of Labor

Department of Defense

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

AUG 8 1991

Honorable Tim Valentine
Chairman, Subcommittee on Technology
and Competitiveness
Committee on Science, Space and Technology
Suite 2320
Rayburn Office Building
Washington, D.C. 20515

Dear Mr. Chairman:

This is in response to your July 11, 1991 letter to Director Darman which forwarded ten questions for the record of a hearing on computer security held June 27, 1991 before the Subcommittee on Technology and Competitiveness. Answers to those questions are enclosed.

I look forward to our future discussions on this important matter, and appreciate your understanding that I was unable to testify at the hearing.

Sincerely,

Signed

James B. MacRae, Jr.
Acting Administrator and
Deputy Administrator
Office of Information
and Regulatory Affairs

QUESTIONS FROM COMPUTER SECURITY HEARING
JUNE 27, 1991

1. The Department of Veterans Affairs was not identified on the list of agencies visited or initiated visits. The newspapers are reporting problems such as inconsistent medical records of patients. Why have you not visited the VA?

A: As I noted in my statement, our first visits were to agencies that had identified specific weaknesses in their automated systems. We wanted to provide them with assistance in addressing those weaknesses. We are now visiting the other agencies as quickly as practicable. We plan to visit the Department of Veterans Affairs later this Summer.

2. Mr. MacRae, in your testimony last year, you referred to the ultimate weapon, "defund," systems whose security plans are not adequate. After your visits to the agencies, are there systems that you now think should be "defunded"?

A: As I noted last year, the ultimate weapon is a very heavy weapon. It is not one that we would employ lightly. During the past year, we did not need to eliminate entire funding for any agency system. In several instances, however, such as during our budget review of the IRS Modernization effort, we worked with agencies to ensure that they included adequate funding for security in particular system plans. Based upon our discussions with agency management during the visits, we anticipate that a number of agencies will seek funding this year to enhance the security of their systems.

I should also point out that several agencies described instances where their management has elected not to use computer technology -- not to fund and build a system -- because the technology could not provide them with sufficient security.

3. Last year you could not identify a single agency outside the intelligence community where you would consider there to be an operating, effective and sufficient computer security program. After your visits to the agencies, have you identified agencies that you now evaluate to have adequate plans and programs? If so, which ones? If none was identified, what is OMB's next step to developing adequate programs at the agencies?

A: All of the agencies that we have visited so far have viable computer security programs underway. Each of them is coping with new security risks introduced by a rapidly changing technology. Each agency program has incorporated security planning into its program and appears to be progressing toward adequate security of its systems. However, as I said last year, in our view no agency's program yet provides sufficient security for all of its systems. We believe that our visits as well as the Subcommittee's continued interest are contributing to the agency's progress in improving their security.

Our next steps toward continuing that progress will include an assessment of what we heard in all of our visits leading to conclusions of needed next steps -- which we will be reporting on later this year. In addition, we plan to reemphasize the need for viable security programs through clear, updated policy guidance in a revised OMB Circular No. A-130, which we plan to propose later this year. Finally, we will assure operational oversight of system security through the reporting and monitoring activities of the Federal Manager's Financial Integrity Act (FMFIA).

4. During OMB's evaluation of the systems included in the Program for Priority Systems, what emphasis is placed on computer security? Do all of the systems have computer security plans? If yes, do you evaluate the computer security plan for each system? If no, why not?

A: In the Program for Priority Systems (PPS) emphasis is placed on efforts to improve Government through effective uses of modern information technology (IT) and focusing attention on the IT planning phase. The planning phase includes identifying the problem, clarifying objectives, developing concepts that achieve the objectives, design of system architecture, and computer and communications security.

PPS reviews and evaluations at various planning checkpoints focus on assuring that all facets of the system have been well thought out and integrated. This includes ensuring that adequate security is recognized, defined, and planned into the system requirements. Even before separate computer security plans became a requirement, PPS reviews included evaluations of system security.

5. During your visit to the Department of Justice, which systems were discussed and was the security adequate?

A: We discussed four specific systems as well as the overall security program with senior officials of the Department during our visit:

1. Interagency Border Inspection System

2. National Crime Information System

3. Enhanced Automation for Government Legal Environment;

4. SENTRY.

As in all of our visits, instead of identifying specific weaknesses in individual systems, we are trying to raise the awareness of and improve the management processes by which agencies themselves identify weaknesses, correct problems and thus improve security. The Justice officials we visited were concerned about the adequacy of the security of their systems, and in each instance were taking appropriate management action to improve it.

I should note that based upon recent security incidents, the Department now plans to address computer security as a material weakness under the Federal Manager's Financial Integrity Act. We have also identified the Department's computer security as an area of high risk, requiring greater OMB attention. In addition, we recently asked NIST and the General Services Administration to apprise the other Executive agencies of the types of vulnerabilities found in those incidents, and ways to mitigate against those vulnerabilities.

6. How long will OMB continue the visits to the agencies? Can the Subcommittee expect to receive the report on the findings of the visits? What is the next step that OMB plans to encourage agencies to increase the computer security of their systems that contain sensitive information? Is there a need to periodically renew emphasis by visiting the agencies?

A: We plan to complete the first round of our visits -- to each large agency -- by the end of the Summer. At the conclusion of those visits, we plan to issue a report that will summarize what we found government-wide, which of course we will share with the Subcommittee.

In part, our next steps will depend on the overall findings described in that report. But at this point, it is safe to say that those efforts will include renewed emphasis on computer security through reissuance and updating the policy in OMB Circular No. A-130. That will likely include closely tying the requirement for computer security planning together with internal control oversight mechanisms under the FMFIA. Working with NIST, we will define those areas of security vulnerability that most readily imply a substantial internal control weakness.

As with all forms of security, over time computer security procedures tend to atrophy. Therefore, we need to focus attention on the subject. Based on the reviews so far, periodic visits with senior managers are apparently an excellent way to do this, and I would anticipate that we would use them.

7. How actively are the agencies using the computer security plans, developed as a requirement of the Act, to implement security at the agencies?

A: Many agencies actively used the planning requirements of the Act to stimulate awareness on the part of users of computer systems about the need for improved security of those systems. The mandatory requirement for security plans allowed security managers to elicit judgements from that community about the need for and the kinds of security that were most important. It therefore served to focus agency security programs on securing those systems where the risk and magnitude of loss was highest.

In many agencies, the plans serve as checklists of areas of security emphasis, particularly during the design phase of new systems. As actual plans to be followed for implementation, however, they are used less. Implementation of technical security measures requires comprehensive and detailed plans related to specifics of individual systems. To be readily implemented, such plans are normally incorporated into the plans for development and implementation of the system itself.

8. When do you project that OMB will provide guidance to the agencies on the Computer Security and Privacy Board's recommendation regarding noncompliance with certain requirements of OMB Circular No. A-130 and A-123 being defined as "material weaknesses?" How much of the recommendation will be included in guidance?

A: Earlier this month, we began this process in issuing our instructions for this year's report under the Federal Manager's Financial Integrity Act. In those instructions, we told agencies to take into account recent activities to improve the integrity, availability and confidentiality of automated information systems, including consideration of whether non-compliance with commonly accepted security practices in a sensitive system is a material weakness.

We also plan to incorporate more comprehensive guidance into OMB Circular No. A-130, which we will propose for comment later this year. In drafting that proposal, we will consider the entire list of critical controls that was forwarded to us with the Board's recommendation.

9. Does OMB support the National Research Council's (NRC) concept of an Information Security Foundation (ISF)? If so, does OMB support ISF being included as part of the NIST computer security program?

A: The NRC report is important in that it contributes to the discussion about our need as a nation to assure adequate security of the automated systems upon which we depend. At the same time, however, we do not support the report's concept of a government sponsored ISF, wherever that may be located. In our view, government sponsorship of such an entity, would be an unwarranted government regulatory intrusion into the computer and communication industries. We believe that there are incentives already at work within the marketplace for vendors to provide security in their products and systems.

Should such an entity be formed in the private sector as a voluntary organization that speaks for industry, we could see its role as complementary to NIST's role in the Federal community.

10. Does OMB support a sensitivity labeling system for identifying sensitive information across the government? Why or why not?

A: We support the need to label information so that the possessors of the information understand the security risks associated with the confidentiality, integrity and availability of the information they have.

At the same time, we have reservations about defining standard categories of sensitivity of unclassified information that can readily be labeled. For example, a file of addresses may need protection. How much may be very different -- depending upon what the addresses are and what they will be used for. Consider the difference between a file of addresses of employees versus a file of addresses of employees that have tested positive for drug use.

Security decisions need to be made on a case-by-case basis, rather than on the basis of broad categories of types of information. Part of the wisdom of the Computer Security Act, is its recognition of the need for security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to the information contained in computer systems. Defining broad categories of information to be afforded a given level of protection is not consistent with that policy, and would result in overprotection of some information and under protection of other information. Therefore, we have not supported them.

[Whereupon, at 11:55 a.m., the subcommittee was adjourned, to reconvene subject to the call of the Chair.]

○

ISBN 0-16-035475-7