AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

COMPUTER SECURITY IMPACT OF Y2K: EXPANDED RISKS OR FRAUD?

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY

OF THE

COMMITTEE ON SCIENCE

AND THE

SUBCOMMITTEE ON
GOVERNMENT MANAGEMENT, INFORMATION,
AND TECHNOLOGY

OF THE

COMMITTEE ON
GOVERNMENT REFORM
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

FIRST SESSION

AUGUST 4, 1999

Science Serial No. 106–23

Government Reform Serial No. 106–57

Printed for the use of the Committee on Science

U.S. GOVERNMENT PRINTING OFFICE
60–842 WASHINGTON : 2000

COMMITTEE ON GOVERNMENT REFORM

DAN BURTON, Indiana, *Chairman*

BENJAMIN A. GILMAN, New York
CONSTANCE A. MORELLA, Maryland
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
STEPHEN HORN, California
JOHN L. MICA, Florida
THOMAS M. DAVIS, Virginia
DAVID M. MCINTOSH, Indiana
MARK E. SOUDER, Indiana
JOE SCARBOROUGH, Florida
STEVEN C. LATOURETTE, Ohio
MARSHALL "MARK" SANFORD, South Carolina
BOB BARR, Georgia
DAN MILLER, Florida
ASA HUTCHINSON, Arkansas
LEE TERRY, Nebraska
JUDY BIGGERT, Illinois
GREG WALDEN, Oregon
DOUG OSE, California
PAUL RYAN, Wisconsin
HELEN CHENOWETH, Idaho
DAVID VITTER, Louisiana

HENRY A. WAXMAN, California
TOM LANTOS, California
ROBERT E. WISE, JR., West Virginia
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
PATSY T. MINK, Hawaii
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, Washington, DC
CHAKA FATTAH, Pennsylvania
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
ROD R. BLAGOJEVICH, Illinois
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
JIM TURNER, Texas
THOMAS H. ALLEN, Maine
HAROLD E. FORD, JR., Tennessee
JANICE D. SCHAKOWSKY, Illinois

BERNARD SANDERS, Vermont (Independent)

KEVIN BINGER, *Staff Director*
DANIEL R. MOLL, *Deputy Staff Director*
DAVID A. KASS, *Deputy Counsel and Parliamentarian*
CARLA J. MARTIN, *Chief Clerk*
PHIL SCHILIRO, *Minority Staff Director*

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

STEPHEN HORN, California, *Chairman*

JUDY BIGGERT, Illinois
THOMAS M. DAVIS, Virginia
GREG WALDEN, Oregon
DOUG OSE, California
PAUL RYAN, Wisconsin

JIM TURNER, Texas
PAUL E. KANJORSKI, Pennsylvania
MAJOR R. OWENS, New York
PATSY T. MINK, Hawaii
CAROLYN B. MALONEY, New York

EX OFFICIO

DAN BURTON, Indiana
HENRY A. WAXMAN, California

J. RUSSELL GEORGE, *Staff Director and Chief Counsel*
MATT RYAN, *Senior Policy Director*
BONNIE HEALD, *Communications Director/Professional Staff Member*
GRANT NEWMAN, *Clerk*
TREY HENDERSON, *Minority Counsel*

COMMITTEE ON SCIENCE

F. JAMES SENSENBRENNER, JR., Wisconsin, *Chairman*

SHERWOOD L. BOEHLERT, New York
LAMAR SMITH, Texas
CONSTANCE A. MORELLA, Maryland
CURT WELDON, Pennsylvania
DANA ROHRABACHER, California
JOE BARTON, Texas
KEN CALVERT, California
NICK SMITH, Michigan
ROSCOE G. BARTLETT, Maryland
VERNON J. EHLERS, Michigan
DAVE WELDON, Florida
GIL GUTKNECHT, Minnesota
THOMAS W. EWING, Illinois
CHRIS CANNON, Utah
KEVIN BRADY, Texas
MERRILL COOK, Utah
GEORGE R. NETHERCUTT, JR., Washington
FRANK D. LUCAS, Oklahoma
MARK GREEN, Wisconsin
STEVEN T. KUYKENDALL, California
GARY G. MILLER, California
JUDY BIGGERT, Illinois
MARSHALL "MARK" SANFORD, South Carolina
JACK METCALF, Washington

RALPH M. HALL, Texas
BART GORDON, Tennessee
JERRY F. COSTELLO, Illinois
JAMES A. BARCIA, Michigan
EDDIE BERNICE JOHNSON, Texas
LYNN C. WOOLSEY, California
LYNN N. RIVERS, Michigan
ZOE LOFGREN, California
MICHAEL F. DOYLE, Pennsylvania
SHEILA JACKSON LEE, Texas
DEBBIE STABENOW, Michigan
BOB ETHERIDGE, North Carolina
NICK LAMPSON, Texas
JOHN B. LARSON, Connecticut
MARK UDALL, Colorado
DAVID WU, Oregon
ANTHONY D. WEINER, New York
MICHAEL E. CAPUANO, Massachusetts
BRIAN BAIRD, Washington
JOSEPH M. HOEFFEL, Pennsylvania
DENNIS MOORE, Kansas
VACANCY

CONTENTS

	Page
August 4, 1999:	
Opening Statement by Representative Constance A. Morella, Chairwoman, Subcommittee on Technology, U.S. House of Representatives ...	1
Opening Statement by Representative Stephen Horn, Chairman, Subcommittee on Government Management, Information and Technology, U.S. House of Representatives ...	3
Opening Statement by Representative Mark Udall, Member, Subcommittee on Technology, U.S. House of Representatives ...	6
Witnesses:	
Mr. Joe Pucciarelli, Vice President and Research Director, Gartner Group Inc.:	
Oral Testimony ...	7
Prepared Testimony ...	10
Biography ...	15
Financial Disclosure ...	16
Mr. Harris Miller, President, Information Technology Association of America:	
Oral Testimony ...	17
Prepared Testimony ...	19
Biography ...	33
Financial Disclosure ...	35
Mr. Dean Rich, Vice President for Security Services, WarRoom Research:	
Oral Testimony ...	36
Prepared Testimony ...	39
Biography ...	41
Financial Disclosure ...	44
Mr. Wayne Bennett, Chair, Commercial Technology Practice Area, Bingham Dana LLP:	
Oral Testimony ...	45
Prepared Testimony ...	47
Biography ...	52
Financial Disclosure ...	56

APPENDIX 1: ADDITIONAL STATEMENTS

Statement by Representative Debbie Stabenow, Member, Subcommittee on Technology, U.S. House of Representatives ...	76

APPENDIX 2: MATERIALS FOR THE RECORD

USA Today Article, Y2K fixes open door for electronic heist, M.J. Zuckerman .	78
Gartner Group Report, Year 2000 and the Expanded Risk of Financial Fraud, April 1, 1999 ...	80

HEARING ON THE COMPUTER SECURITY IMPACT OF Y2K: "EXPANDED RISKS OR FRAUD?"

WEDNESDAY, AUGUST 4, 1999

HOUSE OF REPRESENTATIVES, SUBCOMMITTEE ON TECHNOLOGY, COMMITTEE ON SCIENCE, AND THE SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY, COMMITTEE ON GOVERNMENT REFORM,

Washington, DC.

The subcommittees met, pursuant to notice, at 10:06 a.m., in Room 2318, Rayburn House Office Building, Hon. Constance A. Morella [chairwoman of the subcommittee] presiding.

Present: Representatives Morella, Horn, Bartlett, Gutknecht, Turner, Rivers, Stabenow, Udall, and Wu.

Chairwoman MORELLA. I'm going to call to order the latest in our series of ongoing hearings on our House Y2K Working Group made up of the Science Committee's Technology Subcommittee and the Government Reform Committee's Government Management, Information, and Technology Subcommittee.

On behalf of my colleagues Chairman Horn, Ranking Members Barcia and Turner, and Mr. Udall, I want to welcome our distinguished panel as we discuss today the concerns raised by a number of information technology experts that Y2K fixes may pose a substantial security threat to computer operating systems.

While the Technology Subcommittee has been reviewing the year 2000 problem over the past 3 years, during that time we have also been looking closely at the issue of computer security.

Many of you have heard me compare our Nation's lack of adequate information security to the year 2000 computer problem.

Well, it now appears that Y2K and computer security aren't just inviting comparisons, but have overlapped into one issue.

A lot of recent attention has been focused on the April 1, 1999, GartnerGroup report suggesting that as part of every year 2000 system fix, every aspect of every single information technology system is potentially subject to change and manipulation, raising the risk of theft, fraud, or corruption.

The GartnerGroup report also stated that at least one publicly reported theft exceeding $1 billion may occur through lapses in security directly resulting from Y2K remediation efforts.

Since the publication of the report, a number of independent scientists, security professionals, and others in the Y2K community

appear to have few quarrels with the GartnerGroup's dire prediction.

The concern is that Y2K employees who have been hired to correct systems might have left "trap doors" or may manipulate the computer code through which they can clandestinely take control of the system at a future date—leaving vulnerable the systems that electronically move $11 trillion a year among financial institutions, corporations, governments, and private organizations.

The computer security threat, however, may not be motivated merely by just financial theft and fraud.

Some Y2K programmers with malicious intent may be quietly installing malicious software codes—such as a logic bomb or a time-delayed virus—to sabotage companies or gain access to sensitive information sometime in the new millennium.

Most troubling is that several security firms say that they have already found "trap doors" in Y2K programming.

If used successfully for hostile purposes, these computer "trap doors" can open to make sensitive national and proprietary information systems vulnerable to be accessed, stolen, compromised, or disrupted.

With less than 150 days now before the January 1, 2000, deadline, the last thing we want to do is to defer any Y2K remediation efforts.

It should be made clear that nobody should halt or suspend fixing their Y2K problems simply because there exists this potential for computer security breaches.

The goal of this hearing is not to create a how-to guide and stoke the embers of those Y2K programmers with a felonious heart and malicious intent.

The goal of this hearing is to determine what measures can be undertaken to protect our computer systems and to limit the potential of Y2K computer security breaches.

It is my hope that, today, this panel can collectively come up with measures and guidelines that both the private and public sectors can review and utilize in their current remediation efforts to deter and catch any computer security breach that may occur as a result of the Y2K fix.

Toward that end, I am pleased that we have a very distinguished panel.

I welcome Mr. Joe Pucciarelli, Vice President, Research Director of the GartnerGroup, a leading and influential information technology research firm, which we know very well through our hearings, and the author of the GartnerGroup Y2K computer security report.

Also joining us is a familiar figure to us, Mr. Harris Miller, President of the Information Technology Association of America.

The Technology Subcommittee has worked very closely with Mr. Miller and the ITAA in the past on both the Y2K and the computer security issue, and it is great to see him back as a witness before us.

We also have Mr. Dean Rich, Vice President for Security Services at WarRoom Research in Annapolis, Maryland, who is a computer security consultant with a great deal of expertise and experience in

both the public and private sectors. I'm somebody who knows Annapolis well. I welcome you also, Mr. Rich.

Additionally, Mr. Wayne Bennett, Chair of the Commercial Technology Practice Area of the law firm of Bingham Dana in Boston and an expert in computer security laws and practice, is with us today. A pleasure to have you, Mr. Bennett.

So I look forward to everybody's testimony, and I would now like to turn to our distinguished Co-Chair of today's hearing, the member from California, Chairman of the Government Management, Information and Technology Subcommittee, Mr. Horn, for any opening statement that he may wish to make. Mr. Horn.

Mr. HORN. Thank you very much.

For the past 3 years, these two Subcommittees have been prodding agencies in the executive branch of the Federal Government to prepare their computer systems for the year 2000. Nearly all seem to have made good progress toward avoiding major computer disruptions at the end of this year. However, the rush to solve the year 2000 problem may have created another more insidious and potentially troubling problem.

Today, we will discuss the danger that government agencies, corporations, and individuals are now more vulnerable to computer fraud, whether it is in the form of electronic robberies or information warfare.

The reality is that computer systems can be compromised for any number of reasons—some far more damaging than the loss of money. Among them are the threats of industrial or military espionage and the use of computers and the network systems by terrorists or organized crime.

Private companies and government agencies alike have opened up their most sensitive computer systems to outside contractors who are helping them sort through billions of lines of computer code to ensure their year 2000 compliance.

Although the vast majority of these contractors are honest and truthworthy people, even a few unscrupulous operators could create a significant problem.

The GartnerGroup, which is represented here today, has predicted that by 2004, there will be at least one reported $1 billion or more theft due to the year 2000 remediation effort.

The concern involves something called "trap doors," computer coding that can give unscrupulous contractors access to the sensitive information in a computer long after the year 2000 work is completed.

From bank accounts and intellectual property to medical records and defense secrets, companies and government agencies have given contractors the keys that unlock an enormous storehouse of information.

With only 149 days left until the new millennium, we must ensure that our critical information technology infrastructure is secure long after the year 2000 has passed away.

So, with Mrs. Morella, I welcome the witnesses we have today, and I'm sure you will enlighten us in a number of areas.

[The prepared statement of Hon. Stephen Horn follows:]

DAN BURTON, INDIANA,
CHAIRMAN
BENJAMIN A. GILMAN, NEW YORK
CONSTANCE A. MORELLA, MARYLAND
CHRISTOPHER SHAYS, CONNECTICUT
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. McHUGH, NEW YORK
STEPHEN HORN, CALIFORNIA
JOHN L. MICA, FLORIDA
THOMAS M. DAVIS III, VIRGINIA
DAVID M. MCINTOSH, INDIANA
MARK E. SOUDER, INDIANA
JOE SCARBOROUGH, FLORIDA
STEVEN C. LaTOURETTE, OHIO
MARSHALL "MARK" SANFORD, SOUTH CAROLINA
BOB BARR, GEORGIA
DAN MILLER, FLORIDA
ASA HUTCHINSON, ARKANSAS
LEE TERRY, NEBRASKA
JUDY BIGGERT, ILLINOIS
GREG WALDEN, OREGON
DOUG OSE, CALIFORNIA
PAUL RYAN, WISCONSIN
JOHN T. DOOLITTLE, CALIFORNIA
HELEN CHENOWETH, IDAHO

ONE HUNDRED SIXTH CONGRESS

Congress of the United States
House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
MINORITY (202) 225–5051
TTY (202) 225–6852

HENRY A. WAXMAN, CALIFORNIA,
RANKING MINORITY MEMBER
TOM LANTOS, CALIFORNIA
ROBERT E. WISE, JR., WEST VIRGINIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
GARY A. CONDIT, CALIFORNIA
PATSY T. MINK, HAWAII
CAROLYN B. MALONEY, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
CHAKA FATTAH, PENNSYLVANIA
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
ROD R. BLAGOJEVICH, ILLINOIS
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
JIM TURNER, TEXAS
THOMAS H. ALLEN, MAINE
HAROLD E. FORD, JR., TENNESSEE
———
BERNARD SANDERS, VERMONT,
INDEPENDENT

Subcommittee on Government Management, Information, and Technology

"Year 2000 and Computer Security: The Expanded Risk of Financial Fraud"
Opening Statement of Chairman Stephen Horn (R-CA)
August 4, 1999

For the past three years, these two subcommittees have been prodding agencies in the executive branch of the Federal Government to prepare their computer systems for the Year 2000. Nearly all seem to have made good progress toward avoiding major computer disruptions at the end of this year.

However, the rush to solve the Year 2000 problem may have created another more insidious and potentially troubling problem.

Today, we will discuss the danger that government agencies, corporations and individuals are now more vulnerable to computer fraud – whether it is in the form of electronic robberies or information warfare.

The reality is that computer systems can be compromised for any number of reasons – some far more damaging than the loss of money. Among them, are the threats of industrial or military espionage, or the use of computers and network systems by terrorists or organized crime.

Private companies and government agencies alike have opened up their most sensitive computer systems to outside contractors who are helping them sort through billions of lines of computer code to ensure their Year 2000 compliance.

While the vast majority of these contractors are honest and trustworthy people, even a few unscrupulous operators could create a significant problem.

The Gartner Group, which is represented here today, has predicted that by 2004, there will be at least one reported loss of $1 billion or more due to the Year 2000 remediation effort.

The concern involves something called "trap doors," computer coding that can give unscrupulous contractors access to the sensitive information in a computer long after their Year 2000 work is completed.

From bank accounts and intellectual property to medical records and defense secrets, companies and Government agencies have given contractors the keys that unlock an enormous storehouse of information.

We have only 149 days left until the new millennium. We must ensure that our critical information technology infrastructure is secure long after the Year 2000 has passed away.

I welcome today's witnesses and look forward to their insights.

Chairwoman MORELLA. Thank you, Chairman Horn.

I am now pleased to recognize for any opening comments Mr. Udall, who is our ranking member today.

Mr. UDALL. Thank you, Madam Chairman. I want to join my colleagues in welcoming all of you here today to the hearing. This hearing focuses on two issues, the way I see it: computer and network security and then, secondly, whether Y2K-related computer system upgrades have increased the threat to a company's or a federal agency's computer security.

I'd like to take a few minutes to speak about the Science Committee's role in the area of computer security. Going back into the late 1980s, the members of this Committee were aware that the first computer networks, such as ARPANET, which became NSFNET and is now known, of course, as the Internet, had a two-edged quality: they improved electronic communication but also compromised computer security.

In 1987, the Science Committee was instrumental in developing and passing the Computer Security Act. This was the first effort to improve the security of federal computer systems. Ever since, the Science Committee has maintained a high profile in this area.

I mention this issue because many believe that Congress has not given sufficient attention to this issue of computer security. I wanted to highlight that at least one Congressional Committee has worked diligently to raise public and government awareness of computer security issues for more than a decade. This was long before most people even knew that the Internet existed, let alone before related computer security issues became important.

Today's hearing, as my fellow colleagues have mentioned, was prompted by recent newspaper stories about a GartnerGroup report warning that by 2004 there will be at least one publicly reported electronic theft exceeding $1 billion and that steps to solve the Y2K problem will be a root cause of the security lapses that have allowed this step to happen.

This is a serious assertion that raises more questions than it answers. For example, if it's true there will be at least a $1 billion theft, what about the likelihood of several thefts in the range of $100 million or the tens of thousands of dollars?

Further, how credible are these alarms? After all, the warnings themselves could undermine public trust in our financial systems and the government's ability to provide public services and in our computer-based infrastructure as a whole.

So, in that spirit, there are several issues that I hope our witnesses will address today. The first is: What data substantiates claims that there's an increased risk of fraud as a result of these Y2K fixes? Secondly, federal agencies, including Congress, and industry have relied on contractors to service their computer systems since their first installation. What has been the past experience of this type of fraud? And then, finally, if this Y2K-related fraud is a real problem, what steps can federal agencies and large corporations take to determine if the malicious code, the so-called trap doors, have been inserted into their programs?

I want to thank you for being here. I very much look forward to hearing what you have to say.

Thank you.

Chairwoman MORELLA. Thank you, Mr. Udall, and thank you for also mentioning sort of the genesis of the Science Committee's interest and involvement in this issue.

I'm now going to ask our panelists if they would rise and raise their right hand. It's the policy of this Committee to swear in those who will testify.

Do you swear that the testimony you are about to give is the truth, the whole truth, and nothing but the truth?

Mr. PUCCIARELLI. I do.

Mr. MILLER. I do.

Mr. RICH. I do.

Mr. BENNETT. I do.

Chairwoman MORELLA. The record will reflect an affirmative response from all. And, again, we'll try to follow a tradition, to give time for questions and other comments, of asking each panelist to speak about 5 minutes, and then we'll open it up to questions. And we'll start off then in the order in which I mentioned you.

Mr. Pucciarelli, you will start off with the Gartner report.

STATEMENTS OF JOSEPH C. PUCCIARELLI, VICE PRESIDENT AND RESEARCH DIRECTOR, GARTNERGROUP, INC., STAMFORD, CONNECTICUT; HARRIS N. MILLER, PRESIDENT, INFORMATION TECHNOLOGY ASSOCIATION OF AMERICA, ARLINGTON, VIRGINIA; L. DEAN RICH, VICE PRESIDENT FOR SECURITY SERVICES, WARROOM RESEARCH, ANNAPOLIS, MARYLAND; AND WAYNE D. BENNETT, CHAIR, COMMERCIAL TECHNOLOGY PRACTICE AREA, BINGHAM DANA LLP, BOSTON, MASSACHUSETTS

STATEMENT OF JOSEPH C. PUCCIARELLI

Mr. PUCCIARELLI. Madam Chairman—Madam Chairwoman, Mr. Chairman, and Members of the two Subcommittees, I appreciate the opportunity to testify——

Chairwoman MORELLA. I think you should either move it closer or make sure it's on.

Mr. PUCCIARELLI. Madam Chairwoman, Mr. Chairman, and Members of the two Subcommittees, I appreciate the opportunity to testify today on the computer security impact of year 2000 and the expanded risks of fraud. Key points in my testimony we will discuss: our prediction, the analysts of GartnerGroup, that by 2004 there will be at least one publicly reported electronic theft exceeding $1 billion, 70 percent likelihood; our forecast that year 2000 remediation efforts will be identified as a root cause of the security lapses that will have allowed this theft to happen, 70 percent likelihood; and how input from our clients was factored into these predictions and caused us to increase the probabilities.

My role is to advise business and financial executives in the public and private sector on actions they should take to protect and maximize the effectiveness of their investments in computer technology. We found medium and large organizations in the United States spend some 8 percent of sales revenue—that is, 8 cents of every sales dollar—for computer systems. Ten years ago, this number was only 1 percent. During the same period, our financial systems have largely migrated to an electronically interconnected

business model. Best estimates are that $11 trillion in electronic transfers occurred in the United States in 1998.

Earlier this year, as part of my ongoing research, I reviewed those issues that may require action by my clients. I concluded, by reviewing the technical research conducted by my colleagues at GartnerGroup, that many firms had not taken adequate steps to secure and audit a year 2000 remediation process. Based on these observations, I formulated a recommendation to our clients.

I reviewed these preliminary findings with some 300 clients on Tuesday, March 2, 1999, at a conference in New Orleans. Our clients had differing opinions. Their feedback indicated that the risk of theft was even higher than I had proposed. As a result, we formally advised our clients in April that we believe that by 2004 there will be at least one publicly reported electronic theft exceeding $1 billion, and that Y2K remediation efforts will be a root cause of those—that allowed this theft to happen, 70 percent likelihood.

Predicting what will happen is challenging. Anticipating how it may happen raises the bar considerably. In the case of the first $1 billion electronic theft, the motive will likely be one of greed combined with feelings of underappreciation by a highly skilled software engineer, especially related to the stress of the year 2000 remediation effort. The means will be the tools at hand—the same electronic systems reliably transact the business of the day will be instructed to transfer funds beyond the boundaries of the enterprise into the hands of a thief. The opportunity to perpetrate the crime will come in an odd moment, a situation outside the bounds of the operating manual. A system will crash unexpectedly and a single software engineer could make changes without the normal reviews, due diligence, or oversight. Further, the incident will likely occur long after January 1, 2000.

Clearly, a billion dollars is a huge sum of money. However, compared with the $11 trillion in annual volume of financial electronic data interchange transfers during 1998, which are growing some 40 percent annually, it represents only 0.0009 percent. To use a metaphor, a $1 billion theft compared to the $11 trillion in throughput equates to 48 minutes over the course of a year. In this context, a billion seems somewhat less significant. Opposing all this money is the unbounded creativity of the human mind—which has proved the world round, produced Einstein's theory of relativity, placed a man on the moon, and committed countless crimes throughout history. From the Brinks armored car robbery through the Great Train Robbery, to the most recent financial scandals including BCCI and Barings, each generation adapts theft and fraud to the technological circumstances of the day.

Given the enormity of the year 2000 remediation process, the scope of the cash flowing through these systems and the resourcefulness of the human mind in finding different ways to steal, a large theft seems much more likely perhaps inevitable.

Specific steps need to be taken now and continually re-emphasized to minimize risk. Specifically, we recommended:

One, the most effective theft and fraud deterrent is maintaining the perception that there are high levels of security. To accomplish this, we advise our clients to collaborate to create a year 2000 secu-

rity team with the requisite technical and auditing skills to review procedures, assess the threats, and implement a containment plan.

Second, procedure reviews must limit the ability of a single individual to make changes or initiate activities without a second person participating in the process.

Third, risk assessment must include reviewing all enterprise insurance coverage as well as contracts with external service providers and independent (programmer) contractors.

Four, risk management plans should include careful reconsideration of all existing theft and fraud deterrence activities in light of this expanded threat profile.

The law of very large numbers dictates that we will have a vastly increased risk of theft after the year 2000 remediation efforts. In the rush to aggressively solve one problem, enterprises need to ensure appropriate resources have been rededicated to protecting the enterprise from the increased risks of electronic theft and fraud—possibly the most important artifact created by year 2000 remediation. These nonlinear consequences of the year 2000 computer maintenance effort may have a more profound implication than the linear consequences such as a failure of a specific computer system.

Thank you.

[The statement of Mr. Pucciarelli follows:]

Year 2000 and the Expanded Risk of Financial Fraud

Expert Testimony of

Joseph C. Pucciarelli,

Vice President and Research Director,
Business Management of Information Technology Research Center,
GartnerGroup, Inc.,

to the

U.S. House of Representatives Science Committee's Subcommittee on Technology
and the Committee on Government Reform's Subcommittee on Government Management
Information and Technology,

Washington, D.C.

4 August 1999

Entire contents ©1999 by Gartner Group, Inc. All rights reserved.

Madam Chairwoman, Mr. Chairman, and Members of the Two Subcommittees:

I appreciate the opportunity to testify today on the computer security impact of year 2000 and the expanded risks of fraud. Key points in my testimony we will discuss:

- Our prediction (the analysts of GartnerGroup — see Note 1) that by 2004 there will be at least one publicly reported electronic theft exceeding $1 billion (70 percent likelihood — see Note 2).
- Our forecast that year 2000 remediation efforts will be identified as a root cause of the security lapses that will have allowed this theft to happen (70 percent likelihood).
- How input from our clients was factored into these predictions and caused us to increase the probabilities.

Introduction

My role is to advise business and financial executives, in the public and private sector, on specific actions they should take to protect and maximize the effectiveness of their investments in computer technology. We found in a recent survey that medium and large organizations in the United States spend some eight-percent of sales revenue (eight cents of every sales dollar) for computer systems. Ten years ago, we estimated this number to be only one-percent. Today it is difficult to buy any product in the U.S. that has not been influenced by computers — and the use of this technology is accelerating. During the same period, our financial systems have largely migrated to an electronically interconnected business model. Best estimates are that $11 trillion dollars in electronic transfers occurred in the U.S. in 1998 (see Note 3). To support this activity, we have created computerized systems to manage every aspect of these transactions.

Earlier this year, as part of my ongoing research, I reviewed those issues that may require action by my clients — executives involved in the financial aspects of managing enterprise-class computer systems. I concluded, by reviewing the technical research conducted by my colleagues at GartnerGroup, that many firms had not taken adequate steps to secure and audit the year 2000 remediation process — which is of course needed to maintain the integrity of these systems. As a result of the remediation process, we will, by Dec. 31, 1999, have systematically examined virtually every line of code, every interconnection, and every computer involved in this process (see Note 4). Based on these observations, I formulated a recommendation to our clients advising them to take immediate remedial action to manage this risk.

Research Findings

I reviewed these preliminary findings with some three hundred clients on Tuesday, March 2, 1999 at a conference in New Orleans. Our clients had differing opinions — their feedback indicated that the risk of theft was even higher than I had proposed. As a result of our research and our client's input, we concluded and formally advised our clients in April that given the enormity of this undertaking, the scope of the assets that flow through these computer systems, and the unbounded creativity of the human mind, we believe that by 2004 there will be at least one publicly reported electronic theft exceeding $1 billion (70 percent likelihood). Year 2000 remediation efforts will be a root cause of the security lapses that will have allowed this theft to happen (70 percent likelihood).

Entire contents © 1999 by Gartner Group, Inc. All rights reserved.

Outcome Scenario
Predicting *what* will happen is challenging, anticipating *how* it may happen raises the bar considerably. Law enforcement authorities attempting to solve a crime search to identify the *means* by which the crime occurs, establish the *motive* for the crime, and attempt to prove that a particular suspect had an *opportunity* to commit the crime. In the case of the first billion-dollar electronic theft or fraud, the *motive* will likely be one of greed combined with a highly skilled software engineer who feels unappreciated or under-recognized for his or her efforts and accomplishments (especially related to the very stress of the year 2000 remediation effort). The *means* will be the tools at hand — the same electronic systems that so reliably transact the business of the day will be instructed to transfer funds beyond the boundaries of the enterprise into the hands of the thief. The *opportunity* to perpetrate the crime will come in an odd moment: a situation outside the bounds of the operating manual. A system will crash unexpectedly and a single software engineer will make changes without the normal reviews, due diligence or oversight. Further, the opportunity will likely occur long after Jan. 1, 2000. One hypothetical scenario: unauthorized changes are made to the software during the year 2000 remediation process which allow the thief to come back after fact, by-pass normal security and commit the crime. A second hypothetical scenario: An artifact of the year 2000 remediation effort will cause a problem; a system will fail during an odd hour requiring emergency repairs. Someone will make a heroic save by working long hours so that a deadline can be met — and, along with the save, make unauthorized changes leading to the crime.

The Law of Large Numbers and the Human Mind
Clearly, a billion dollars is a huge sum of money; however, compared with the $11 trillion in annual volume of financial electronic data interchange during 1998 (which is growing some 40 percent annually), it represents only 0.0009 percent. To use a metaphor, a $1 billion theft compared to the $11 trillion in throughput equates to 48 minutes over the course of a year. In this context, a billion seems somewhat less significant. Opposing all this money is the unbounded creativity of the human mind — which has proved the world round, produced Einstein's theory of relativity, placed a man on the moon, and committed countless crimes throughout history. From the Brinks armored car robbery, through the Great Train Robbery, to the most recent financial scandals including BCCI and Barings, each generation adapts theft and fraud to the technological circumstances of the day.

Given the enormity of the year 2000 remediation process, the scope of the flowing through these systems, and the resourcefulness of the human mind in finding different ways to steal, a large theft seems much more likely — perhaps even inevitable.

Recommendations
Specific steps need to be taken now and continually reemphasized because, despite our wish for highly stable, status quo operations, changes in competition, business models and distribution channels will bring a much more dynamic operational norm. Specifically:

Entire contents © 1999 by Gartner Group, Inc. All rights reserved.

1. The most effective theft and fraud deterrent is the perception that there are very high levels of security. To accomplish this, we advise IS and finance organizations to collaborate to create a year 2000 security team composed of individuals with the requisite technical and auditing skills to review procedures, assess the risks and implement a risk containment plan.
2. Procedure reviews must limit the ability of a single individual to make changes or initiate activities without a second person participating in the process.
3. Risk assessment must include reviewing all enterprise insurance coverage as well as contracts with external services providers and independent (programmer) contractors.
4. Risk management plans should include careful reconsideration of all existing theft and fraud deterrence activities in light of this expanded threat profile.

Conclusion

The law of very large numbers dictates that we will have a vastly increased risk of electronic theft and fraud after the year 2000 remediation efforts. In the rush to aggressively solve one problem (year 2000), enterprises need to ensure appropriate resources have been rededicated to protecting the enterprise from the increased risks of electronic theft or fraud — possibly the most important artifact created by year 2000 remediation. These nonlinear consequences of the year 2000 computer maintenance effort may have more profound implications than linear consequences such as failure of specific computer systems.

Note 1
Background

GarnterGroup is a worldwide business and information technology advisory company, providing research and advice in more than eighty major focus areas of business, technology and E-business. One of those focus areas is year 2000. GartnerGroup researches year 2000 status, issues and best strategies, and provides advice and methods to companies and governments throughout the world. We are commonly referred to as the best year 2000 experts and the company with the most accurate and realistic understanding of year 2000 progress, status and risks worldwide.

Note 2
Probabilities and Scenario Planning

When making forecasts and predictions for our clients, GartnerGroup adopted the practice of assigning probabilities to our predictions so they could be appropriately factored into an organization scenario planning process. By assigning a 70 percent probability, we are saying to our clients that we believe they should definitively include this scenario as part of their planning process. This event is *likely* to happen. A scenario with a probability of 80 percent or higher almost certainly *will* happen.

Note 3
Volumes of Corporate Electronic Payments

Financial electronic data interchange (EDI) over the Automated Clearing House (ACH) Network grew by 42.7 percent in 1998, according to statistics released by the National Automated Clearing House Association. In 1998, more than 64.5 million financial EDI transactions crossed the ACH Network, up 42.7 percent from 1997. This figure includes business-to-business and government-to-business financial EDI, non-EDI payments, and intrabusiness cash concentration and cash management transfers. The dollar amount of these payments exceeded $11 trillion. Financial EDI is the electronic exchange of payments, payment-related information or financially related documents in standard formats between business partners. With financial EDI, the remittance information accompanies the payment; that is, the money and the data stay together.

Entire contents © 1999 by Gartner Group, Inc. All rights reserved.

Note 4
Year 2000 Remediation and Fraud
Year 2000 date remediation for software programming doesn't create the possibility of fraud *per se*. Rather, it is the requirement to open the code and allow changes in the hands of someone with nefarious intent that is the risk. Ideally, nonauthorized changes to parts of the program other than changes required for date remediation would be identified, reviewed in detail and certified by the quality assurance process. If either the change control process fails by not detecting other changes, or the quality assurance process fails by not certifying the appropriateness of all changes, then authorized changes could be made that, in combination with other security lapses, could combine to allow a theft. It is highly likely that, when and if this were to occur, it would be the result of a string of related failures and lapses. The problem is that, since we have never gone through this type of a broad-scale disruption, the "failure" mode will likely be a series of events we have never seen before. In other words, security teams need to think very creatively as they review and reconsider risk management and risk containment strategies.

Entire contents © 1999 by Gartner Group, Inc. All rights reserved.

Joseph Pucciarelli is a vice president and research director of GartnerGroup's Research and Advisory Services. He focuses on IT financial economics and life cycle management strategies, including IT budgeting, investment justification, scenario planning and asset management practices. Since joining GartnerGroup, he has actively participated in development of IT infrastructure management practices, IT procurement and leasing strategies.

Prior to joining GartnerGroup, Mr. Pucciarelli spent 15 years in the financial services industry with GE Capital, where he was involved in mergers and acquisitions, business strategy, marketing, and product and program management activities. During the last six years, these activities were centered on the formation and operation of captive leasing companies for IT manufacturers and distributors. Before that, Mr. Pucciarelli held a range of financial, operational and business management responsibilities with General Electric.

Mr. Pucciarelli earned a bachelor's degree, with honors, in systems planning and management from Stevens Institute of Technology, Hoboken, N. J.

GartnerGroup

56 Top Gallant Road
P.O. Box 10212
Stamford, CT 06904-2212

203.316.1277
203.316.6576
http://www.gartner.com

Date: August 2, 1999

To: F. James Sensenbrenner Jr.
Chairman House Committee on Science

Subject: Funding disclosure for J. Pucciarelli testimony 8/4/99

Gartner Group has one research and advisory service that is specifically focused on Y2K issues, one software assessment product and we [redacted] offer consulting services around Y2K assessment. In fiscal year 1999,we are doing approximately $2 million of business with federal government agencies around the Y2k issue.

Diane L. Julian
Regional Vice President, Federal Region

Mr. MILLER. Thank you, Chairwoman Morella and Chairman Horn and other Members of the Subcommittee. It is an honor to appear before your joint Subcommittees, and I want to commend you and your colleagues for holding this hearing on computer security as attention moves from the Y2K problem to the next and even greater challenge—Information Security or Critical Information Infrastructure Protection, as it is often called.

Just as your two Subcommittees were among the leaders in educating Congress and the Nation on the year 2000 challenge, I know that you will play the same role on Information Security. Make no mistake about it: Information Security is the next Y2K issue for the IT community and its users.

The evildoers are not just unscrupulous Y2K repair firms. The infosec threat comes in numerous guises: mischief-minded hackers, disgruntled employees, corporate spies, cyber criminals, terrorists, and unfriendly nations.

Virus episodes like Melissa and Chernobyl are becoming more frequent. The Symantec Anti-Virus Research Center estimates that new viruses are being launched at a rate of 10 to 15 per day and that over 2,400 currently exist, and 35 percent of those are considered to be intentionally destructive.

And, of course, there are the unintended consequences associated with our new dynamic information technology evolution, and, of course, year 2000 is the exhibit number one.

Assessing the ultimate infosec roles for government and the private sector is really very simple. Our new information-based assets must be protected and preserved. Participants and users must understand that along with the obvious benefits of information technology are corresponding commitments to protect information technology. With rights—the right for IT to become the firmament on which most of our society, our government, and our economy are built—come responsibilities. And the primary responsibility is to ensure the security of our information society. The societal stakes involved compel government and industry to seek common ground on the issue.

Security is much more challenging in the digital world because it is not the traditional security of wire fences, thick walls, and guard dogs. And it is not an activity just to be left to the experts, for all of us are part of the information age and must be sensitive to protecting it.

The road to a common ground between government and industry will never be a straight line. On the contrary, while the ends are commonly shared, the policies that government and industry will develop in order to provide this protection are likely to be quite different. Again, I remind the Subcommittees that the year 2000 is the wake-up call. A well-prepared and well-informed private sector can work with government to find the proper balance which optimizes the government's needs to protect the critical infrastructure with business' needs to manage risks appropriately.

Significant reservations exist, however, on the part of both private industry and government, and ITAA is attempting to address both from a theoretical and practical standpoint.

In developing industry positions on national infosec issues, ITAA has established a list of general principles that will guide the development of our policy. They emphasize industry leadership, communication and collaboration, infosec commensurate with the true threat involved without embellishment or magnification, and international collaboration. My written statement provided to the Committee outlines these principles in more detail.

But there are also many questions that must be addressed, including the question, for example: What should be the mechanism for sharing information between government and the private sector, or even within the private sector itself? What type of threat and intrusion reporting will be required as opposed to optional? What type of organizations should plan and execute the strategy for critical information infrastructure defense? And what kind of legal and regulatory obstacles are there to information sharing and information security?

And, of course, a less tangible concern must be addressed, particularly development of trust, both within the private sector and between the private sector and government. So as you can see, there is much to be done.

We are working with our customers and with our government to build the necessary bridges. ITAA is taking a number of actions to focus on this issue. Following, for example, the issuance of Presidential Decision Directive 63 last year, ITAA was appointed as the sector coordinator for the IT sector along with two other high-tech trade associations. We are involved in massive education efforts, including White Papers, and we have held frequent meetings with representatives across the government to educate, discuss, and provide input.

Education and outreach will be critical to the success of our efforts collectively. This past March, ITAA created the framework for a new Cybercitizen Partnership in conjunction with Attorney General Janet Reno. The partnership will focus on promoting individual responsibility in cyberspace and creating a private-public sector forum for exchange and cooperation.

In all honesty, we at ITAA face a daunting job of convincing the IT industry and our customers to work with government on these initiatives. But it is a challenge we must step up to if we are to achieve any degree of success in opening lines of communication.

The United States and much of the world are building their economic house on an information technology foundation. This is an extremely positive approach to take, delivering tangible benefits to a fast-growing percentage of the world's population. If year 2000 is the first challenge to place our economic house at risk, failure to adopt a rigorous approach to infosec will be the second and even more dangerous. ITAA and its member companies are committed to a private sector leadership role in ensuring that the necessary, timely, and cost-effective solutions are implemented.

Thank you, and I would be happy to answer any questions you may have.

[The statement of Mr. Miller follows:]

"The Computer Security Impact of Y2K: Expanded Risks of Fraud"

Testimony of

Harris N. Miller,
President
Information Technology Association of America

Presented to:

House Subcommittee on Technology and the Subcommittee on Government Management, Information, and Technology

August 4, 1999

Harris N. Miller
President
Information Technology Association of America (ITAA)

Harris N. Miller became President of the Information Technology Association of America (ITAA) in 1995. Miller directs the day-to-day operations of the association and reports to the ITAA Board of Directors. ITAA is the largest and oldest information technology (IT) trade association, representing 11,000 software, services, internet, telecommunications, electronic commerce and systems integration companies. ITAA has grown more than 25% each year that Miller has been President.

Miller is also President of the World Information Technology and Services Alliance (WITSA), an "association of associations" representing 38 high tech trade groups around the world. Recently he has been named a member of the Board of Directors of ITT Educational Services, Inc., a publicly traded corporation.

Miller leads ITAA's public policy focus in other areas such as encryption, taxation, IT workforce shortage, intellectual property, telecommunications reform, Year 2000 date conversion, and business immigration. He has testified before Congress and state legislatures on numerous issues, and briefed federal, state, and local officials on issues critical to the IT industry. He was a member of the Board of Directors of the 1998 World Congress on Information Technology. He has written and spoken widely on a variety of high tech issues and has been published in various popular and academic journals -- among others, *IT Professional Magazine* published by the Institute of Electrical and Electronics Engineers, and *The World Today* published by The Royal Institute of International Affairs. He also serves on the advisory boards of The Alliance for Technology Education (TATE) and *IT Staffing Solutions*, a Harcourt Brace Professional Publication. He is a much sought after conference presenter both nationally and internationally.

Among many significant accomplishments during the past four years, Miller:

- Conceived the ground-breaking study, "Help Wanted: The IT Workforce at the Dawn of a New Century." Under his leadership, ITAA produced the National Information Technology Workforce Convocation, which brought together leaders from education, government, and industry to formulate partnerships and "best practices" to increase the quantity and quality of IT workers.
- Led the IT industry in supporting the passage of Telecommunications Act of 1996 and assuring statutory protections for IT companies.
- Directed the association's creation of a multifaceted Year 2000 Century Date Change Program. ITAA is widely recognized by both government and industry as the foremost trade association in the Year 2000 area. Played an instrumental role in formulating the International Year 2000 Cooperation Center (IY2KCC) and conducted the first global summit on the Year 2000 issue, bringing together representatives from over 130 nations.
- Helped achieve numerous legislative and regulatory victories for the Information Technology industry, including creation of the Foreign Sales Corporation credit for software exporters, extension of the Research & Education tax credit, an Internet tax moratorium, extension of the H1-B visa limit for highly skilled foreign professionals, and government procurement reform.
- Secured ITAA's position as IT industry sector coordinator for Critical Information Infrastructure Protection under Presidential Decision Directive 63.
- Appeared on numerous network and cable television programs, radio programs and has been quoted in virtually all major national news publications. These include CBS, NBC, CNN, CNBC, BBC, *Wall Street Journal, New York Times, Washington Post, Business Week, Financial Times, The Economist* and many more.

Miller has a broad range of additional public policy experience. Prior to joining ITAA, he was president of Immigration Services Associates, a government relations firm based in Washington, D.C. specializing in immigration issues. Concurrently, he acted as government relations director for Fragomen, Del Rey & Bernsen, P.C., a nationwide law firm specializing in immigration, and he operated his own government relations firm, Harris Miller & Associates, with clients in high tech, agriculture and banking.

In addition to private sector experience, Miller has many years of government service, including assignments as Legislative Director to former U.S. Sen. John A. Durkin (D-NH); Deputy Director, Congressional Relations, U.S. Office of Personnel Management; and Legislative Assistant, Subcommittee on Immigration, Refugees and International Law, Committee on the Judiciary, U.S. House of Representatives.

Miller is also active in professional and civic activities. He served as chairman of the Fairfax County, Virginia Democratic party for six years. He served as co-chair of the Virginia Opera Northern Virginia Finance Committee and was a member of the Virginia State Lottery Board. Miller was chairman of the American Heart Association, Northern Virginia Council; member, Virginia Governor's Commission on the Federal Funding of State Domestic Programs; and served on the board of the National Conference of Christians and Jews, National Capitol Area Region. Currently, he serves on the Boards of Directors of The National Center for Technology and the Law - George Mason University's Tech Center, and The Center for Innovative Leadership in Blacksburg, Virginia. Miller is Co-Chairman of the 1999 Wolf Trap Ball Corporate Committee, and was recently featured on the cover of *Association Management Magazine*. In June of 1999, Mr. Miller was the recipient of *Federal Computer Week's* "Federal 100 of 1999 Award", presented to "...executives from government, industry and academia found by an independent panel of judges to have had the greatest impact on the government systems community..."

Miller holds an undergraduate degree from the University of Pittsburgh and a graduate degree from Yale University.

Introduction

I am Harris Miller, President of the Information Technology Association of America (ITAA), representing over 11,000 direct and affiliate member companies in the information technology (IT) industry - the enablers of the information economy. Our members are located in every state in the United States, and range from the smallest IT start-ups to industry leaders in the custom software, services, systems integration, telecommunications, Internet, and computer consulting fields. These firms are listed on the ITAA website at www.itaa.org.

Chairwoman Morella and Chairman Horn, it is an honor to appear before your joint Subcommittees. I want to commend you and your colleagues for holding this hearing on computer security as attention moves from the Y2K problem to the next and even greater challenge—Information Security (Infosec), or Critical Information Infrastructure Protection (CIIP), as it is also called.

Just as your two Subcommittees were the leaders in educating Congress and the nation on the Year 2000 challenge, I know you will play the same role on information security. When I first had the opportunities to testify before your Subcommittees three years ago on Y2K, it was tough to scare up a quorum. But because of your perseverance, gradually the country's leaders, the American people, and people around the globe became aware of Y2K. We must work together to achieve the same result on information security.

Information technology represents over 6 percent of global gross domestic product (GDP), a spending volume of more than $1.8 trillion, and over 8% of US GDP, according to Digital Planet, a report recently released by the World Information Technology and Services Alliance (WITSA). WITSA is a group of 38 IT trade associations around the world, and I am proud to serve as president of the organization. Enormous in its own right, the Digital Planet figures mask the contribution made by this technology to the growth, competitiveness and vitality of other industries. From China to Mexico, from Argentina to Germany, countries have come to recognize that information technology is the engine of national development, accelerating the expansion of business opportunity and investment while acting as a buffer against economic downturns. The recent US Department of Commerce report indicates that an incredible 35% of the nation's real economic growth from 1995 to 1998 came from IT producers.

The Year 2000 software glitch and other well-publicized episodes of natural or man-made disasters have also triggered an awareness of the importance of and vulnerabilities posed by disruptions to information technology. But to focus on the issue of computer malfeasance through a Y2K lens primarily is to peer at the issue from the wrong end of the telescope. Will there be some tampered code and loss of intellectual or monetary assets as the result of disingenuous Year 2000 fixes? No doubt about it. But at the margins of a multi-billion industry,

similar losses are occurring with or without Y2K. The real issue is what we have collectively learned about vulnerability from the date rollover, and where we go from here with this knowledge. Unlike Y2K, the Infosec challenge is not a point in time. Safeguarding our information assets is a job, which stretches from now to eternity. And the evil doers are not just unscrupulous Y2K repair firms. The Infosec threat comes in numerous guises. Mischief minded hackers. Disgruntled employees. Corporate spies. Cyber criminals. Terrorists. Unfriendly nations.

Make no mistake about it: Information Security is the next Y2K issue for the IT community and its users.

Aggressors attack at the point of maximum leverage. For modern society, this means critical infrastructure—transportation, telecommunications, oil and gas distribution, emergency services, water, electric power, finance and government operations. A critical information infrastructure supports all of these vital delivery systems and becomes itself a target of opportunity for terrorists, adversary nations, criminal organizations, and non-state sponsored actors. Disrupting the underlying information infrastructure of a transportation or finance system often can be as effective or even more effective than disrupting the physical infrastructure. Why blow up a power grid, when destroying the computers that control the power grid will have the same impact?

The International Institute for Strategic Studies (IISS) recently published a study on this topic citing one expert claiming he could bring down the U.S. information infrastructure with 10 computer specialists and in 90 days time. This potential vulnerability—even if overstated --raises numerous difficult questions for industry and government about how to best provide critical information infrastructure protection.

A recent Computer Security Institute (CSI) survey reports 62 percent of companies have experienced computer breaches; 51 percent of respondents reported financial losses due to computer security problems; criminal hacking losses of the 163 responding organizations was placed at $123 million in 1998 and is climbing at an extraordinary pace. The Institute found that system penetration by outsiders has risen in each of the past three years as has unauthorized access by insiders. Twenty-six percent of respondents in the CSI study reported theft of proprietary information and 27 percent reported financial fraud. Twenty percent reported unauthorized use or misuse of websites.

Virus episodes like Melissa and Chernobyl are becoming more frequent. The Symantec Anti-Virus Research Center estimates that new viruses are being launched at a rate of 10 to 15 per day and that over 2400 currently exist. Thirty-five percent are considered to be intentionally destructive.

Not all threats are man-made. As has been demonstrated by the 1997 Red River flooding of Grand Forks, North Dakota; the 1995 Kobe earthquake in Japan; and

the 1994 Northridge earthquake in California; and South Florida's Hurricane Andrew in 1992, natural disasters pose substantial threats to both major systems themselves and the critical information infrastructure on which their operation depend. This is indicative of the fact that the physical element of the information infrastructure requires a similar level of attention and concern. The Kobe earthquake, for instance, caused over 5,000 deaths, damaged or destroyed 180,000 buildings and left 300,000 people homeless. Total damages reached $147 billion. Telecommunications and computer infrastructures were out of commission for weeks and, in some cases, months.

And then there is that set of "unintended consequences" associated with a new and dynamic period in the evolution of technology. I refer to the Year 2000 computer bug as exhibit number one. As a global information economy, we stand at the very edge of the Year 2000 divide. Just five months remain for companies all over the world to complete their Y2K remediations. How successfully countries will make this transition is the subject of much speculation. The only sure prediction for Y2K prognosticators is that no one knows for sure the Y2K endgame. Year 2000 underscores the interconnectedness of society and its computers and the dependence of one on the other. Where we do not have all the technology bases protected, we have social, economic, and political vulnerabilities instead.

We have difficult challenges ahead. In the cyber realm, ambiguity reigns supreme. What makes our new environment so different? Some of the factors include:

- Increasing technological and environmental complexity – new technologies are replacing "old" ones at a breathtaking pace as hundreds of thousands of new players enter cyberspace on an almost daily basis;
- Boundless environment – geographic boundaries are irrelevant in cyberspace raising jurisdictional conflicts;
- Ambiguous laws;
- Anonymous adversaries – The anonymous nature of the Internet combined with a lack of geographic boundaries makes it extremely difficult to distinguish between nuisance hackers, vandals, criminals, terrorists and nation-states. This results in indistinguishable motives or intentions;
- Conflicting responsibilities and jurisdictions – while cyberspace is boundless, turf battles abound;
- Limited consequence management preparedness – if progress for preparations for Y2K and the recent Melissa and Chernobyl viruses are any indication, world-wide, individuals and enterprises are unprepared to manage contingencies and consequences of such incidents;
- Low levels of awareness – it was, and is still, difficult to get leaders to focus on Y2K as a major issue. We must now take pains to point out that Y2K is solely one "incident" on the continuum of potential vulnerabilities to our critical systems: the proverbial tip of the iceberg. A significant hurdle to meeting the

most basic challenges, however, is low level of awareness and understanding. These issues must be raised to the executive level;

- Limited human resources – The public and private sectors continue to struggle to find the skilled workers to manage the resources they currently have. Assuring our information infrastructures calls for more highly specialized individuals who are in extremely limited supply.

Government and Industry: Seeking Common Ground

Assessing the ultimate Infosec roles for government agencies and the private sector is really very simple: our new information-based assets must be protected and preserved. The proliferation of low cost computers and networks have spread information technology to every quarter of society. As technologies have advanced and been implemented, we have seen enormous payoffs in the form of increased efficiency, increased productivity and newfound prosperity. Chairman Alan Greenspan of the US Federal Reserve Board recently credited large investments being made in computers and other high-tech products for the dramatic boost in the nation's productivity. Even previously skeptical economists now concede that IT driven productivity increases have enabled our country to have what they said we could not have: high growth, low unemployment, low inflation, growth in real wages.

Rights come with responsibilities. Participants and users must understand that along with the obvious benefits of information technology are corresponding commitments to protect IT. The societal stakes involved in critical information protection compel government and industry to seek common ground on the issue.

The road to this common ground will never be a straight line. On the contrary, while the ends may be commonly shared, the policies that government and industry will develop in order to provide this protection are likely to be quite different.

For instance, government policy may seek to establish both internal and externally directed standards to protect infrastructure elements from physical or cyber attack, to require systems to detect when attacks are imminent or underway, to develop processes to react to the attack, and to reestablish the critical service. By definition, if the service has been deemed critical to the nation, then the federal, state and local governments will have increased interest in the operation, management and protection of the private businesses and services which comprise the infrastructure elements. The manner in which this government concern is manifested can have a significant effect on private sector interests.

Similarly, industry can be expected to react to infrastructure threats in appropriate ways, guided by sound business considerations. Individual

companies will make infrastructure protection investments commensurate with the risk management principles in their industries. Government policies that impose protection standards more stringent than those inherent in the private sector risk mitigation process may not be acceptable. Additionally, requirements for reporting incidents to government operations centers and responding to government directed reconstitution plans might impose burdens that need to be developed in consultation with the private sector.

Private sector firms face other real world pressures in formulating an Infosec response. First, companies run the significant risk of negative publicity and exposure. Companies are concerned that revealing and admitting past mistakes, shortcomings, negative experiences or incidents can open them up for criticism from the press, their competitors, their customers and their shareholders. Along the same lines, and for good reason, companies are loath to share proprietary or privileged corporate information. Additionally, firms run the risk of harming consumer, customer, partner and investor confidence. The private sector is also unprepared to share information and/or experiences out of fear that such information will be misused, abused or released to the public by the government or competitors. Lastly, with the focus in today's corporate world on the immediate bottom line, most firms see no clear short-term return on their information sharing investment.

To minimize the likelihood of, minimize the possible impact from, or prepare a response to a coordinated, comprehensive attack on critical US infrastructure will require coordinated, comprehensive teamwork by government and industry. No matter what the business or political pressures, we all have a stake in protecting our information infrastructure. The nature of that teamwork is being decided through national debate, substantive analysis and constructive dialogue. As we look ahead, our nation is in need of new modes of cooperation, collaboration and experience sharing among the private sector and between the public and private sectors. Year 2000 is the wake-up call. A well prepared and informed private sector can work with government to find the proper balance which optimizes the government's need to protect the critical infrastructure with business' need to manage risks appropriately.

Significant reservations on the part of both private industry and government to fully collaborate on these important issues exist, however, which ITAA is attempting to address from both a theoretical and practical viewpoint.

Infosec: Establishing First Principles

In developing industry positions on national Infosec issues, ITAA has established an initial list of general principles that will guide the development of future policy.

- The protection of the national information infrastructure must be based on the minimum amount of government (federal, state, and local) regulation as is feasible.

- The cost of protecting the national information infrastructure must be kept to the lowest level possible commensurate with the threat and the consequences of attack. Parties must be able to differentiate between potential vulnerabilities and specific threats.

- Industry owns and operates the Global Information Infrastructure and, as such, has primary responsibility for Infosec requirements, design and implementation.

- Industry and government share an interest in the proliferation of a free and open Internet, electronic commerce, other value-added networks, and an efficient, effective information infrastructure generally.

- In protecting these resources, the specific and immediate priorities of government and industry are apt to diverge.

- Industry will be guided by business considerations to protect itself against physical and cyber-attack as the threat to the information infrastructure evolves.

- Where corrective Infosec action is required to protect the public good, government must identify such instances and create appropriate funding mechanisms.

- The Internet and electronic commerce are inherently global in nature; therefore, information security will require collaboration among international bodies.

- Infosec measures must be commensurate with the threat involved; risks must be appropriately identified and managed but not magnified or embellished.

- Positive interaction between government and industry is essential. Among issues which will require on-going communication and assessment is the need to balance the Constitutional right to privacy with national security concerns.

- Industry must monitor the private sector portion of the national information infrastructure and cooperate both internally and with government in reporting and exchanging information concerning threats, attacks, and protective measures. Coordination among principals must facilitate creation of early warning systems.

- In creating the information infrastructure, as well as attendant tools and technologies, industry must be provided safe harbor protections and its works viewed as incidental to losses caused by criminal or malicious misbehavior or natural disasters.

- Distinctions must be made among cyber-mischief; cyber-crime and cyber-war to clarify jurisdictional issues and determine appropriate responses. The adequacy of current laws to prevent these threats must be reviewed.

- Existing laws must be adapted as necessary to allow appropriate levels of information sharing among companies, and between the private sector and government.

- Current policy in areas such as the R&E tax credit, software encryption, workforce training and long-term government research, and development funding must be reviewed in light of common Infosec goals and objectives.

- Law enforcement agencies must gain sufficient cyber-crime expertise to combat specific threats and to investigate specific criminal acts.

- Emergency response organizations must gain sufficient disaster recovery expertise to minimize the effect of catastrophic events on the information infrastructure.

Implementing this diverse set of principles will require substantial work, resources, and cooperation.

Difficult Issues Remain

At this nascent stage, many questions remain unanswered:

- What are the criteria for determining the individual elements of the critical information infrastructure, and who is involved in the determination?

- What should be the process/mechanism by which the government will provide threat, indications and warning information to critical information infrastructure companies?

- What legislative remedies are necessary to overcome the current legal barriers to information sharing?

- Will shared information be protected from FOIA requests?

- What threshold should be established for reporting anomalous activity? What type of reporting will be required, given that industry will be motivated to

monitor and protect itself against cyber-attack for business reasons, and how will reported information be protected?

- What government restrictions/legislation must be modified or lifted so that private sector companies may implement active cyber-defense and/or counter-measures (i.e., anti-trust provisions leading to NSTAC-like organizations)?

- What type of organization(s) should plan and execute the strategy for critical information infrastructure defense?

- What policy determinations are required to distinguish between law enforcement and national security (warfare) jurisdictions as a result of attacks on critical information infrastructure elements?

- How should industry organize itself to represent private sector views, to exchange relevant "lessons learned," and to participate in policy development? Given that IT is both a vertical industry sector itself, but also underlies all the other vertical sectors, what should be the relationship between the IT sector and the others?

- What considerations must be allowed for those elements of the critical infrastructure, which are foreign controlled or are part of multi-national businesses, considering that most infrastructures are international in nature?

- How should the information technology private sector assess the implications of liability and insurance for critical services?

- Is there a sufficient research and development effort underway to improve the ability of the private sector to monitor and protect its designated critical elements? Who should fund this effort? How should R&D information be distributed?

- If information system security becomes a competitive market differentiator, how will the private sector accommodate the needs of the government for infrastructure protection while maintaining market competitiveness?

- How does our country develop a corps of IT workers with particular skills to focus on security and infrastructure protection, particularly in light of the overall IT workforce shortage?

In addition to substantive legal and policy issues, less tangible concerns must also be addressed, particularly the development of trust—within the private sector and between the private sector and government. ITAA and its member companies are working with government to help build the necessary bridges. I would like to describe briefly a few of these initiatives now.

ITAA and Infosec

ITAA is taking a number of actions, has initiated programs, and motivated its membership to address the Infosec challenges that the nation and our industry face. ITAA realized the importance of this issue and took it on over two years ago with the establishment of a dedicated Critical Information Protection Task Group to examine and analyze policy developments in this area and to offer input into the policy process. In the past year ITAA's Critical Information Protection Task Group, now called the Information Infrastructure Assurance Committee (IIAC), has continued its mission of providing ITAA outreach and education to Administration officials, federal civilian, military, national security, and law enforcement agencies, Congress, the media, international organizations, and the public on the issues of information security and assurance. The IIAC has been very active particularly in the wake of Presidential Decision Directive 63 (PDD63), which was issued last spring. IIAC activity is increasing as federal agencies and industry grapple with the implementation of PDD63 which has provided the initial outline and direction for the development of a more comprehensive national infrastructure protection strategy and plan.

In the past 12 months, much has happened. Through the IIAC, our members have been active in what has been the rapid development of information infrastructure security issues and policy. Our organization has produced one of the first concerted industry efforts to address Infosec issues. We have issued white papers focused on critical information infrastructure protection. We prepared an industry response to President's Commission on Critical Infrastructure Protection (PCCIP) report and recommendations when they were released in the fall of 1997.

Since then, we have held frequent meetings with representatives across the government to educate, discuss and provide input into the evolving national policy developments.

In February of this year, the Department of Commerce selected ITAA as a Sector Coordinator for the Information and Communications Infrastructure sector, in conjunction with two other associations focused primarily on the telecommunications industry—the US Telephone Association and the Telecommunications Industry Association. As a Sector Coordinator, we are continuing to work with the federal government and, in particular, with NTIA on the implementation of PDD 63.

Education and outreach will be critical to the success of our efforts. This March, ITAA created the framework for a new Cybercitizen Partnership in conjunction with Attorney General Janet Reno. The Partnership will focus on promoting individual responsibility in cyberspace and creating a public-private sector forum for exchange and cooperation. Through the Partnership, private sector representatives hope to work with federal partners, including the Attorney General, the Department of Justice and National Security Agency

representatives, on development of a critical infrastructure protection education and awareness campaign and other initiatives. In addition to an awareness campaign we will be coordinating with the FBI's National Infrastructure Protection Center to identify and coordinate industry representation and participation in Center activities to build the communication and trust that will be so essential in moving forward.

Also of note: In October 1998, I was appointed by the World Information Technology and Services Alliance (WITSA) to chair a new task force on critical information infrastructure. WITSA has been quick to recognize the need for industry to take a proactive role in protecting information infrastructures. At a meeting in Taipei earlier this spring, WITSA members approved a policy statement that encourages government-industry dialogue at the local, national and international levels.

While both private industry and governments at all levels agree that there is a growing need to address the challenges of Infosec, there is little agreement on what measures, if any, should be taken to protect those infrastructures. At the heart of the Statement is the message that industry has a vested interest in anticipating and confronting infrastructure threats in appropriate ways, guided by business considerations. While countries have very different ways of approaching Infosec, WITSA believes that it is of critical importance that governments and international organizations always cooperate fully with industry in shaping information security policy.

In all honesty, we at ITAA face a daunting job of convincing the IT industry to work with these agencies on these initiatives. It is a challenge we must step up to if we are to achieve any degree of success in opening lines of communication. Our industry continues to have reservations about working too closely with the federal law enforcement and national security community, particularly with the scars of the encryption conflict still fresh.

ITAA and our members will continue to look forward to cooperating with all agencies and elements of government to meet the Infosec challenges. Yet we feel that NTIA is the proper representative to work with our industry to begin to build the necessary levels of cooperation to help develop the National Infrastructure Protection Plan. Within DOC, NTIA has the knowledge of and experience and relationships with the IT and Communications industries that are necessary.

Over the past two years, ITAA, its members and the IT industry have begun to develop collegial and constructive relationships with the leadership and staff of the Department of Justice (DOJ), the National Security Council (NSC), the National Security Agency (NSA), the National Information Protection Center (NIPC), the Critical Information Assurance Office (CIAO), the Commerce Department (DOC), NTIA and the Critical Information Infrastructure Assurance

Program Office (CIIAP) at NTIA in their capacity as the lead agency for our industry. While significant, positive levels of trust, cooperation and communication have been developing; the important work that must be done has barely started. This is not because of any lack of desire or ability on behalf of NTIA or the CIIAP Office, but because they have been asked to do their job without the necessary resources. They lack even the minimum funding and support that is necessary for them to carry out their mission. It is essential that the necessary programmatic funding and resources be appropriated to the NTIA to carry out its mission. $3.5 million is a small price to pay for getting these important programs moving down the track.

Conclusion

The U.S. and much of the world are building their economic house on an information technology foundation. This is extremely positive approach to take, delivering tangible benefits to a fast growing percentage of the world's population. As we build this house which reaches to a better, more prosperous and democratic future, we must be ever vigilant of cracks in this structure. If Year 2000 is the first challenge to place our economic house at risk, failure to adopt a rigorous approach to Infosec will be the second and even more dangerous. I have offered a conceptual framework on which government and industry can work towards common ground. ITAA and its member companies are committed to a private sector leadership role in insuring that the necessary, timely and cost effective solutions are implemented.

Thank you and I would be happy to answer any questions you may have.

Harris N. Miller
President
Information Technology Association of America (ITAA)

Harris N. Miller became President of the Information Technology Association of America (ITAA) in 1995. Miller directs the day-to-day operations of the association and reports to the ITAA Board of Directors. ITAA is the largest and oldest information technology (IT) trade association, representing 11,000 software, services, internet, telecommunications, electronic commerce and systems integration companies. ITAA has grown more than 25% each year that Miller has been President.

Miller is also President of the World Information Technology and Services Alliance (WITSA), an "association of associations" representing 38 high tech trade groups around the world. Recently he has been named a member of the Board of Directors of ITT Educational Services, Inc., a publicly traded corporation.

Miller leads ITAA's public policy focus in other areas such as encryption, taxation, IT workforce shortage, intellectual property, telecommunications reform, Year 2000 date conversion, and business immigration. He has testified before Congress and state legislatures on numerous issues, and briefed federal, state, and local officials on issues critical to the IT industry. He was a member of the Board of Directors of the 1998 World Congress on Information Technology. He has written and spoken widely on a variety of high tech issues and has been published in various popular and academic journals -- among others, *IT Professional Magazine* published by the Institute of Electrical and Electronics Engineers, and *The World Today* published by The Royal Institute of International Affairs. He also serves on the advisory boards of The Alliance for Technology Education (TATE) and *IT Staffing Solutions*, a Harcourt Brace Professional Publication. He is a much sought after conference presenter both nationally and internationally.

Among many significant accomplishments during the past four years, Miller:

- Conceived the ground-breaking study, "Help Wanted: The IT Workforce at the Dawn of a New Century." Under his leadership, ITAA produced the National Information Technology Workforce Convocation, which brought together leaders from education, government, and industry to formulate partnerships and "best practices" to increase the quantity and quality of IT workers.
- Led the IT industry in supporting the passage of Telecommunications Act of 1996 and assuring statutory protections for IT companies.
- Directed the association's creation of a multifaceted Year 2000 Century Date Change Program. ITAA is widely recognized by both government and industry as the foremost trade association in the Year 2000 area. Played an instrumental role in formulating the International Year 2000 Cooperation Center (IY2KCC) and conducted the first global summit on the Year 2000 issue, bringing together representatives from over 130 nations.
- Helped achieve numerous legislative and regulatory victories for the Information Technology industry, including creation of the Foreign Sales Corporation credit for software exporters, extension of the Research & Education tax credit, an Internet tax moratorium, extension of the H1-B visa limit for highly skilled foreign professionals, and government procurement reform.
- Secured ITAA's position as IT industry sector coordinator for Critical Information Infrastructure Protection under Presidential Decision Directive 63.
- Appeared on numerous network and cable television programs, radio programs and has been quoted in virtually all major national news publications. These include CBS, NBC, CNN, CNBC, BBC, *Wall Street Journal, New York Times, Washington Post, Business Week, Financial Times, The Economist* and many more.

Miller has a broad range of additional public policy experience. Prior to joining ITAA, he was president of Immigration Services Associates, a government relations firm based in Washington, D.C. specializing in immigration issues. Concurrently, he acted as government relations director for Fragomen, Del Rey & Bernsen, P.C., a nationwide law firm specializing in immigration, and he operated his own government relations firm, Harris Miller & Associates, with clients in high tech, agriculture and banking.

In addition to private sector experience, Miller has many years of government service, including assignments as Legislative Director to former U.S. Sen. John A. Durkin (D-NH); Deputy Director, Congressional Relations, U.S. Office of Personnel Management; and Legislative Assistant, Subcommittee on Immigration, Refugees and International Law, Committee on the Judiciary, U.S. House of Representatives.

Miller is also active in professional and civic activities. He served as chairman of the Fairfax County, Virginia Democratic party for six years. He served as co-chair of the Virginia Opera Northern Virginia Finance Committee and was a member of the Virginia State Lottery Board. Miller was chairman of the American Heart Association, Northern Virginia Council; member, Virginia Governor's Commission on the Federal Funding of State Domestic Programs; and served on the board of the National Conference of Christians and Jews, National Capitol Area Region. Currently, he serves on the Boards of Directors of The National Center for Technology and the Law - George Mason University's Tech Center, and The Center for Innovative Leadership in Blacksburg, Virginia. Miller is Co-Chairman of the 1999 Wolf Trap Ball Corporate Committee, and was recently featured on the cover of *Association Management Magazine*. In June of 1999, Mr. Miller was the recipient of *Federal Computer Week's* "Federal 100 of 1999 Award", presented to "...executives from government, industry and academia found by an independent panel of judges to have had the greatest impact on the government systems community..."

Miller holds an undergraduate degree from the University of Pittsburgh and a graduate degree from Yale University.

TRUTH-IN-TESTIMONY DISCLOSURE

Part I: Witness Identification

1. Name:	2. Address:
HARRIS N. MILLER	1616 N FT. MYER DR. ARLINGTON VA 22209
3. Phone Number: 703-284-5340	

Part II: Group Identification

4. Please identify the group(s) or organization(s) on whose behalf you are testifying. If you are not testifying on behalf of any group or organization, please indicate "none."		
INFORMATION TECHNOLOGY ASSOCIATION OF AMERICA (ITAA)		
5. Are you testifying on behalf of a governmental organization, meaning a federal department or agency, or a state or local department, agency, or jurisdiction? (If "yes," skip to item 7.)	YES	NO ✓

Part III: Federal Grants and Contracts

6a. Have you, or any of the organizations or groups which you may be representing, received any federal grants or contracts (including subgrants or subcontracts) that are relevant to the subject of the hearing during the current fiscal year or any of the two (2) preceding fiscal years?	YES	NO ✓

6b. If you checked "yes" for item 6a above, please list the source and amount for each grant, contract, subgrant, or subcontract, received within that period. Please attach additional sheets if necessary.

Source	Amount

Part IV: Signature

7. Please sign and date indicating that to the best of your knowledge the information provided on this form is both true and accurate.	
Signature	Date 8/2/99

Chairwoman MORELLA. Thank you, Mr. Miller. And I want all of the panelists to know that the entirety of their statements as submitted to us will be included in the record, and I know that you have submitted extensive statements, and we appreciate that.

Mr. Rich, I now recognize you, sir. May I indicate that we have been joined by Mr. Bartlett from the great State of Maryland. Mr. Rich is from Maryland, Mr. Bartlett.

STATEMENT OF L. DEAN RICH

Mr. RICH. Thank you. Chairwoman Morella, Chairman Horn, and Members of the Subcommittees, I appreciate the opportunity to appear before you and I thank you for continuing to address the problems associated with information assurance and national critical infrastructure. As a lead into Y2K, I'd like to submit that Y2K, while a problem in itself, is a manifestation of a much larger issue—overall infrastructure assurance. We can look at Y2K as a wake-up event to better understand and manage those systems that are increasing in control or influencing every aspect of our lives.

I come to this Committee with a background of information security as a Naval Reserve Officer in the Naval Cryptologic community and as a businessman working with industry to address the very issues we are discussing today. I support the Naval Criminal Investigative Service in my reserve capacity addressing threat issues. In my civilian position, I am currently with WarRoom Research as Vice President of Security Services, addressing both threat and vulnerability issues.

You might recall that WarRoom research services the U.S. Senate's Permanent Subcommittee on Investigations under the 1996 Security in Cyberspace Hearings where we collected information security risk profiles of 205 Fortune 1,000 corporations.

As we move even further into the digital age, those elements that comprise electronic commerce, networked systems, and national infrastructure are increasingly at risk. In order for this networked world to be viable and to be able to operate without concern and with all the worries transparent to the user, there must be an underpinning of robust security. Often we take security for granted or, using traditional cost analysis, will accept a certain level of risk as a cost of doing business. However, in today's environment, the cost of doing business without a strong security posture is too high. Yet many are unaware of these costs. In order to understand the new requirements of the digital age, governments and businesses must understand that security can no longer be an afterthought or redlined when budgets get squeezed. Security must be integral to one's overall management picture.

To effectively manage security, one must manage risk. I believe in the formula risk equals threat multiplied by vulnerabilities and apply it to my own business decisions. You can see that with zero threat no matter the vulnerabilities, you will have zero risk. Likewise, if you have zero vulnerabilities and a world of "bad actors," you have zero risk. Unfortunately, we have a great number of both, which is driving the risk index skyward.

Vulnerabilities within our infrastructure are exposed on almost a daily basis. The scale of the infrastructure affected magnifies the

impact of these vulnerabilities. Popular computer programs that get larger distribution have a larger impact. This has been demonstrated recently by a vulnerability that allows the promulgation of Macro viruses via e-mail. Using the risk formula, this vulnerability would not be an issue if it were not for the immense threat we live with on a daily basis.

I believe the threat to our infrastructure is real. During the hearings on security in cyberspace in June of 1996, Mr. John Deutch did a great job of summarizing the threat and the need for increased public awareness. Many companies and government agencies have taken a skeptic's approach when discussing threats. They will say, "My network and systems are running fine. I don't see any threat here." They lack the ability to see the threat and, therefore, deny it exists. They would be surprised to see, with an intrusion detection package—or intrusion detection application on their Internet perimeter, they would detect at least one unusual occurrence a day.

A number of years ago, while on active duty in the Navy, I was deployed aboard a submarine for a couple of months. Having an interest in the sonar system, I asked one of the crew to give me an overview. The young officer was very proud of the system and said, "If something were out in the water, we would hear it." I caught him by surprise when I said, "So, let me get it straight. If you don't hear, it isn't there?" I think that overconfidence in current capabilities and the unwillingness to "think out of the box" will lead to complacency. You need to look before you can see the threat. I support innovated efforts to look where no one has looked before.

I'd like to share a couple of short stories, and I will keep it to the first one in the interest of time. In early 1995, I was running a vulnerability assessment on a large number of Internet connected systems operated by the Department of Defense—a Department of Defense organization. During the assessment, I entered a computer that was used by software developers to maintain the source code for a communications package. The source code was clearly unclassified, but it was disturbing for me to know its only use was on a classified network. A "total systems" approach was not used when implementing a support structure for the communications package.

Others have demonstrated similar events over the last couple of years, and we'll still continue to have these problems.

I'd like to address the Y2K vulnerability issue. A recent newspaper article brought to light a problem of outsourcing Y2K remediation and the threat of foreign nation states inserting backdoors for future year. I believe this is a valid threat and agree it needs to be addressed today. On the other hand, many Fortune 500 companies have been outsourcing source code development and maintenance for years. A large number of these U.S. companies have permanent network connections into their corporate networks to facilitate the work from overseas. I can tell you that without intrusion detection or traffic analysis, these foreign companies have the potential to run free and obtain unauthorized access to U.S. corporate proprietary information.

In summary, I would recommend programs that support a total risk management approach to infrastructure assurance. I recommend protecting the critical path and the life cycle of high-value

infrastructure, not just the end product. Keeping vigilant in the search for vulnerabilities and new threats. I fully support the requirement for collaboration between government and commercial organizations. We will not survive as a country without a framework of trust, dialogue, and collaboration. I look forward to working with this Subcommittee and others on this issue within the months to come.

Again, thank you for the opportunity to speak, and I'd be happy to answer any questions.

[The statement of Mr. Rich follows:]

STATEMENT BY
MR. L. DEAN RICH
VICE PRESIDENT, SECURITY SERVICES
WARROOM RESEARCH INC.
BEFORE
THE SCIENCE COMMITTEE'S SUBCOMMITTEE ON TECHNOLOGY
AND
THE COMMITTEE ON GOVERNMENT REFORM'S SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION AND TECHNOLOGY

AUGUST 04, 1999

10:00 A.M.

HEARINGS ON
"THE COMPUTER SECURITY IMPACT OF Y2K: EXPANDED RISKS OF FRAUD?"

Chairwoman Morella, Chairman Horn, and members of the sub-committees, I appreciate the opportunity to appear before you and I thank you for continuing to address the problems associated with information assurance and national critical infrastructure. As a lead into Y2K, I'd like to submit that Y2K, while a problem in itself, is a manifestation of a much larger issue—overall infrastructure assurance. We can look at Y2K as a wake up event to better understand and manage those systems that are increasing in control or influencing every aspect of our lives.

I come to this committee with a background of information security as a Naval Reserve Officer in the Naval Cryptologic community and as a businessman working with industry to address the very issues we are discussing today. I support the Naval Criminal Investigative Service in my reserve capacity addressing the threat issues. In my civilian position I am currently with WarRoom Research, as Vice President of Security Services addressing both threat and vulnerability issues. You might recall that WarRoom Research served the U.S. Senate's Permanent Subcommittee on Investigations under the 1996 Security in Cyberspace Hearings where we collected information security risk profiles of 205 Fortune 1,000 corporations.

As we move ever further into the digital age, those elements that comprise electronic commerce, networked systems, and national infrastructure are increasingly at risk. In order for this networked world to be viable, to be able to operate without concern and with all the worries transparent to the user, there must be an underpinning of robust security. Often we take security for granted or, using traditional cost analysis, will accept a certain level of risk as the cost of doing business. However, in today's environment, the cost of doing business without a strong security posture is too high—yet many are unaware of these costs. In order to understand the new requirements of the digital age, governments and businesses must understand that security can no longer be an afterthought or redlined when budgets get squeezed. Security must be integral to one overall management picture.

To effectively manage security, one must manage risk. I believe in the formula Risk = Threat multiplied by Vulnerabilities and apply it to my own business decisions. You can see that with zero threat no matter the vulnerabilities, you will have zero risk. Likewise, if you have zero vulnerabilities and a world of "bad - actors", you have zero risk. Unfortunately, we have a great number of both, which is driving the risk index skyward.

Vulnerabilities within our infrastructure are exposed on an almost daily basis. The scale of the infrastructure affected magnifies the impact of these vulnerabilities. Popular computer programs that get a larger distribution will have a larger impact. This has been demonstrated recently by a vulnerability that allows the promulgation of Macro viruses via email. Using the risk formula, this vulnerability would not be an issue if it were not for the immense threat we live with on a daily basis.

I believe the threat to our infrastructure is real. During the hearings on "Security in Cyberspace", in June of 1996, Mr. John Deutch did a great job of summarizing the threat and the need for increased public awareness. Many companies and government agencies have taken a skeptic's approach when discussing threats. They will say, "my network and systems are running fine, I don't see any threat here". They lack the ability to see the threat and therefore deny that it exists. They would be surprised to see that with an intrusion detection application on their Internet perimeter, they would detect at least one unusual occurrence each day. A number of years ago while on active duty in the Navy, I was deployed aboard a submarine for a couple of months. Having an interest in the sonar system I asked one of the crew to give me an overview. The young officer was very proud of the system and said that if something were out in the water, we would hear it. I then caught him by surprise when I said, "so, let me get this straight, if you don't hear it, it isn't there?" I think that overconfidence in current capabilities and the unwillingness to "think out of the box" will lead to complacency. You need to look, before you can see the threat. I support innovated efforts to look where no one has looked before.

I'd like to share a couple of short stories to make a point of how vulnerabilities in a low value environment can migrate to a high value environment.

- In early 1995, I was running a vulnerability assessment on a large number of Internet connected systems operated by a Department of Defense organization. During the assessment, I entered a computer that was used by software developers to maintain the source code for a communications package. The source code was clearly unclassified, but it was disturbing for me to know its only use was on a classified network. A "total system" approach was not used when implementing a support structure for the communications package.

- During the fall of 1995, I was asked to give a demonstration of network based vulnerabilities to the Naval Research Advisory Committee. I brought in my home computer running a popular operating system called Linux. I then proceeded to dialup to the Internet through a commercial Internet provider to give an unrehearsed demo. Right before their eyes I was able to find a system that did not have a "root" or system administrator password. We found that the system was running a 30-GigaByte Oracle database used for joint logistics support. Clearly the system was not configured properly and given the value of the data, one would think it should have had some form of intrusion detection implemented.

Others have demonstrated similar events over the last couple of years and we still continue to have these problems.

I'd like to address the Y2K vulnerability issue. A recent newspaper article brought to light a problem of "outsourcing" Y2K remediation and the threat of foreign nation states inserting "backdoors" for future use. I believe this is a valid threat and agree that it needs to be addressed today. On the other hand, many of the Fortune 500 companies have been "outsourcing" source code development and maintenance for years. A large number of these US companies have permanent network connections into their corporate networks to facilitate the work from overseas. I can tell you that without intrusion detection or traffic analysis, these foreign companies have the potential to run free and obtain unauthorized access to US corporate propriety information.

In summary, I would recommend programs that support a total "Risk Management" approach to Infrastructure Assurance. I recommend protecting the "critical path" and life cycle of high value infrastructure, not just the end product. Keeping vigilant in the search for vulnerabilities and new threats. I fully support the requirement for collaboration between government and commercial organizations. We will not survive as a country without a framework of trust, dialogue and collaboration. I look forward to working with this Subcommittee and others on this issue in the months to come.

Again, thank you for this opportunity to speak with you and I would be happy to answer any questions.

L. Dean Rich, Vice President, WarRoom Research Inc.

As Vice President at WarRoom Research, Mr. Rich leads the firm's Security Services business supporting Business Intelligence.

Mr. Rich joined WarRoom in July 1999 after serving as Vice President and Chief Security Officer for USinternetworking Inc, a market leader Applications Service Provider. Mr. Designed and established a robust security program to address the ever increasing threats and vulnerabilities associated with Internet connectivity. Prior to USinternetworking, Mr. Rich held senior positions with Booz-Allen & Hamilton and Internet Security Systems.

Mr. Rich has fifteen years of experience in the field of security. He designed the configuration and implemented the nation's first federal 'network wiretap' in support of a historical Department of Justice case against an international hacker. Mr. Rich has extensive experience in multi-platform system/network analysis, operations, and management, and is a specialist in conducting penetration analysis. He designed and wrote the original software program used by the Defense Information Systems Agency (DISA) to conduct penetration analysis of networked systems (SeaWitch). Mr. Rich, while on active duty in the US Navy, designed and implemented the US Navy's Defensive Information Warfare Program at the Fleet Information Warfare Center. Mr. Rich is the author of 'UNIX Security: a Penetration Analysis of Navy Computer Systems,' and ' Military Computer Network Security in the UNIX Environment.' He has a Bachelor of Science in Marine Engineering from the Maine Maritime Academy and a Master of Science in Computer Science from the Naval Postgraduate School in Monterey, CA.

L. DEAN RICH
(410) 571-1080
deanr@warroomresearch.com

OBJECTIVE Senior Level Executive for Innovative Technology and Information Security

EDUCATION M.S. Computer Science, Naval Postgraduate School, Monterey CA, 1992
B.S. Marine Engineering, Maine Maritime Academy, Castine Maine, 1985

OVERVIEW Broad professional background in leadership, management and technical positions.

Designed and implemented the configuration of our Nation's first federal "network wiretap" in support of the Department of Justice case against an Argentine national named Julio Cesar Ardita. This case made history in that it was the first time law enforcement had received approval for a "wiretap" without naming a suspected individual in the affidavit. The Judge allowed monitoring to occur based on known methods unique to the "hacker" after "minimization" rules had been approved to protect innocent citizens' privacy.

Extensive experience in multi-platform system/network analysis, operations, and management with specialization in conducting penetration analysis. Personally designed and wrote the original software program used by the Defense Information Systems Agency (DISA) to conduct penetration analysis of networked systems. A major emphasis of the penetration analysis has been in evaluating UNIX security controls and associated risk management techniques required to protect national defense data, proprietary information, integrity and confidentiality of privacy data and enhance user productivity.

PROFESSIONAL HISTORY

VICE PRESIDENT SECURITY SERVICES – Joined WarRoom Research Inc., a business Intelligence Company, in July 1999. Responsible for providing a number of security services focused on a secure environment for the exchange of very sensitive/propriety information. Security services offered become a catalyst for a client's business intelligence program.

VICE PRESIDENT/CHIEF SECURITY OFFICER – Lead a team of security experts to design and implement a "Total Security Architecture" program for USinternetworking Inc. The program addressed security at every layer of the ISO networking model. USi is considered the leader in Internet based Managed Applications (iMAP) where a good strong security program is paramount to obtain and maintain client trust. (July 1998 – May 1999)

REGIONAL DIRECTOR – Professional Services Director for Internet Security Systems Inc. Responsible for establishing and managing a team of security professionals that specialize in vulnerability and threat detection. Focus of this work is in offering subject matter experts to help customers with implementation and integration of the ISS SafeSuite of products and all security related issues. (Dec 1997 – July 1998)

CORPORATE PRESIDENT – President of Strategic Security Solutions Inc (S3I) located in Manassas, Virginia. S3I provides information security assistance to corporations that wish to achieve "self-reliance". Assistance is provided in a multiphase approach: Operations Assessment, Risk Assessment, Risk Reduction Plan, Training and Reduction Plan Implementation. The last phase is a "Step-Back with Retainer" service providing long-term strategic consulting support to corporate management (June 1997 – Nov 1997).

MANAGEMENT CONSULTANT - Specialized in providing short focused vulnerability assessments to commercial companies called "Commercial RedTeams". These RedTeams were designed to test any aspect of information protection measures implemented at a client's site. Testing primarily focused on LAN/WAN attack scenarios but also included other means to gain data/access to include "social engineering", physical access and "dumpster diving". Each assessment included operational assessment, risk assessment and a risk reduction plan.
Booz-Allen & Hamilton Inc., McLean VA. November 1996 – May 1997.

PROGRAM MANAGER - Personally designed and implemented the U.S. Navy's Defensive Information Warfare Program at the Fleet Information Warfare Center. Exercised overall management, control and technical authority for the Navy Computer Incident Response Team (NAVCIRT), Vulnerability Analysis and Assistance Program (VAAP) and the Automated Security Incident Measurement Program (ASIMP).
Fleet Information Warfare Center, Norfolk VA. July 1995 - November 1996.

DEPARTMENT HEAD - Information Systems Technical Manager for complex multi-functional Local and Wide Area Networks processing sensitive national defense data. Created, directed and maintained an information system security hierarchy based on teamwork to enhance the protection, preserve the integrity of proprietary and access information.
Naval Security Group Activity, Pensacola FL. January 1993 - June 1995.

PROGRAMMER - Designed, integrated, and tested user software applications which effectively and efficiently protect sensitive data, without degrading service or end user productivity. A majority of these applications deal with information security or user account management and billing for Internet Service Providers.
January 1991 – November 1996.

TECHNICAL MANAGER - Lead technical manager for a project that transferred mission critical national defense processing from a DEC PDP/1170 to a desktop 386 personal computer. This project saved the Navy an estimated $750,000 annually.
Naval Security Group Activity, Fort George G. Meade MD Jun 1988 - Jun 1990.

PRIOR EMPLOYMENT

During the period of June 1978 and August 1980, I was serving in the US Navy as an Electronics Technician with a specialty in Satellite Communication maintenance. After graduation from Maine Maritime Academy in April of 1985, I was commissioned a Naval Officer and reconvened my Naval career. As a Naval Officer I held a number of challenging positions both at sea and ashore. I have lead and managed up to 53 personnel and held positions such as: Electronics Material Officer, Electrical Officer, Weapons Officer and Assistant Engineering Officer. I changed my career path from Surface Warfare to Intelligence during the summer of 1988.

COMPUTER SYSTEMS

Hardware: SUN HPW; Macintosh; HP HPW; IBM PC(compatible); VAX/PDP(series);
Operating Systems: UNIX (BSD, SUN-OS, HP-UX, SCO); DEC-VAX/VMS; MS-DOS.
Tools/Applications: OpenWindows; X-Windows; MS-Windows; WordPerfect; MS-EXCEL; MS-Word; Lotus 123; Harvard Graphics; VAX/VMS Utilities; and various other applications.
Programming Languages: Perl; ANSI C; C++; ADA; FORTRAN; Basic.

SECURITY CLEARANCE

TS/SCI based on a SSBI and polygraph

PUBLICATIONS

UNIX Security: A penetration Analysis of Navy Computer Systems, Masters Thesis, Naval Postgraduate School, Monterey CA, 1992.
Military Computer Network Security in the UNIX Environment, IEEE Military Communications Conference, 1992.

August 2, 1999

To Whom It May Concern:

Since its inception in 1995, neither WarRoom Ventures, Inc, nor WarRoom Research, Inc. nor any subsidiaries of these corporations has received federal funds of any kind.

Sincerely,
WarRoom Ventures, Inc.

Mark L. Barnett
President

WarRoom Research, Inc. • 401 Defense Highway • Annapolis, Maryland 21401 • USA
Tel: 410.571.1080 • Fax: 410.571.1081 • email: info@warroomresearch.com • www.warroomresearch.c

Chairwoman MORELLA. We thank you very much, Mr. Rich, and it's now my pleasure to recognize Mr. Bennett.

STATEMENT OF WAYNE D. BENNETT

Mr. BENNETT. Thank you, Chairwoman Morella, Chairman Horn, members of the Subcommittee. My name is Wayne Bennett. I'm a partner at the law firm of Bingham Dana, and I chair the Commercial Technology Practice Area at our firm. Thank you for inviting me to this hearing.

The nearly boundless creativity of the criminal mind will likely one day result in a billion dollar computer fraud. But I believe the apparent increased risk presented by the Y2K remediation effort is more than offset by the improvements in remediation procedures that have been implemented at large and mid-sized companies precisely to deal with the behemoth Y2K effort. When the billion dollar fraud occurs, its connection to the Y2K remediation effort will be more in the nature of serendipity than statistical inference, and law enforcement will be in a better position to identify the perpetrator because of the changes that the Y2K effort has brought.

Consider the recent testimony of Gary Beach, Publisher of CIO Magazine, before the Senate Special Committee on the Y2K Technology Problem. I'm a member of the CIO Magazine editorial advisory board, and I can attest to the efforts that organization has made to look past the Y2K hype and its coverage. While the purpose of Gary's testimony was to report the results of a Y2K tracking poll, Gary added a particularly incisive thought at the conclusion of his remarks that one positive legacy of the Y2K exercise is that many companies were finally moved to undertake comprehensive inventories of their information technology systems.

I would expand on that notion of a positive legacy. The learning at many corporate IT departments, particularly at mid-sized corporations, has been greatly enhanced since the Y2K wake-up call went out. My clients are from diverse industries, including banks, mortgage companies, manufacturers, distributors, broker dealers, grocers, IT hardware, software, and services lenders, and e-commerce companies. Many of them contacted leading experts to teach their IT personnel the best industry practices for implementing their Y2K projects, and they're applying that learning to their maintenance activities generally.

Before the Y2K exercise, systems maintenance was in some IT shops just a tedious chore that was relegated to anonymous junior programmers. Maintenance was a stepchild, and many IT departments struggled with version control, documentation, and accountability. Often IT personnel would open a source code file and find no written clue regarding who worked on the code last, what changes had been made, or even when or why it was changed.

The best maintenance practices recently introduced by consultants have a by-product. Many systems environments are now more secure than they were just a couple of years ago. For example, the introduction of project notebooks requiring formal sign-offs by responsible employees and contractors have employees staking their reputations on their work. Each sign-off indicates that a software routine is ready and that it successfully integrates into the larger system. Testing naturally becomes more comprehensive. Validation

efforts are enhanced to ensure that no unwanted changes have been introduced into the system. Internal and external auditors review project notebooks as part of their Y2K and technology operations audits. Reports are generated at each management level until a summary is presented to the board of directors. Visibility and accountability at every level has increased. Security has been enhanced.

Trap doors and the attendant risk of major fraud have been around since shortly after the beginning of commercial computing.

Then you enacted the Computer Fraud and Abuse Act of 1986, the Information Infrastructure Act of 1996, the Economic Espionage Act of 1996, and the No Electronic Theft Act of 1997. The criminal laws are in place. Now, with the introduction of better maintenance practices, the forensic evidence is more likely to be available to track down a wrongdoer.

A billion-dollar fraud is inevitable at some point since no security system is completely airtight. But is it more likely now as a result of the Y2K effort? I don't think so.

Consider the current criminal opportunity. With increased scrutiny of every line of code, choosing this juncture to hide nefarious software in systems is akin to the decision of a second story man choosing to burglarize the police chief's house. Some burglars may find the prospect challenging, but most won't and those that do will find the going rather rough.

At the July 22nd Senate Y2K hearing, Senator Bennett put the question of the reported increased security risk to a panel of IT executives. The panelists acknowledged that the security risk is increasing every day because of the increase in computer usage generally. But they also responded that the procedures implemented to perform Y2K remediation make them more confident today that while they can never fully prevent a security problem, they can at least better now detect a security problem.

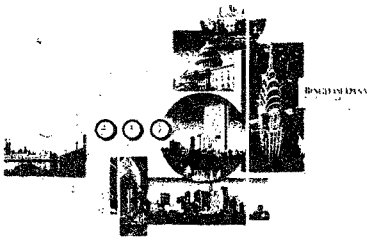
These procedures can fail, so we need to be ever vigilant about security. But we should also be careful about any message that we send to those thousands of employees and contractors who are honestly and diligently trying to solve the Y2K problem.

The Nation's IT personnel are right now working at a breakneck pace doing thankless, yeoman's work against an unforgiving deadline. If they succeed in their Herculean task, some—perhaps even some here today—will question why we spent billions of dollars on a crisis that never came about. If they fail, they will be blamed.

At this point, I suggest that we let the security officers quietly pursue their jobs while we lend all necessary support to the employees and contractors working on the Y2K effort—without any inadvertent suggestion from any quarter that any of them might be criminals, even in the face of continuing risk. The job of fixing the Y2K problem and the consequences of failure are so enormous that the ongoing risk of fraud pales by comparison. We should keep our focus over these next critical few months.

Thank you for your time.

[The statement of Mr. Bennett follows:]



BINGHAM DANA
LLP
150 FEDERAL STREET, BOSTON, MASSACHUSETTS 02110-1726
(617) 951-8000 FAX: (617) 951-8736 www.bingham.com

BOSTON • NEW YORK • WASHINGTON
LOS ANGELES • HARTFORD • LONDON

Joint Hearing
of
The Science Committee's Subcommittee on Technology
and
The Government Reform Committee's Subcommittee on Government Management, Information and Technology:

"The Security Impact of Y2K: Expanded Risks of Fraud?"

United States House of Representatives
Wednesday, August 4, 1999
10:00 A.M.
Room 2318
Rayburn House Office Building

Testimony of Wayne D. Bennett

Chairwoman Morella, Chairman Horn, Members of the Subcommittee, my name is Wayne Bennett. I am a partner at the law firm of Bingham Dana and I Chair the Commercial Technology Practice Area at our firm. Thank you for the opportunity to present my views here today.

I was asked by the joint committee to testify concerning the recent GartnerGroup report regarding the "Year 2000 and the Expanded Risk of Financial Fraud." That report suggests that that the risk of electronic financial theft and fraud will have "vastly increased" as a result of Y2K remediation efforts because so much remedial programming activity invokes the "law of large numbers" with respect to the likelihood that unauthorized changes could be made, causing financial harm. The report predicts with 70% probability that at least one publicly reported $1 billion fraud will occur by 2004. The report raises serious concerns about the confluence of Y2K and security risks.

I do not doubt that the nearly boundless creativity of the criminal mind will likely one day result in a $1 billion computer fraud. I would suggest, however, that the increased risk presented by the Y2K remediation effort is more than offset by the improvements in remediation procedures, particularly in the area of accountability, that have been implemented at large and mid-sized companies precisely to deal with the behemoth Y2K effort. That billion dollar fraud will one day occur, but I believe that its connection to the Y2K remediation effort would be more in the nature of serendipity than statistical inference; and law enforcement will be in a better position to identify the perpetrator because of the changes that the Y2K effort has brought.

My testimony is not based upon any formal study. It is anecdotal, based upon my own experience, beginning in the '70s as a mathematician and systems developer (both in government and in private industry) and in the '80s and '90s as a lawyer and, for a time, CEO of a technology company that

provided software to the nation's fire service under the brand name, FireSoft. This career path has given me an opportunity to see the Y2K and computer security problems from many sides. I was there in the '70s when the Y2K problem was openly laughed about, even among some of our own federal government software developers (on the theory that no one would be using this software by 2000 and in any event, they would then be retired). As an attorney, I have advised companies that supply software and IT services, as well as those who purchase them. I have suffered security breaches and advised clients who have suffered security breaches. I currently advise Y2K committees at banks, mortgage companies, a stock exchange, manufacturers, grocers, software companies, hardware companies, service companies and internet companies.

I am pleased to report that my clients and their suppliers are taking both Y2K and security very seriously. By seriously, I mean they are allocating their most precious commodities -- their time, money and reputations -- to these issues.

While concerns about Y2K and computer security are each considerable and justified, I would caution against concluding that any significant multiplier is at work; or that the possibility of fraud exacerbates the risk that is inherent and is already being addressed in connection with the Y2K problem -- namely, the risk that critical operations will be disrupted because of systems that are not Y2K compliant.

It is true that the Y2K effort has involved the remediation of an unprecedented number of programs by an unprecedented number of programmers. This multiplies the *opportunity* for bad actors intent upon disrupting or stealing, by way of hidden software of various kinds. But the conclusions that might otherwise be drawn by simply applying the law of large numbers should be tempered at least somewhat by the other events that have attended the massive Y2K remediation effort that is currently underway.

I recommend to your attention the recent testimony of Gary Beach, Publisher of CIO Magazine before the Senate Special Committee on the Y2K Technology Problem. I am privileged to sit on the editorial advisory board of CIO Magazine and I can attest to the efforts that organization has made to look past the Y2K hype and to discover what is really going on in corporate America to address the problem. While the purpose of Gary's testimony was to report the results of a comprehensive Y2K tracking poll, Gary added a particularly incisive thought at the conclusion of his remarks: He indicated that one positive legacy of the Y2K exercise is that many companies were finally moved by the Y2K problem to undertake comprehensive inventories of their information technology systems, something they ought to have been doing all along.

I would expand on that notion of a positive legacy. The learning at many corporate IT departments throughout the United States, particularly at mid-sized corporations, has been greatly enhanced since the Y2K wake-up call went out a couple of years ago. Many of my clients, from diverse industries, contacted leading experts to teach their IT personnel the best industry practices for implementing their Y2K projects, and they are applying that learning to their maintenance activities generally.

Before the Y2K exercise, systems maintenance was, in some IT shops, just an expensive, tedious chore that was relegated to anonymous programmers who were hoping to one day escape to a better life in software development -- where the action, career opportunity and real learning has been thought to be. Maintenance was the step-child in the IT department and although vast resources have been spent on maintenance since the dawn of commercial computing, many IT departments constantly struggled with version control, documentation and accountability. It was not uncommon, before the Y2K exercise began, for IT personnel to open up a source code file and have no written clue regarding who worked on the code last, what changes had been made or even when or why changes had been previously made.

Many maintenance endeavors were just plain sloppy. The real learning regarding various versions of any program was not evident from the in-line documentation or a project notebook, which often did not exist, but in the head of the programmer who had to most recently modify the code. That programmer might or might not still be with the company. I dare say that more time has been spent in many maintenance efforts trying to decipher past maintenance efforts than has been spent actual fixing the problem that gave rise to the maintenance effort in the first instance.

The introduction of consultants to teach "best practices" in maintenance in order to accomplish Y2K remediation has changed the nature and profile of maintenance activities at many organizations. And a by-product of that improved profile is that many systems environments are now more secure than they were just a couple of years ago.

An example might help. You may recall that in 1998, about 10% of the nation's banks received notices from bank regulators that their Y2K progress was not then satisfactory and that until additional strides were demonstrated, those banks would not be permitted to acquire other banks. In an era of bank merger mania, these notices were taken quite seriously. One such bank that I know of had an acquisition in progress when the notice was received. The initial reaction of some bank personnel was that their Y2K efforts were sufficient but that the bank had simply done an inadequate job of explaining to regulators how much progress had been made.

The CEO of the bank called in our law firm, as well as a leading accounting firm to help prepare a further response to regulators. After a swift, but detailed joint investigation, the Bingham Dana view and the Arthur Andersen view were presented to the Board of Directors. We reported that the problem was only partly that the bank had not adequately explained its progress to regulators; that a bigger problem was that the regulators were right – inadequate progress had been made; further, that the two problems were inextricably related. We explained that without proper planning, resource allocation and record keeping, the bank would forever be unable to demonstrate its progress because it would have no real idea what its progress was. Without any real idea of progress, the bank could work for a very long time and never complete the task.

After much hand-wringing, the accountants brought in a team to teach the bank's personnel the best industry practices in maintenance. These included extensive planning exercises in which assumptions were repeatedly tested and re-tested, and realistic resource allocations that took into consideration the fact that some remediation personnel still had day-to-day operating responsibilities because this was not one of the nation's largest banks. Perhaps most importantly, detailed project notebooks were introduced into the process, in order to measure progress against plans, enhance accountability and facilitate audits and testing.

This last point is critical. The introduction of project notebooks requiring formal sign-offs by responsible employees and contractors, changes the nature of the process. Once employees are required to stake their reputations on their work with formal sign-offs, the care with which each step is undertaken is significantly enhanced. Where before, an ill-defined group of people might work on various aspects of a system, now each individual software routine has an owner who is responsible to the point of initialing a page in a project notebook to indicate that the routine itself is ready and that it successfully integrates into the larger system. Testing becomes more comprehensive. Validation efforts are enhanced to ensure that no unwanted changes have been introduced into the system. Internal auditors and even external auditors have started including review of these project notebooks as part of their Y2K and technology and operations audits. Roll-up reports are generated regularly at each level until an overall summary is available for presentation to the Board of Directors by the Y2K Committee. Visibility and accountability at every level has increased, as compared to maintenance activities of just a couple of years ago.

That bank got back on track quickly and I am pleased to report that it completed its acquisition and has impressed bank regulators upon every subsequent visit. But once every week since the dreaded regulatory notice arrived at that bank more than a year ago, a subcommittee of the Board of Directors reviews the progress of the bank's Y2K efforts. And bank personnel will happily admit that they are a better organization for having gone through the painful process.

Remember that the Y2K problem is just a series of software bugs. Bugs have plagued all but the most trivial software systems since Grace Hopper coined the term "bug" decades ago. Many bugs have adversely affected mission critical systems and throughout those decades, employees and contractors have routinely performed maintenance surgery on these systems. The most unique aspect of the Y2K bug is that the deadline for fixing it is absolutely inflexible. But the inflexibility of the deadline was an excellent motivator for mid-sized companies -- it forced many of them to implement the kind of careful practices that had previously been used principally by the world's largest companies.

Trap doors and other, similar software have been around from shortly after the beginning of commercial computing. Throughout the history of computing, the risk of major fraud by way of computer has been a real issue. From the earliest computer software maintenance activities decades ago until the commencement of the Y2K effort more recently, a huge number of programmers have engaged in maintenance and a still larger number of programs have been maintained. The risk of fraud and theft by way of maintenance activities has been present from the outset and the threat has not only come from contractors, but even from employees.

This risk has already led to federal legislation, notably in the form of The Computer Fraud and Abuse Act of 1986, as amended by the Information Infrastructure Act of 1996 (18 USC §1030 *et seq.*, providing criminal penalties for computer fraud), the Economic Espionage Act of 1996 (18 USC §1831 *et seq.*, providing criminal penalties for theft of trade secrets) and the No Electronic Theft Act of 1997, which amended 18 USC §2319 to provide criminal penalties for a broader range of copyright infringements, including those that were the subject of *United States* v *LaMacchia*, 871 F.Supp. 535 (D. Mass. 1994). The criminal laws are in place and now, with the introduction of better maintenance practices, the forensic evidence is more likely to be available to track down a wrongdoer, irrespective of whether he or she is an employee or a contractor.

I lump together contractors and employees because the nation's employers are scarcely in a better position to assess the trustworthiness of a new employee than they are as to a contractor. The human resources directors who call their law firms for guidance concerning employee references are told pretty much the same thing throughout the United States: say as little as possible. Give dates of employment and position and title. Be polite but get off the phone by indicating that it is your corporate policy not to give references. This applies with even greater force to former employees who were suspected of bad behavior. Why? Because employers face lawsuits and substantial liability to former employees if they share information with prospective employers and that person is denied a job.

This state of affairs is quite dangerous for all employers. Consider also, the longstanding judicial disfavor of non-compete clauses in employment contracts (and in California, a near-complete prohibition on non-competes), and you will quickly understand the real fear among employers: not the billion dollar financial fraud, but the theft of competitive intelligence, both from computer attacks and the nearly unfettered mobility of employees between competitive firms.

Is it possible that either during the remediation process or in the midst of confusion at the moment of a Y2K crisis at the start of the new year, an employee or contractor will insert code into a program that will result in a billion dollar financial fraud? Of course it is, just as it has been possible throughout

commercial computing. In fact, such a fraud at some point is inevitable, since no security system is completely airtight and criminals are quite innovative. But is it more likely now? I doubt it.
Put yourself in the mind of a criminal for a moment. With new accountability procedures in place and increased scrutiny of every line of code, choosing this juncture to hide nefarious software in systems is akin to the decision of a second story man choosing to burglarize the police chief's house. Some burglars might find the prospect challenging, but most won't and those that do will find the going rather rough.

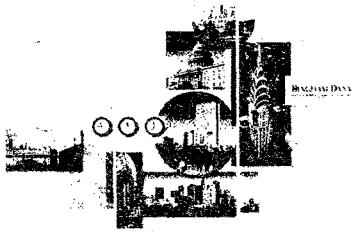
At the July 22, 1999 hearing held by the Senate Special Committee on the Year 2000 Problem, Senator Bennett put the question of the reported, increased security risk to a panel of IT executives from Ford Motor Company, Ahold USA, Philip Morris and Proctor & Gamble. The panelists acknowledged that the security risk is increasing every day because of the increase in computer usage generally. But they also responded that the procedures implemented to perform Y2K remediation (including accountability, testing and version control procedures) make them more confident today that while they can never fully prevent a security problem, they can at least now better detect a security problem. I agree.

As GartnerGroup suggests in its report, these procedures can fail, so companies need to be ever vigilant on the security front. Those companies that have not upgraded their procedures need to do so right away; those that already implemented proper procedures need to constantly revise and upgrade those procedures because security will always be a cat and mouse game of sorts, not unlike the police battle against ever-improving radar detection, but with different stakes. But we should also be careful about any message we send to those who are honestly and diligently trying to solve the Y2K problem, including thousands of contractors.

The nation's IT personnel are right now working at a breakneck pace doing thankless, yeoman's work against an unforgiving deadline. Many have already agreed to forego their holidays and much-needed vacations. If they get away at all, it will be with a pager or cell phone strapped to their waist and powered on, ready for a summons on a moment's notice. If they succeed in their Herculean task, some (perhaps even some here today) will question why we spent billions of dollars on a crisis that never came about; if they fail, they will be blamed.

At this point, I suggest that we let the security officers quietly pursue their job while we lend all necessary support to the employees and contractors working on the Y2K effort -- without any inadvertent suggestion from Congress that any of them might be criminals, even in the face of continuing risk. The job of fixing the Y2K problem and the consequences of failure so enormous that the on-going risk of fraud, particularly at a time when detection methods, as well as accountability have improved, pales by comparison. My recommendation is to thank the nation's IT workers for their efforts and to ask them if we can offer any support during these next critical 150 days.

Chairwoman Morella, Chairman Horn, Members of the Subcommittee; thank you for your time.



BINGHAM DANA
LLP
150 FEDERAL STREET, BOSTON, MASSACHUSETTS 02110-1726
(617) 951-8000 FAX: (617) 951-8736 www.bingham.com

BOSTON • NEW YORK • WASHINGTON
LOS ANGELES • HARTFORD • LONDON

Wayne D. Bennett

Wayne Bennett is a partner in the Boston law firm of Bingham Dana LLP. He is in the Firm's Entrepreneurial Services Group, where he maintains a general corporate and commercial practice, focusing on emerging companies and the effective use of intellectual property. Wayne leads the Firm's Commercial Technology Practice (which also includes the Firm's Y2K Practice) and he Co-Chairs the Firm's Intellectual Property Practice. Mr. Bennett graduated from Syracuse University in 1974 and Georgetown University Law Center in 1981.

Mr. Bennett worked as a mathematician in the public and private sectors before joining the Firm in 1981. As a mathematician, Wayne was responsible for the design, development and world-wide deployment of mainframe applications and operating systems, as well as the development of assemblers and compilers for minicomputers. In the course of his work with the Department of the Navy and the National Bureau of Standards, Mr. Bennett was one of a handful of practitioners involved in the application of queueing theory to the measurement of computer performance and was a frequent lecturer on the topic of computer performance measurement and simulation.

In 1986, he left the Firm to serve as CEO of a troubled software company, where he led the company's turnaround, which involved retooling its product, restaffing and identifying new market directions. After several years as an entrepreneur, he returned to Bingham Dana to help other high technology companies.

Mr. Bennett's practice focuses on both emerging and established companies in technology licensing, outsourcing, OEM, reseller, distribution and related strategic alliances, systems integration and technology development arrangements, Y2K issues, equity financing and a broad range of commercial and e-commerce matters. Clients include E-Ink, Streamline.com, Boston Scientific, BankBoston, USTrust, InfoLibria, Ab Initio Software, Boston Equiserve, Avid Sports, Excelergy, GMAC, McCracken Financial, NECX, Tanger Factory Outlets, RealityWave, Vacation.com, ThinkMart.com, FLEXCon, National Broach and the New England Revolution.

The Y2K Practice spans a diverse client base, including technology providers as well as licensees: banks, mortgage companies, broker/dealers, a stock exchange, manufacturers, distributors, service providers, grocers, software developers, integrators and outsourcing vendors. After the Spring 1998 round of Federal Reserve notices to banks indicating inadequate Y2K progress (and holding up pending bank acquisition applications), Wayne became involved in one of the first successful efforts to "rehabilitate" a bank's Y2K program. Bennett sits on the Y2K Steering Committees of several client companies.

Wayne is Vice Chair of the ABA Subcommittee on Software Contracting, which is tasked with helping to shape the draft software licensing and electronic commerce provisions of the Uniform Computer Information Transactions Act (*UCITA*). He lectures on internet- and software-related topics and authored the Firm's *Business Guide to Intellectual Property*. Wayne is a member of the Editorial Advisory Board of CIO Magazine and a member of the Board of Directors of the Massachusetts Interactive Media Council.

BINGHAM DANA LLP

Intellectual Property & Technology Activities

- Vice Chair of the Software Contracting Subcommittee of the ABA's UCC Committee, helping to shape the proposed Uniform Computer Information Transactions Act (*UCITA*) to address licensing, software services, systems integration, EDI and continuous access contracts
- Member, Editorial Advisory Board, *CIO Magazine*
- Member, Board of Directors, Director, Massachusetts Interactive Media Council
- Authored *A Business Guide to Intellectual Property*
- Editor, *Bytes & Rights* newsletter covering business and legal developments in intellectual property and technology
- Co-authored E-Mail & Attorney-Client Privilege, *The Data Law Report*, July 1996
- Co-authored Raising Capital: Some Basics, The MIT Enterprise Forum of Cambridge, *ForumReporter*, January, 1997.
- Authored The Surprisingly Long Arm of the Law, *Webmaster Magazine*, March 1997
- Authored (on behalf of ABA Article 2B Subcommittee) Technological Self-Help: Draft UCC §716, *Commercial Law Newsletter*, July 1997
- Authored Looking Both Ways: An Employer Perspective On Policies Governing Internet Use At Work, *CIO Magazine*, October 1, 1997
- Authored A Very Public Affair: Using Information Collected Over the Internet From Customers, *CIO Web Business*, December 1, 1997.
- Authored, Legal & Blinding: The UCC2B Debate, *CIO Magazine*, October 1998
- Authored Hot Potato: The Hardware Sizing Risk, *CIO Magazine*, April 1999
- Authored A Code Day in Hell: Software Escrows, *CIO Magazine*, June 1999
- Authored Dear Leader: IT Purchasing, *CIO Magazine*, September 1999
- Lectured at **Massachusetts Institute of Technology**, The Electronic Frontier: Public Policy & Legal Dimensions, Catherine N. Stratton Seminars on Critical Legal Issues, October 1995
- Lectured at **The Communications Business & Finance Conference**, Telecommunications Convergence: Legal & Business Issues, February 1996
- Lectured at **Boston College Graduate School of Business**, Intellectual Property & Entrepreneurship, Entrepreneurship, April 1996, July 1999
- Lectured at **Emerson College**, Graduate School, Legal Issues on the Internet, Internet Publishing, December 1996
- Lectured at **Babson College**, Entrepreneurial Finance: Negotiations, February 1997; October, 1997, October 1998, March 1999
- Lectured at **Emerson College**, Management Information Systems: Cyberlaw, April 1997
- Lectured at **Harvard University**, Legal Aspects of Web Business, July, 1997
- Lectured at **University County Cork** (Ireland), Technology & Entrepreneurship, February, 1999
- Workshop panelist at **The Entrepreneurship Institute: The President's Forum of Boston:** How To Make the Intranet/Internet Pay Off (September 1997) and Year 2000 (October 1998)
- Panelist, **MIT Enterprise Forum JumpStart Clinic**, Protecting Intellectual Property – Startups, November 1997
- Panelist, **Massachusetts Continuing Legal Education Electronic Commerce '97 Conference:** UCC Article 2B: The Future of Information Contracts, December, 1997
- Panelist, **Massachusetts Software Council Legal Series: Electronic Commerce:** UCC Article 2B & Electronic Commerce, January 1998.
- Panelist, **KPMG/CITGroup Y2K Roundtable:** Practical Y2K Issues, April, 1998
- Panelist, **MIT Startup Clinic**, May 1998
- Panelist, **Risk & Technology Conference**, Electronic Commerce, May 1998
- Panelist, **Association of Commercial Finance Attorneys:** Year 2000 – Nightmare or Non-Event?, October 1998
- Panelist, **U.S. Naval War College:** Year 2000 Scenarios, December 1998

BINGHAM DANA LLP

Representative Technolgy Transactions

- Represented on-line travel provider in loan and private label internet transaction with Prodigy for the development of *Prodigy Vacations*
- Represent spin-off business unit in software and patent license and equity arrangements with Avid Technology
- Represented bank in negotiations with Computer Associates concerning scope of use dispute
- Represented consulting firm in systems integration work for various government and commercial customers
- Represented consulting firm in acquisition of hardware and software to fulfill systems integration contract work
- Represent Boston University in patent licenses and equity deals relating to the commercialization of federally funded research; developed standard form of omnibus patent license with equity
- Drafted RFPs and evaluated proposals for custom software development, systems integration, outsourcing and service bureau arrangements
- Represented bank in five-year check processing outsourcing arrangement
- Developed standard form of license for large corporate licensee use in all major software contracts
- Advised bank/licensee concerning scope of use exposure under 100+ software contracts, in light of bank's merger and acquisition strategy
- Represent on line magazine in advertising/sponsorship negotiations with Netscape, Novell and Oracle
- Represented consulting firm in large scale system specification and development project arrangements
- Prepared proposals in response to large scale consulting RFPs
- Represented on-line magazine in ownership dispute
- Advise large software licensees and publishers concerning Year 2000 issues
- Represent biotech companies in licensing transactions
- Represented large system customer (multiple locations) in system integration and hardware/software and infrastructure acquisition contract
- Represented software company/licensee in exclusive licensing arrangements with software developer
- Represent cellular service marketing company in marketing arrangements with MCI and Cellular One
- Represent MIT professor in patent licenses and consulting contracts
- General counsel to several software companies
- Represent large company (licensee) in custom software development and systems integration dispute
- Represent independent facilities/software maintenance and support company in licensing and maintenance deals
- Represent design engineering firm in all patent licensing and proprietary rights matters
- Represented strategic consulting firm in the acquisition of technology
- General counsel to intelligent agent software developer
- Represented neurochemical company in patent licensing, distribution and strategic alliances
- Represented manufacturer of recycled rubber powder employing proprietary processes in equity financing and acquisition of intellectual property rights
- General counsel to content provider, including broadcast, on-line and other licensing and distribution deals as well as corporate matters
- Represented on line consumer goods provider in ownership dispute and in licensing transactions
- Represent videoconferencing hardware/software company in OEM/Reseller deals with telcos and others
- Represented software company in settlement of intellectual property dispute in connection with unconsummated merger

BINGHAM DANA LLP

Representative Technolgy Transactions

- Represented creditors in disposition of patented technology
- Represented game inventor in distribution deal with Mattel Europa
- Represented hardware manufacturer in strategic alliance with software developer/publisher
- Represent parallel processing software company in license transactions with large customers
- Represent medical device manufacturer in licensing, cross-licensing, distribution and mask work arrangements
- Represented radio station in copyright dispute with Arbitron
- General counsel to public, surveillance system company in all manufacturing, distribution and hardware/software/mask works development transactions.
- General counsel to internet supplier of domain name surrogates.
- Represent bank in dispute with custom software developer.
- Represent content provider in copyright disputes.
- Represent various trademark owners in domain name disputes and other trademark infringement disputes
- Represent watermark (music encryption) developer in licensing transactions
- Represent "electronic ink" inventor in technology transfer arrangements with MIT
- Represent inventors of patentable intelligent caching internet software in technology transfer arrangements with Boston University
- General counsel to internet-based home delivery provider
- Represented start-up company in technology-for-warrants strategic alliance with Intel
- Represented bank in co-development deal with European software developer (internet-based commercial cash management software)
- Represent bank in outsourcing of trust processing services and technology
- Represent outsourcing contractor: accounts payable processing and technology
- Represent biotech company in custom software development arrangements
- Represent compression and image enhancement technology company in strategic alliance with chip manufacturers and scanner manufacturers
- Represent news publishers in web site matters, including on-line sweepstakes and chat room rules
- Represent bank in Y2K regulatory responses
- Represented Argentina bank branch in technology acquisition in Argentina and Spain
- Represented Irish manufacturer in enterprise resource planning project
- Represented records management company as software licensor to U.K. joint venture
- Represented consultant in utilities ERP services joint venture with French ERP provider
- Represented internet-based electronics exchange in Singapore joint venture

AUG 03 '99 15:13 FR BINGHAM DANA LLP 22A 617 951 8736 TO 912022254438 P.02

BINGHAM DANA

BINGHAM DANA LLP
150 FEDERAL STREET
BOSTON, MASSACHUSETTS 02110-1726
TEL: (617) 951-8000
FAX: (617) 951-8736

BOSTON, NEW YORK, WASHINGTON,
LOS ANGELES, HARTFORD AND LONDON

August 3, 1999

VIA TELECOPIER 202-225-4438

Mr. Joseph Sullivan
Science Committee
U.S. House of Representatives
Washington, DC

Dear Mr. Sullivan:

This letter confirms that I have not received any federal funds in connection with any Year 2000 inquiry.

Respectfully,

Wayne D. Bennett

/dp

BUSDOCS:765854.1

** TOTAL PAGE.02 **

Chairwoman MORELLA. Thank you very much, Mr. Bennett. I'm glad we, you know, ended with you because then you put another perspective on the concept of computer security being important, but not necessarily, I was going to say, increased because of Y2K. I understand also you were at the—what used to be called the National Bureau of Standards.

Mr. BENNETT. Yes, I was.

Chairwoman MORELLA. Which is now NIST, which has been very much involved with our computer security system and more legislation coming up on that.

As you could tell, we do have a vote coming up. Maybe I could start off by asking one question, and then we could recess for about 15 minutes, if you'll all be here, and then continue with questions. Unless you wanted to start off with a question, Chairman Horn?

Mr. HORN. I'll be glad to, if you'd like. I don't know if you want to go vote and then I can go vote and keep the show on the road. Whatever you'd like.

Chairwoman MORELLA. All right. He's got a great idea. I will go vote, and then he will keep this—keep it going, and then I'll come back.

Mr. HORN. Mr. Bennett, I was interested when you said the criminal laws seem to be in place. Is that true in every state? Have we done an analysis of that? Mrs. Morella and I can request the American Law Division to look at that now that you've raised the question.

Mr. BENNETT. Well, I think the federal laws are in place. In fact, there was just a recent article in, I believe, Computer World where a defense attorney based in San Francisco was complaining that the federal laws are set up so that her—this is not surprising—that her clients are having a tough time going and are pleading out instead of going to trial because they risk very severe criminal penalties. I do not know, however, on a state-by-state basis what the answer is.

Mr. HORN. Any comments from anyone else here on that point?

Well, the $1 billion does catch a headline, and that's, I think, more likely to be banks. What will happen with the non-banks where you could not have money to move, is blackmail. And the question would be: To what degree can we already cope with blackmail, the disgruntled employee that was mentioned? No question about it. You could—with a smart programmer, you could have chaos within a computer system.

Mr. MILLER. Mr. Chairman——

Mr. HORN. Mr. Miller.

Mr. MILLER. Mr. Chairman, we had Mr. Scott Charney, who heads the Criminal Division area of computer crimes speak at a conference we cosponsored last week with George Mason University. And Mr. Charney indicated in his public comments, at least—and maybe the Subcommittee would want to contact him directly, but I think I would agree with Mr. Bennett—that the federal laws are pretty strict.

The challenge is finding the miscreants and prosecuting them. But I think they feel that the laws are pretty strict, and they've been fairly successful in prosecutions. State laws, I don't have any information on them.

Mr. HORN. If it is blackmail and it isn't moving money around from accounts here to accounts abroad and so forth, how do we deal with the blackmail aspect?

Mr. MILLER. They're both federal statutes, as I understand it. I'm not a lawyer.

Mr. HORN. Have we had much computer security blackmail?

Mr. MILLER. I've been told of stories anecdotally. Nothing's been reported publicly.

Mr. HORN. Well, I realize it's like rare-book libraries. They don't want to talk about it, and that was the mistake of their life because now that they started talking about it, you find these people. And the thief just had a field day, can walk off with all the precious books, and they did it at Harvard and Yale and my own university and so forth. But it just seems to me we need a strategy here in educating chief executives. As we went through the Y2K bit in the last year, one of the things that discouraged me was the bad advice that their lawyers gave, which was, Chief, don't say anything, then they can't do something to you in court. Well, that's utter baloney because they'll do you for not doing anything, and we really needed CEOs to provide some leadership, which they finally woke up and did.

But how would you deal with this in this way to get top management to understand that they've got to do some strategies and tactics here to protect themselves in the interest of their stockholders?

Mr. PUCCIARELLI. Congressman Horn?

Mr. HORN. Yes?

Mr. PUCCIARELLI. If I could just say, in my opinion, security is to computers what safety was to automobiles in the 1960s. We have a relatively immature technology, relatively in the context of 20 and 30 years versus 100 years. And what goes with a new technology is a certain exuberance and a denial of some of those risks.

And I think what happens over time, the experience of using the technologies, of understanding the consequences, and understanding the implications will bring to light to the executives and to the leadership of the organizations that use these tools the risks. So rather than delegating the leadership and management of these systems to technical specialists, the executives will become more involved and more active in establishing security procedures for the overall enterprise.

Mr. HORN. Now, with the Presidential Directive—by the way, if you have your mikes still on, turn them off so we don't get a feedback

On the Presidential Directive, how active has the security community and the information technology community been helpful in that? And where are we in the progress under the Presidential Directive?

Mr. MILLER. I think there's some good news and there's some bad news there. I think the good news is that the various government agencies are trying to come up with a plan. We saw a leaked version of it in the New York Times very recently, an article by Mr. Markoff which focused on just the privacy issue. But there has been extensive consultation, and I do commend the people in the government for trying to get as much industry input as possible into the process.

As an example of bad news, though, Mr. Chairman, I'll give you one specific example. We were designed by the Department of Commerce, as I mentioned in my testimony, as the sector coordinator for the information technology sector along with the Telecommunications Industry Association and the U.S. Telephone Association. That office within the U.S. Department of Commerce is probably going to be defunded in the year 2000. So, on the one hand, we are trying to undertake activities in conjunction with the Department of Commerce agency. On the other hand, the Department of Commerce, even though they did request some money, apparently it's not a very high priority. Congress hasn't seen it as a high priority. So we're going to—may find ourselves on October 1st being designated by the sector coordinator of an office that no longer exists.

Mr. HORN. Well, we thank you for alerting us because we ought to keep on top of that.

I'm going to have to declare a recess now so I don't miss a vote. So we're in recess until Mrs. Morella returns to chair the meeting. Thank you very much.

[Recess.]

Chairwoman MORELLA. Thank you, gentlemen and others, for bearing with us as we had two votes instead of one vote. And matter of fact, one was on——

Mr. HORN. Patent policy.

Chairwoman MORELLA. Yeah, patent policy, which might interest some of you.

Ms. Rivers is here from Michigan, and I guess I'll start off with a question or two and then let Ms. Rivers ask any questions.

Mention was made—I think you, Mr. Miller, mentioned the Presidential decision, Directive 63, which was issued in May of 1998, and that explains the Administration's policy on critical infrastructure protection. Incidentally, we had the first House hearing on the critical infrastructures report. The infrastructures include telecommunications, banking and finance, and all the essential government services. The directive requires immediate Federal Government action, including risk assessment and planning to reduce exposure to attack.

Maybe I'd start off with you, Mr. Miller, in responding to this, but I want to hear from the others, too. In your opinion, has the implementation of this directive been effective? And why or why not? Does more need to be done?

Mr. MILLER. The process has been a little slower than I think many of us anticipated, but maybe that's all for the good. The trial CIAO office, which everyone sort of chuckles at, but the Critical Information Assurance Office, which has coordinated the development of the longer-term plan, has been somewhat slow, but they have to engage numerous federal agencies. They have done a good job, Madam Chair, I believe, of trying to engage industry and academia in getting input in the development of that plan. So I think they are moving forward in a reasonable pace to come up with a plan.

It's very tricky, though, because the exact lines of responsibility between the private sector and government—there may be differing views, as I suggested in my testimony. The private sector may be-

lieve that the government needs to be less involved, and some people in government want to be more involved.

The point I mentioned to Chairman Horn while you were away was some of the things that disturb us, for example, is the government, to industry, is not necessarily someone we like to work with all the time. I have a little bit of concern about it. One of the departments, however, I think industry is most comfortable with is the Department of Commerce. The Department of Commerce in the National Telecommunications Information Agency, headed by Assistant Secretary Irving, has responsibility for this critical information issue, and we were designated, along with two other associations, as a sector coordinator for the IT industry.

But now it looks like they are going to have no money for FY 2000. There was a request for a small amount of money, I believe $3.5 million, for FY 2000, but, candidly, I don't think it's very high on the Administration's priority list. And from what I understand, with all the pressures that you all have to cut domestic spending, that money may disappear.

So that's an example of where we thought there were good plans in place to try to move forward, and we were excited about the opportunity to be the sector coordinator for the IT industry. But if that agency funding goes away and there's nothing in Commerce for us to work with, then in some sense industry's role is back to square one. At least my sector's role is back to square one.

Chairwoman MORELLA. Would any of the other panelists like to comment on that? I'm going to ask a question also that you might want to respond to at the same time. Do you think we need a computer security czar? I don't mean to overuse that term, but somebody in the Federal Government such as the role that John Koskinen has played with Y2K that will be an oversee also of critical infrastructures, computer security. Mr. Pucciarelli?

Mr. PUCCIARELLI. Congresswoman, first a quick comment on the Presidential Policy Directive 63. In general, the entire area of cyber warfare and security is moving extremely quickly. It's very difficult to design a solution, just from an engineering perspective to design a solution to address a threat, and to do it and get it implemented in a timely fashion.

If you look at the typical procurement cycle right now, from the time an engineering solution is designed until it's presented, run through for hearings, funded and implemented, it could take 2 years. The problem is, is that it's difficult to anticipate—it's virtually impossible to anticipate 2 years ahead of the threat what needs to be done because this area is moving so quickly.

So just one comment on that is just I would counsel you to look at the time lines to actually acknowledge the threat, design a solution, and implement it.

As far as your question on the computer security czar, I think there's a plus and a minus. My own personal perspective and the perspective of the GartnerGroup is that security is an enterprise issue. It is not an issue that belongs dedicated to somebody who sits in the back room of the organization or off to the side in an ancillary role. So I think there's a risk with setting up a czar in that it might be viewed as something that is the domain of the technical specialists.

I think the challenge is how do we elevate security to an executive issue and an executive priority, and if a computer security czar was able to portray the issue with that type of presentation, I think there's an opportunity to have a very positive impact.

Chairwoman MORELLA. Mr. Rich.

Mr. RICH. I support his statement. I think having a computer security czar would probably be not a good idea, that security is part of an infrastructure, an enterprise implementation, and that we need to support the current infrastructure assurance directives that have been put out there.

Chairwoman MORELLA. Mr. Bennett, would you like to comment on——

Mr. BENNETT. I think that anything that's done has to draw some very clear lines between government and corporate enterprises. I think that the prospect of a czar might actually frighten some corporations who may have some operations that are even part of what you might consider infrastructure. I mean, I think that there are a lot of large corporations out there that would be happy to just have government approve their international use of very strong encryption methods and then stay out of the picture as far as their own security is concerned until such time as there is—where their own security procedures fail, and then they'll want the help of law enforcement officials to try to track down whoever did it.

Their biggest issues right now do not involve a billion-dollar fraud. If they look past Y2K and they're talking about people taking things from them, they're worried about competitive intelligence.

Chairwoman MORELLA. Would either of you like to comment on Directive 63?

Mr. RICH. I haven't been myself involved a great amount with the directive. From what I've observed and talking with others, I support Mr. Miller's comment on that it's moving maybe not as fast as some would expect, but I think it's moving in the right direction. And I've seen a lot of corporations now starting to talk to the government. I like the idea of collaboration and trust. Unless we can get the point across to the commercial organizations that the government can help and not mandate or dictate and more or less work together, I think we'll get longer—further down the path.

Chairwoman MORELLA. I didn't mean to be rigid when I said computer security czar. I guess I'm thinking to implementation of current policies in terms of coordinating. There is no doubt in my mind we lack that in the Federal Government, but we can get into that in some other questioning.

I would like to now recognize Ms. Rivers.

Ms. RIVERS. Thank you, Madam Chair.

Mr. Miller, I have a question regarding funding you raised in your written commentary, and I apologize that I wasn't here for the testimony. But in your written statement, you raised concerns that the $3.5 million that is now being allocated for CIIAP is inadequate in your view or barely adequate. Are you aware that the Commerce, Justice, State bill, appropriations bill that we're going to vote on this afternoon, zeroes out that program? And what will the effects be of that decision?

Mr. MILLER. I heard—I haven't actually seen the language of the legislation, Congresswoman Rivers, but I heard that they were going to zero it out. I think that would be most unfortunate from the perspective of private industry.

Clearly, the issue of information security has spread throughout the government—the Department of Defense, the Department of Justice, National Security Agency, et cetera, et cetera. And, by the way, in response to Congresswoman Morella's question, I would support a czar for exactly that reason.

But, clearly, the government is perceived by many people in industry as kind of threatening, particularly if you're talking to national security people or law enforcement people. To the extent the industry is comfortable, I think they're most comfortable talking to the Department of Commerce, and so that's a logical place for business to communicate. And zeroing out that budget item from within NTIA I think would be most unfortunate. Even a relatively small amount, $3.5 million, is better than nothing, and I think the problem is—I've spoken to Assistant Secretary Irving about this—is he's already had severe budget cuts over the last 2 or 3 years, and if this money gets cuts down, he can't find it to take out of hide somewhere else. So I'd hope that the Congress would take another look at that, and whether $3.5 million is exactly the right number or not, I don't know. But I hope the Congress would take another look at that and put some funding in there because that would make industry much more comfortable in terms of working with government.

Again, there's no disrespect to the FBI or the Defense Department, but if we have to talk to somebody, it's a lot easier to talk to the Commerce Department.

Ms. RIVERS. Thank you.

Mr. Pucciarelli, I have a question for you. In your comments, you talk about a 70 percent probability that there would be at least one electronic theft of a billion dollars, which—I may not have it right, but that would seem to be the biggest theft in our history. I mean, I don't think we've ever had a billion dollar theft. And you use the terminology that really reflects sort of the science of statistics.

How did you arrive at that?

Mr. PUCCIARELLI. What we do, Congresswoman, is, as part of our recommendations at GartnerGroup, we have a practice of assigning a probability to a particular prediction. And the reason that we assign probabilities is so that our clients have an ability to take these predictions and appropriately factor them into their business plans. The probabilities were not scientifically derived. They were arrived—derived based on judgment, and there is an explanation of the probability process in my formal written testimony which has been submitted to the Committee.

Ms. RIVERS. How do you translate a probability—or a judgment into a 0.7 likelihood?

Mr. PUCCIARELLI. A 0.7 likelihood, in terms of how we explain that to our clients and advise that to our clients, is we would say that you should assume that this is likely to happen. If you—if it had a 0.8 probability as an example, we would say assume it will happen. So with a 0.7 probability there is still some risk that it

won't happen. The range of probabilities that we publish goes from 0.6 to 0.9.

The whole notion and the whole purpose of this piece of research was to advise our clients to escalate their risk management practices. And in the context of that, what we are really saying with the probabilities is that we believe it's likely that there will be at least one large outrageous theft.

Ms. RIVERS. So what you're saying is it's really not a scientific tool, it's a sales tool?

Mr. PUCCIARELLI. No. That's—not at all, Congressman. What my point was, it's not a sales tool at all. What it is is it's a way for management within our client organizations to appropriately weigh the probability.

Ms. RIVERS. That's what I'm trying to understand, given my training, is how you are creating your probabilities, what you are actually using that can be replicated by someone else. Looking at the same data, can they come up with the same conclusion?

Mr. PUCCIARELLI. The way that we actually create the probabilities is based on—first of all, it is not data. It is—it is qualitative interactions with our clients and qualitative assessments of what's going on in the environment. The intention of the probabilities is to factor them into the management process within our clients. So the idea is that we can give our clients a degree of confidence as to how sure we are that this will happen.

Ms. RIVERS. What are the elements that you weigh in coming to this conclusion?

Mr. PUCCIARELLI. We look at three different major aspects in forming a probability. First we do primary research, which is to look at the specific area. And as I testified earlier, we did that based on direct examination and in conversations with our clients, what was going on in terms of the process itself. We then review preliminary findings with our clients and ask their opinions and their assessments of our recommendations. Then the third and most important thing is, before we publish a recommendation and assign a probability, we—as a community of analysts, GartnerGroup has over 700 analysts review the major policy statements, and as a community of analysts, we have to agree on what those probabilities are, and we have to agree what the major statements are.

So this forecast represents a consensus position of literally hundreds of people within our organization to support—and it has to agree with their qualitative and quantitative observations as well.

Ms. RIVERS. Okay. Thank you.

Thank you, Madam Chair.

Chairwoman MORELLA. Thank you, Ms. Rivers.

Chairman Horn.

Mr. HORN. I've had 5 minutes, so let everybody else go, and then I'll have one question.

Chairwoman MORELLA. Mr. Turner from Texas.

Mr. TURNER. I will yield to Mr. Horn.

Chairwoman MORELLA. Chairman Horn? I mean, I'll ask a question.

Mr. HORN. Let me just ask one question. I've appreciated the various papers you four gentlemen have submitted.

You've suggested, Mr. Miller, that we grade federal agencies on computer security, much like we currently do for the year 2000 work. And I'm just curious, What categories of criteria in relation to this subject would you suggest and use?

Mr. MILLER. I think, Mr. Chairman, your grading system the last 3½ years or so for the government's reliability and readiness for Y2K has been a tremendous tool toward driving them toward the successes that you mentioned in your statement earlier today, and you deserve a great deal of credit, as does Congresswoman Morella, for focusing attention.

A similar system, I believe, could be developed. I'm not prepared to give you the exact criteria, but things like the percentage of spending on IT devoted to computer security, the attention paid by senior management to computer security; reports of intrusions and detections of intrusions could be another metric that you could look to. So I think you could get—probably put together a fairly straightforward and easily agreed upon list of indicia that you could use to use your excellent grading system, and I think that would help drive the agencies toward more attention to this problem.

Mr. HORN. Where do—where are the data on intrusions kept? Is it simply by agency? Does OMB have any information that they've collected over the years?

Mr. MILLER. There are two sets of data. There are data from the private sector, which are reported to what's called CERT, the Computer Emergency Response Team, at Carnegie Mellon University. They're, of course, voluntary reports. And to go back to Congresswoman Rivers' question about hard data versus theoretical data, I do note that the number of incidents reported to CERT has increased dramatically over the last few years.

Within the government, my understanding is that they don't necessarily share information among agencies, and that's one of the issues being looked upon—looked at within the PDD–63, is to exactly how do you make sure that all the information is being shared appropriately among the agencies.

Mr. HORN. Are the Carnegie information—are those data accessible?

Mr. MILLER. In some cases, the specifics are accessible, and sometimes it's just the generic numbers. I think one of the biggest challenges that this issues faces, as Mr. Pucciarelli was suggesting in his earlier comments, is how much willingness is there among companies as they mature to share information. Certain industries such as the financial services industry have already been exposed. Citibank had a relatively large potential theft several years ago, and so Citibank is now wanting to talk about this publicly. You can get them to go to any conference, any open meeting, and they'll come and talk about it. But if you ask 99 percent of all financial institutions or other types of organizations, "Do you want to admit times that you've had intrusions or thefts or breakdowns?" most of them are going to be totally silent, totally mum.

So one of the challenges we've had as an industry, Mr. Chairman, is figuring out how to get companies to share information in a way that will help everyone fight off other potential intrusions and threats, but at the same time not be concerned that propri-

etary information will leak out or that their competitors will get an advantage or it will leak to the press and hit the stock price, et cetera. So companies are always trying to balance these two things off. It's not just the legal issue which you raised before in regard to the Y2K. It's a whole set of potential down sides to exposing information as opposed to the one up side, which is to sort of be a good citizen and by reporting the information about an intrusion that you had, you may save somebody else or you may help to protect the entire economy. And we are not yet at a position, I think, where the leadership of business in this country has made that balance of that equation and said in all cases we will share information. And one of the reasons is that they're not sure about sharing information.

Let me just bring one more specific problem to your attention, is the Shelby amendment. I think industry supports the Shelby amendment generally. We believe that federally funded research results should be available to the public. And what Senator Shelby has done is good. But my companies have come to me and said, Now, what if we share information and there's some kind of federal grant involved with the organization that has that information and we believe it's confidential and then a FOIA request comes in? Government FOIA exemptions can't be used because it's a private sector organization. Then what do we do?

So I think that's not—it's an unintended consequence of the Shelby amendment which is something we're trying to puzzle through right now.

Mr. HORN. Yeah, well, as you know, we're going to struggle through on that, and you have to protect the people that, let's say, are trying to win the Nobel Prize or something. We shouldn't have their data all around and polluted. That will get tested soon enough. And we don't want to discourage science. On the other hand, we don't want to—in this situation, we're talking about, we don't want to have sitting-duck targets because they say, boy, look at all the entries there, let's see if we can do it. And I suspect that's worrying some. The Good Samaritan law has helped on the year 2000 a bit, and industry plants have been working with each other, from the best we can understand on that. I don't know if that's your feeling or not. There's much sharing of information.

Mr. MILLER. Definitely. But it took legal action to do it. But, again, if Long Beach State, your former institution, set up a classified center and encouraged companies to provide information and they got Federal funding somehow, what does the Shelby amendment do to that data? It supposed to be sanitized. It's supposed to be protected within this research center within the university. But can someone use—I don't know, but the questions have been asked. Can someone use the Shelby amendment to come in and say I want access to all that data? And suddenly the whole confidentiality system breaks down, the trust breaks down, and no one supplies information to the Long Beach State center. We've lost the whole purpose of the organization in the first place.

Mr. HORN. Are there any questions and thoughts that none of you have mentioned that you now would like to make? This is at least my wrap-up question. Mrs. Morella might have many more. But just what are we missing that we haven't really focused in on?

Mr. RICH. Mr. Chairman, I'd like to make a quick comment there. In the spirit of PDD–63, rather than requiring—or asking people to give you their particular data on break-ins, if we take a baby step and say how about sharing threat information-these are people that are trying to touch you and look at your networks but not successful in getting in—that would be a first step in establishing the trust relationship.

Mr. HORN. That's a good suggestion.

Chairwoman MORELLA. Thank you, Chairman Horn. That's great.

This is so reminiscent of Y2K when we talk about failure to and concern about sharing information and the coordination that is necessary. And, of course, we're talking about computer security that is troubled particularly because of Y2K compliance.

With regard to the Shelby amendment, it's interesting that here we are in the room where the ranking member, George Brown, is the one who's introduced the legislation to get rid of the Shelby amendment, and, of course, I've heard from National Institutes of Health and a number of other institutions like that that are hoping that—Mr. Miller, that you can—we can work out some kind of a compromise.

I—in terms of where information may come from, I can remember years ago, GAO, you know, when they came out with their list of high-risk areas, they had Y2K there, and they've had computer security there for some time. That maybe another source of information to have GAO do further reporting. And, of course, they've done a number of reports on problems with computer security, particularly in DOD. And I wonder, the inspector generals, would they not also be looking at this, or should we be telling them to begin to look at this? I don't know if any of you are cognizant.

Mr. Pucciarelli.

Mr. PUCCIARELLI. Congresswoman, I think that the whole issue of computer security could clearly fall into the domain of the inspector generals, and I think that depending on which agency is looked at, I think you'll see different degrees of activity in the area. I think that there's clearly an opportunity to raise the issue on the agenda of the IGs, and, again, I'll come back to my point earlier. The real challenge is how do we get the leadership of the organizations involved as well.

Yes, the IG is the means by which to do it, but the challenge is how do we get it to the executives.

Chairwoman MORELLA. And you mentioned—Mr. Miller, you wanted to comment.

Mr. MILLER. I agree exactly with what Mr. Pucciarelli is saying. That's why I endorse your idea of the czar, as long as the czar is conceptualized the way Mr. Koskinen has conceptualized the role, not that the czar——

Chairwoman MORELLA. Right.

Mr. MILLER [continuing]. Is to fix everything himself or, if it's a czarina, herself; but that, number one, that person has the authority to go directly to Cabinet officers and make sure that the Cabinet officers personally are paying attention to the issue; that that person has the ability to work with the private sector by organizing them by sectors, as Mr. Koskinen has done very effectively. He's

not trying to fix the problems with the electricity industry or the retail industry, but he's working with the appropriate private sector groups to do that.

Also, he or she would be able to coordinate among the different agencies, and, frankly, it's a little confusing to the private sector to know whether we should talk to people at the CIAO or Mr. Hamre at DOD or people at the NIPC or people at Commerce. It would be a little bit easier to, if there were someone who had a central role and also had access directly to the President and Vice President, as I believe Mr. Koskinen does on Y2K issues.

Chairwoman MORELLA. And looking at the private sector, Mr. Pucciarelli, you mentioned in your statement that many firms have not taken—you used the term "adequate steps"—to secure and audit the year 2000 remediation process. I wonder, what do you mean by adequate steps?

Mr. PUCCIARELLI. Congresswoman, in forming this scenario that I identified, one of somebody stealing a large amount of money, I started from the premise that somebody would do it. And then I posed the question back to my clients and said how likely is this to happen. And the response back from the practitioners in the field was that, in general, the level of security in their opinion was not very high. And that was one of the reasons why I went forward with this research and deemed it appropriate to recommend to the executive leadership of the various organizations to take as a given that this is a likely event and to implement risk management activities, which was really the underpinning of what my research was.

It basically said you as leaders of these organizations need to implement risk management because the details—the people that are actually doing it, the practitioners, believe that there is a relatively high risk.

Chairwoman MORELLA. Is implementing an independent verification validation process going to mitigate the problems and the trap doors?

Mr. PUCCIARELLI. To implement a comprehensive security program, we have to cover three specific areas. We have to cover people, process, and products. And when talk about people, a metaphor might be to look at the bar exam. If we were to look at process, it might be the equivalent of the FDA certifying a surgical procedure, or a process might be the certification of a particular software development process. And a product might be the equivalent of the regulation that DOT has for automobiles to meet safety standards or, in the public domain, the UL underwriting seal of approval.

To get true security, we're going to have to approach it from all three fronts.

Chairwoman MORELLA. I'm glad you wanted to respond, Mr. Bennett, because I really felt I had to give you an opportunity to engage since your point is that it's not Y2K that is the big problem with computer security. So, sir?

Mr. BENNETT. Well, I think I stated my point on the relationship. I think they're both very important issues. I just don't see them—the statistical inference there. But with respect to the independent audit and the IG's role, it seems to me that the independence of both an IG or an outside auditor is one piece and the only piece

that should be independent of line management. While auditing on the one hand has to be independent, someone has to come in and say how good a job you're doing, there are a couple of stages that have to come before that, and those, if you're ever going to make this work, it seems to me, have to be done by line management because they have to believe in what they're doing.

Now, in defense, there may be a different weighing that takes place. How much—there's a certain drag on productivity that's going to happen when you implement extra security procedures. You try to minimize it, but it happens. That—where—how much of a drag on productivity you're willing to tolerate may be different if I'm trying to keep secret the Nation's defense secrets. At the same time, if I'm a corporation and I am trying to keep competitive information out of my competitor's hands, which is very important, there's a different drag on my productivity that I might accept.

So line management, first of all, has to decide how important is it and to what level are we going to protect it or try to protect it. And then there has to be an implementation process, all of which should stay within line management. And only then, after you've done those two steps, it seems to me, without sort of alienating line management, who you need to do those two steps, then there's a role for an outsider to come in and say, okay, how good a job are you doing?

Chairwoman MORELLA. Prioritize, organize, then verify.

Mr. RICH. I'd like to recommend that we take a look, as was mentioned here earlier about process, that over a period of time in my time working in the government we had process, accreditation for systems for security. And over a period of time, the accreditation process failed to work because it wasn't updated, that we would do the checklists and everything was great. I think as the IG goes through the process of checking, somebody should be checking the IG. Maybe that's the computer security czar that you mentioned, as an oversight position, that we have to keep up with the technology that we're looking at as we go through that.

Chairwoman MORELLA. Thank you.

Mr. Turner.

Mr. TURNER. I was really interested in knowing what suggestions any of you might have regarding how we might strengthen law enforcement in this area. It seems that it's an area that we're really very ill equipped to deal with. We don't have the expertise in local district attorney's offices. I'm not even sure we have it in the Department of Justice.

But I think we really—there seems to be a need to take a good look at the existing criminal laws. Obviously, some of the laws fit. Theft is theft, I guess, no matter how you accomplish it. But in any of the intrusions that don't result in outright theft of dollars, I'm just not sure that the penalties are out there, the laws are out there to really effectively deal with this, nor is there the expertise available to fully prosecute what appears to me, from listening to your testimony, to be a growing area of criminal activity.

Am I correct on that? And do any of you have any suggestions you might——

Mr. MILLER. I think that's a very important point, Mr. Turner. We're working very close with the Justice Department Criminal Di-

vision on this, and they have asked, for example, to help us help them put together a list of experts, cyber experts, that they can call upon for—when they need to do prosecutions so that the Assistant U.S. Attorneys around the country, when they're referred these cases, frequently do not have the kind of expertise that they may have in securities fraud or other kinds of more traditional non-digital fraud. And so we are working with Mr. Scott Charney and Attorney General Reno to help put together a list of those experts that the Assistant U.S. Attorneys can call upon.

Also, I have been told that the Justice Department is doing training for state and local officials on cyber crime, detection, investigation, prosecution. But how extensive that is, I don't really know. You can contact the Justice Department. I don't have any data on how many—how many training sessions have been done.

I understand that when they do offer them, they are heavily subscribed, that there's clearly a lot of interest among law—local law enforcement officials to get this kind of training. But how extensive the training is currently, I don't know.

Mr. BENNETT. Congressman?

Mr. TURNER. Yes?

Mr. BENNETT. I believe you have the laws. You have got your Computer Fraud and Abuse Act. You have the Espionage Act, which covers trade secrets, and both of those have attempt parts to them.

You also have a fair amount of expertise. It is growing within the Department of Justice, but there's a fair amount of expertise. When we call up on behalf of our clients and there's been a problem, we do not get a befuddled person who has either no interest or expertise in the area. We're generally directed to somebody who does that for a living.

I think the only problem we're running into is the usual, and that is, you've got to have enough time and so you've got to allocate scarce resources even in the Department of Justice. And the way they've allocated it, to use one example, one of my clients called up, and someone had scanned their ports looking for a way in, and they were very concerned that some—a specific competitor, in fact, might have been the one doing it. And they wanted to get to the bottom of it. And when we called up, it seemed to us that there was a bright line from the United States Attorney's Office, and that was, really, if you can show us that they got in, then that's going to put it into one basket over here and we're going to have the time to be able to address it. If, on the other hand, you don't know because your firewall software maybe only tracks unauthorized attempts and maybe perhaps doesn't track authorized entries that might have been fraudulent, then we're—maybe you ought to go the civil route and try to discover this by suing the ISP and getting the name and then going after them and finding out who it is on your own.

And, clearly, you don't want to go down both those paths, and we could really understand it. We ended up going down in this last instance, which was only a few months ago, going down the civil route and finding out that it was some teenage hackers attempting to get into a corporate—past a corporate a firewall. But the laws are certainly there. The expertise is there and growing, at least at

the Federal level, and now it's just a matter of putting in a priority because I think they have enough to do with the actual break-ins at this point.

Mr. MILLER. Mr. Turner, my staff reminds me that Senator Leahy has introduced a bill to provide $25 million a year to the Department of Justice for state and local cyber crime training. So obviously Senator Leahy at least believes there's not currently sufficient funds and is trying to increase that.

Mr. TURNER. Thank you, Mrs. Morella.

Chairwoman MORELLA. Thank you, Mr. Turner.

It seems to me there could be a problem with companies overseas and the kind of security because they haven't had a check to do—an opportunity to do background checks of—and this made by the more prone to computer security problems with Y2K. Would any of you like to comment on that, maybe what we could do about it? You look ready, Mr. Bennett, then Mr. Miller.

Mr. BENNETT. I believe this problem's been with us for a while, and to try to put it in perspective, if you got three different levels of folks you might engage—and they've been engaged over the course of time, at least in corporate America, to work on IT systems there, your own employees, your domestic contractors, and then foreign contractors, and I would suggest that at this moment in most states in the United States you can learn not very much about your own new employees for starters. So, yes, it is true that there could be foreigners or contractors who could pose a definite threat to your IT.

But right now, in the position of any ordinary employer—not the government but an ordinary employer, we're just not permitted to get the kind of information you can get, and so I have a live threat right with my employees.

A second quick point is that—put aside just for a moment—I know it's not the scope here, but to try to put this in perspective, you've got the threat to your IT systems, and yet in many, many companies today, the most valuable information that they have walks out the door every single day with their employees. It is not sitting on their computer system.

So when they put this whole thing into perspective for, you know, the billion dollar fraud over here and then the foreign threat and then even the domestic contractor threat, then the employee threat, what they're really worried about is: How can I find out information about the people who are here? And, moreover, where are they going to go? In the State of California, for example, companies cannot use non-competes for some good and wholesome reasons. And so that means that my employee can leave today, go down the street to my competitor, and use that information.

Mr. HORN. I missed the word there. Companies cannot use what?

Mr. BENNETT. They cannot use—in California, as an example, one cannot include a non-competition clause in a contract with an employee to say, look, for 6 months after you leave here please don't go down the street—or you may not go down the street to our competitor to do the same kind of thing.

Mr. HORN. As you were talking, I was thinking, the whole evolution of Silicon Valley is when somebody walked out and started their own firm. American productivity.

Mr. BENNETT. Absolutely correct. And now—and we've gotten a lot of great things from that. In addition, we've gotten ourselves a rash of trade secret lawsuits.

Chairwoman MORELLA. It seems to me—you know how we have the metal detectors going into buildings such as ours? What we really need is a mental detector, and a mental detector would probably take care of a lot of that problem that you mentioned.

Mr. BENNETT. God forbid.

Chairwoman MORELLA. Okay. Right.

Mr. Miller.

Mr. MILLER. Two brief points. One is that there's currently, in addition to the overall challenge of the shortage of information technology workers in our country, there's a specific subset of that. There's a huge shortage of people with sophisticated security training or the ability to carry out these jobs. Going back to Mr. Pucciarelli's earlier point about people being one of the critical three elements, it's very important. I know a very large, sophisticated firm which is doing a lot of work on a contract basis for the government has 1,500 positions to fill, and they have 1,000 people, and they can't find the other 500 because, first of all, you can't use foreign workers 99.9 percent of the time so you can't fall back on H(1)(b)s or anything like that. You can't even fall back on permanent residents. Most of the time they have to be U.S. citizens. They have to have security clearance. They have to have sophisticated training, et cetera, et cetera.

So that's a big job. I know Attorney General Reno and other people are trying to focus on some kind of a cyber corps idea where there'd actually be government incentives, scholarships or a sort to encourage people to get the kind of sophisticated training that they could become specialists in information security. So I think that's an issue.

Also, on the international front, Chairwoman Morella, I know that this is a huge issue in terms of laws. How do you enforce the security laws? And right now the U.S. Government is engaged in discussions with the G–8. Attorney General Reno I know is discussing with other members of the G–8, but it gets to be a huge issue in cyberspace. Let's talk about things like child pornography and getting access. What laws do you use? Do you let Muammar Qadhafi start issuing subpoenas for information that it wants to get from AOL because it believes somebody in Libya who's an AOL customer is violating the laws of Libya? How do you enforce those kind of laws? So there's some incredibly open-ended questions out there right now in terms of our cyber crimes on the international front which are just at the earliest, earliest stages of discussion right now.

Chairwoman MORELLA. Mr. Rich.

Mr. RICH. Yes. I'd like to mention a couple of months ago I went to a national infrastructure protection conference out in Denver, and I support the idea of Mr. Miller mentioning the cyber corps approach. I think that would go a long way, similar to the Peace Corps, in incentivizing those to bring up the awareness within the security area. And then they have a little payback to the government for helping them through school, or similar.

Mr. HORN. If I might be yielded to for a question, I probably haven't unloaded on you my feelings on when that visa deal comes up. I was outraged by it. Why am I outraged by it? Very simply, we've got a community college system—certainly in California where it was founded, there's 107 campuses in California and we've got a Silicon Valley and San Diego, Orange County, and Santa Clara County, and popping up hopefully in other counties. And they need to work together, and we should not be importing people. We should be training our own people.

When I think of the classrooms I go to where students are now exposed to computing, and it seems to me we're derelict both in education in California—and I've unloaded on many of the community college presidents and said, Where are you on this? And where are the CEOs in Silicon Valley that ought to be sitting down with them saying this is the kind of curriculum we need if they're going to be helpful to us? That was the whole purpose of the community college, was both vocational and academic. And you need both to be a good programmer.

And I would hope that they would be working together so they could get the trained force. These are $60,000 jobs, and there are a lot of bright kids. Escalante showed that in the Los Angeles schools, you can teach young people to be as good as anybody, as good as they are at Harvard. And these students proved they could do it. And that's what we ought to be doing, but we need the equipment, which is—the state is always behind, every state in the Nation is behind when it comes to giving and granting and providing computer equipment. And if you're going to work on new generations, this is where Silicon Valley can take a tax writeoff, or wherever, and get something out of it.

But your associations, it seems to me, would be very helpful to be where you get these people together, both the community college president and the CEO of a computer firm. We shouldn't have to be importing people from all over the world, and we shouldn't have to need a government program. I mean, the best education deal in America are the community colleges. There's very little tuition. At least in California it is; in Texas it is. So why aren't we taking advantage of that? Are we still going to just keep importing thousands of people? They're all wonderful people, but what about our own people? That's where I'm coming from.

Mr. MILLER. Did you want a comment, or is that just an observation?

Mr. HORN. Well, I'm just saying—I'd like a comment, and I think—you know, where is that industry and where are those educators to be linked up to get the job done?

Mr. MILLER. Well, I do disagree with you on the immigration question, but I don't disagree with you on your fundamental point, Mr. Chairman. Our educational system is still an educational system designed for the industrial age, not the information age. And we are trying to work with community colleges. In fact, I recently met with the President of the American Association of Community Colleges to discuss potential collaborative activities. We're also working with particular outreach to minority communities. I think as you know, in the—even though—for example, African Americans are 11 or 12 percent of the overall U.S. workforce; they're only

about 5 or 6 percent of the IT workforce. So we're involved in some initiatives in that area, also.

The challenge is to do both at the same time, though. It does take time for people to be trained and educated, and we have to incentivise them to come in. And I think that's why I was suggesting that government, cyber corps or IT tax credit training such as the legislation that Senator Conrad and Congressman Moran have introduced to try to create incentives.

I do believe, Mr. Chairman, that community colleges are much more responsive than universities are in terms of adjusting their curriculum. And you have several in California which have done—moved relatively quickly. But it's—I think the late Governor of Florida once said, the only thing harder to move than a cemetery was the university faculty. So I think they find that trying to change, getting rid of Russian history and political science department for computer science departments isn't always easy; whereas, at community colleges they can move quite quickly. And certainly you see places like Contra Costa Community College. The one that's usually thrown up as the best example is Maricopa Community College in the Phoenix area where they work very closely with Motorola, Intel, and other semiconductor manufacturing firms for training.

So I think we're getting there, Mr. Chairman. It's just slower than we'd like.

Mr. HORN. Well, that's where you have to take these massive systems because most of that is done at the local college, and that's why I suggested the community college. There's more flexibility for the reasons we all know than in the major research universities around.

But if you're doing it, I think that's wonderful. We don't need a government program to do it. We just need you guys on the phone, and gals, to work it out.

Chairwoman MORELLA. I think we also need the partnerships of academia and the business sector and even government, you know, state government, maybe Federal Government in some way, also being kind of part of that partnership. But we have, Chairman Horn and I and Ranking Member Turner, been aware of the personnel needs throughout this whole thing, Y2K, now computer security, and we're trying to do something even legislatively on that, too, to increase fellowships and, as you mentioned, the cyber corps. We'll continue to work on that with your help.

Just a wrap-up, if there are any comments from any one of you, real briefly, in terms of what we should be doing now since we have only that 149 days left to the end of—until we reach 2000, recognizing whether Y2K has been remediated or not with regard to computer security. Any final comments for us?

Mr. MILLER. My only concern is—and I don't think this is Mr. Pucciarelli's intention in releasing his report—is that people don't move more slowly on Y2K because they're concerned about information security. He's correct that information security has to be part of your Y2K, but I hope no one who reads that article uses that as an excuse not to do their Y2K remediation. I certainly know that wasn't his intent. I know that Gartner has been one of the strongest advocates for Y2K remediation. But one could imagine a

situation where someone would misinterpret that message instead of the message being to be more conscious of security and say, well, that's one more excuse not to get my Y2K solution done. So I hope this hearing will help to send the message that that is not the intention. I assume Mr. Pucciarelli would agree.

Chairwoman MORELLA. Thank you.

Mr. PUCCIARELLI. Yes, Mr. Miller. I appreciate your comments.

Congresswoman, one final thought that I have is that simply reminding folks, reminding organizations, enterprises, and the leaderships of those organizations of the need to redouble their efforts and maintain the appropriate risk management criteria while they complete their Y2K remediation activities. And I think that even having this hearing on this matter has served a very important purpose to that end. I think that encouraging the various federal agencies and departments along the same lines would also be of benefit.

Again, clearly our intention was not to suggest that you should—that organizations should go slower, but to merely point out that risk management activities have a role as well.

Chairwoman MORELLA. Thank you.

Mr. Rich, a final comment?

Mr. RICH. Yes, ma'am. I'd like to basically agree here with both of the gentlemen here in that people shouldn't slow down, they should pick it up a little bit and keep vigilant as we go toward the year 2000. And I hope these hearings will allow people to look at other aspects rather than just focus on Y2K remediation.

Chairwoman MORELLA. Good point.

Mr. Bennett.

Mr. BENNETT. I believe that if there are companies out there that are still doing serious remediation and are not now doing contingency planning, then they probably have even more serious issues than worrying about that trap that's probably been set somewhere in one of the other companies that's now doing contingency planning.

Certainly a call has been made to the security officers, and they need to pay attention, as they always have. I think the message from this Subcommittee ought to be to keep focused on the Y2K effort.

Chairwoman MORELLA. I want to thank all of you, and before we adjourn, I just want to mention the staff that have been very helpful always in contacting you and putting some things together: J. Russell George, who's with the Government Reform Subcommittee, Matt Ryan, Bonnie Heald, Grant Newman, Chip Ahlswede, and Seann Kallagher; our Technology Subcommittee, Jeff Grove and Ben Wu, and the clerk, Joe Sullivan. And there are others: Michele Ash, Trey Henderson, Earley Green, Jean Gosa; and the court reporter, Chris Bitsko. I think I covered everybody. Good.

Thank you. You were just a splendid panel. I hope you'll feel free to contact us at any point with any of your suggestions or recommendations. And as usual, if we could—have other members who may have questions and any other questions we may have, if we may forward them to you. Great. Thank you.

The Committee is now adjourned.

[Whereupon, at 12:06 p.m., the Subcommittee was adjourned.]

APPENDIX 1: ADDITIONAL STATEMENTS

Subcommittee on Technology

Subcommittee on Government Management, Information and Technology Subcommittee

Hearing on The Computer Security Impact of Y2K: Expanded Risks of Fraud?

Opening Statement of Congresswoman Debbie Stabenow
of the 8th District, State of Michigan

August 4, 1999

Madame Chairwoman, Mr. Chairman, thank you for convening the House Y2K Working Group for this important hearing. It is especially ironic that as we continue to receive good news about Y2K preparations - with the financial services industry recently reporting it is 99% compliant - we are faced with another potentially daunting Y2K problem. The fact that some experts believe that there is an increased security risk due to contractors hired to fix Y2K-related problems leaving "trap doors" in computer systems for future access, or otherwise tampering with networks, is indeed cause for concern. Estimates of thefts ranging into the billions of dollars because of this activity must be taken seriously. Our task today must be to assess the likelihood of such incidents and what can be done to prevent them.

This possibility is especially maddening because it could serve to keep needed Y2K preparations from going forward, without much time to spare. I have worked hard in my district letting people know what to expect in regard to Y2K, and working with small businesses to take the necessary steps to be ready on January 1 next year. We must continue to emphasize the importance of undertaking this necessary work.

I again commend the leadership of these two subcommittees on both sides of the aisle in continuing to highlight all the ramifications of the Y2K problem. I would also like to thank our distinguished panelists for being here today to share their expertise on this important topic. Together, I am confident that we will make further progress toward ensuring a smooth transition to the year 2000.

APPENDIX 2: MATERIALS FOR THE RECORD

07/15/99- Updated 11:45 PM ET

Y2K fixes open door for electronic heist

By M.J. Zuckerman, USA TODAY

WASHINGTON - The top Y2K research firm predicts that the l single heist in history, an electronic theft exceeding $1 billion, wi occur as a direct result of the Year 2000 computer glitch.

The Gartner Group "would be surprised if there weren't at least o publicly reported electronic theft exceeding $1 billion," says the s to-be-released study of more than 1,000 of the firm's clients worldwide.

Independent scientists, security professionals and others involved Y2K research have few quarrels with the Gartner Group's warnin

"That's certainly a safe prediction," says computer security expe Donn Parker, author of *Fighting Computer Crime*. "Fixing Y2K opened up vulnerable business computer programs to attacks by larger number of people."

The biggest concern, Gartner says, is that employees hired to upg systems might have left "trap doors" or other means through whi they can clandestinely take control of systems, including those th electronically move $11 trillion a year among financial institution corporations, governments and private organizations.

"We have basically had to open up every system we have to peop may not know enough about," says Joe Pucciarelli, author of the study. It urges scrutiny of "disgruntled or opportunistic employe

"I have no way of determining that there is going to be a theft of magnitude. But I think the sentiment is quite correct," says Fred Schneider, professor of computer science at Cornell University. H one of several scientists and policy analysts concerned that Y2K upgrades, designed to repair systems that could misconstrue date after Jan. 1, 2000, are introducing new vulnerabilities.

Several security firms say they have found "trap doors" in Y2K programming. Some were placed to provide reputable firms an e for future repairs, but others have been intentionally hidden.

"I'm aware of at least three such incidents," says Mike Higgins o consulting firm Para-Protect Services. "One was in a major information technology company which used a Pakistani compan do (upgrades). The company left a hidden trap door and has sinc gone out of business."

But Mark Graf of Sun Microsystems says he doesn't consider Y2 itself a serious security problem: "If you had such poor security t you didn't take prudent measures before, I don't see how Y2K re makes you any less secure."

But Higgins, among others, notes that in many businesses, "norm due diligence is lagging due to the breath of the (Y2K) work" tha remains to be completed.

- Go to Nationline
- Go to News front page

Strategic Planning, SPA-07-8292
J. Pucciarelli

Research Note
1 April 1999

Year 2000 and the Expanded Risk of Financial Fraud

As part of year 2000 systems remediation efforts, every aspect of every IT system involved in enterprise financial management has been opened and potentially subjected to change, raising the risk of financial theft and fraud.

Core Topics
IT Management: IT Financial Management; IT Policy

Key Issues
How should business managers, enterprise executives and IS managers co-develop necessary IT policies and practices? What management tools are appropriate for building the business and IT relationship?

Strategic Planning Assumptions
By 2004, there will be at least one publicly reported electronic theft exceeding $1 billion (0.7 probability); year 2000 remediation efforts will be a root cause of the security lapses that will have allowed this theft to happen (0.7 probability). By 2004, the broad implementation of E-commerce-enabled business models, coupled with the increased risk of electronic theft and fraud, will significantly expand the market and scope of the annual financial audit review to include detection and system analysis services (0.8 probability).

Note 1
Volumes of Corporate Electronic Payments
Financial electronic data interchange (EDI) over the Automated Clearing House (ACH) Network grew by 42.7 percent in 1998, according to statistics released by the National Automated Clearing House Association. In 1998, more than 64.5 million financial EDI transactions crossed the ACH Network, up 42.7 percent from 1997. This figure includes business-to-business and government-to-business financial EDI, non-EDI payments, and intrabusiness cash concentration and cash management transfers. The dollar amount of these payments exceeded $11 trillion. Financial EDI is the electronic exchange of payments, payment-related information or financially related documents in standard formats between business partners. With financial EDI, the remittance information accompanies the payment; that is, the money and the data stay together.

Two tremendous but unrelated forces will be intersecting soon and the result will be bad news! First, the world's financial systems have largely migrated to an electronically interconnected business model. Best estimates are that $11 trillion dollars in electronic transfers occurred in the United States in 1998 (see Note 1). To support this activity, we have created computerized systems to manage every aspect of these transactions. And, in order to maintain the integrity of these systems, we will, by Dec. 31, 1999, have systematically examined virtually every line of code, every interconnection, and every computer involved in this process (see Note 2). Given the enormity of this undertaking, the scope of the assets that flow through these systems, and the unbounded creativity of the human mind, we believe that by 2004 there will be at least one publicly reported electronic theft exceeding $1 billion (0.7 probability); year 2000 remediation efforts will be a root cause of the security lapses that will have allowed this theft to happen (0.7 probability).

Law enforcement authorities attempting to solve a crime search to identify the means by which the crime occurs, establish the motive for the crime, and attempt to prove that a particular suspect had an opportunity to commit the crime. In the case of the first billion-dollar electronic theft or fraud, the motive will likely be one of greed combined with a highly skilled software engineer who feels unappreciated or under-recognized for his or her efforts and accomplishments (especially related to the very stress of the year 2000 remediation effort). The means will be the tools at hand — the same electronic systems that so reliably transact the business of the day will be instructed to transfer funds beyond the boundaries of the enterprise into the hands of the thief. The opportunity to perpetrate the crime will come in an odd moment: a situation outside the bounds of the operating manual. A system will crash unexpectedly and a single software engineer will make changes without the normal reviews, due

GartnerGroup

Entire contents ©1999 by Gartner Group, Inc. All rights reserved. Reproduction of this publication in any form without prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. GartnerGroup disclaims all warranties as to the accuracy, completeness or adequacy of such information. GartnerGroup shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

Note 2
Year 2000 Remediation and Fraud
Year 2000 date remediation for software programming doesn t create the possibility of fraud *per se*. Rather, it is the requirement to open the code and allow changes in the hands of someone with nefarious intent that is the risk. Ideally, nonauthorized changes to parts of the program other than changes required for date remediation would be identified, reviewed in detail and certified by the quality assurance process. If either the change control process fails by not detecting other changes or the quality assurance process fails by not certifying the appropriateness of all changes, then authorized changes could be made that, in combination with other security lapses, could combine to allow a theft. It is highly likely that, when and if this were to occur, it will be the result of a string of related failures and lapses. The problem is that, since we have never gone through this type of a broad-scale disruption, the "failure" mode will likely be a series of events we have never seen before. In other words, security teams need to think very creatively as they review and reconsider risk management and risk containment strategies.

diligence or oversight. Further, the opportunity will likely occur years after Jan. 1, 2000. A hypothetical scenario: An artifact of the year 2000 remediation effort will cause a problem; that is, a system will go do as a result of some other subsequent change. As a result, someone will go into the code and make a heroic save by entering last minute changes to a program so that a deadline can be met — and, along with the save, make unauthorized changes leading to the crime.

Specific steps can be taken now and continually reemphasized because, despite our wish to return to highly stable, status quo operations, changes in competition, business models and distribution channels will bring a much more dynamic operational norm. The most effective theft and fraud deterrent is to create the perception that there are very high levels of security. To accomplish, this we advise the IS and finance organizations to collaborate to create a year 2000 security team composed of individuals with the requisite technical and audit skills to review procedures, assess the risks and implement a risk containment plan. Procedure reviews must limit the ability of a single individual to make changes or initiate activities without a second person participating in the process. Risk assessment must include reviewing all enterprise insurance coverage as well as the contracts with external services providers and independent (programmer) contractors. Risk management plans should include careful reconsideration of all existing theft and fraud deterrence activities in light of this expanded threat profile.

Bottom Line: The law of very large numbers dictates that we will have a vastly increased risk of electronic theft and fraud after the year 2000 remediation efforts. In the rush to aggressively solve one problem (year 2000), enterprises need to ensure appropriate resources have been rededicated to protecting the enterprise from the increased risks of electronic theft or fraud — possibly the most important artifact created by year 2000 remediation.