YEAR 2000 RISKS: WHAT ARE THE CONSEQUENCES OF INFORMATION TECHNOLOGY FAILURE?

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 AND OVERSIGHT

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTH CONGRESS

FIRST SESSION

MARCH 20, 1997

Committee on Science
[No. 5]

Committee on Government Reform and Oversight
Serial No. 105–26

Printed for the use of the Committee on Science and the Committee on Government Reform and Oversight

U.S. GOVERNMENT PRINTING OFFICE

42–394CC WASHINGTON : 1997

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-055321-0

COMMITTEE ON SCIENCE

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

SHERWOOD L. BOEHLERT, New York
HARRIS W. FAWELL, Illinois
CONSTANCE A. MORELLA, Maryland
CURT WELDON, Pennsylvania
DANA ROHRABACHER, California
STEVEN SCHIFF, New Mexico
JOE BARTON, Texas
KEN CALVERT, California
ROSCOE G. BARTLETT, Maryland
VERNON J. EHLERS, Michigan
DAVE WELDON, Florida
MATT SALMON, Arizona
THOMAS M. DAVIS, Virginia
GIL GUTKNECHT, Minnesota
MARK FOLEY, Florida
THOMAS W. EWING, Illinois
CHARLES W. "CHIP" PICKERING, Mississippi
CHRIS CANNON, Utah
KEVIN BRADY, Texas
MERRILL COOK, Utah
PHIL ENGLISH, Pennsylvania
GEORGE R. NETHERCUTT, JR., Washington
TOM A. COBURN, Oklahoma
PETE SESSIONS, Texas

GEORGE E. BROWN, Jr., California RMM*
RALPH M. HALL, Texas
BART GORDON, Tennessee
JAMES A. TRAFICANT, Jr., Ohio
TIM ROEMER, Indiana
ROBERT E. "BUD" CRAMER, Jr., Alabama
JAMES A. BARCIA, Michigan
PAUL MCHALE, Pennsylvania
EDDIE BERNICE JOHNSON, Texas
ALCEE L. HASTINGS, Florida
LYNN N. RIVERS, Michigan
ZOE LOFGREN, CalifoRNia
LLOYD DOGGETT, Texas
MICHAEL F. DOYLE, Pennsylvania
SHEILA JACKSON LEE, Texas
BILL LUTHER, Minnesota
WALTER H. CAPPS, CalifoRNia
DEBBIE STABENOW, Michigan
BOB ETHERIDGE, North Carolina
NICK LAMPSON, Texas
DARLENE HOOLEY, Oregon

TODD R. SCHULTZ, *Chief of Staff*
BARRY C. BERINGER, *Chief Counsel*
PATRICIA S. SCHWARTZ, *Chief Clerk/Administrator*
VIVIAN A. TESSIERI, *Legislative Clerk*
ROBERT E. PALMER, *Democratic Staff Director*

SUBCOMMITTEE ON TECHNOLOGY

CONSTANCE A. MORELLA, *Chairwoman*

CURT WELDON, Pennsylvania
ROSCOE G. BARTLETT, Maryland
VERNON J. EHLERS, Michigan
THOMAS M. DAVIS, Virginia
GIL GUTKNECHT, Minnesota
THOMAS W. EWING, Illinois
CHRIS CANNON, Utah
KEVIN BRADY, Texas
MERRILL COOK, Utah

BART GORDON, Tennessee
EDDIE BERNICE JOHNSON, Texas
LYNN N. RIVERS, Michigan
DEBBIE STABENOW, Michigan
JAMES A. BARCIA, Michigan
PAUL MCHALE, Pennsylvania
MICHAEL F. DOYLE, Pennsylvania
ELLEN O. TAUSCHER, California

*Ranking Minority Member
**Vice Chairman

COMMITTEE ON GOVERNMENT REFORM AND OVERSIGHT

DAN BURTON, Indiana, *Chairman*

BENJAMIN A. GILMAN, New York
J. DENNIS HASTERT, Illinois
CONSTANCE A. MORELLA, Maryland
CHRISTOPHER SHAYS, Connecticut
STEVEN H. SCHIFF, New Mexico
CHRISTOPHER COX, California
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
JOHN SHADEGG, Arizona
STEVEN C. LATOURETTE, Ohio
MARSHALL "MARK" SANFORD, South Carolina
JOHN E. SUNUNU, New Hampshire
PETE SESSIONS, Texas
MIKE PAPPAS, New Jersey
VINCE SNOWBARGER, Kansas
BOB BARR, Georgia

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
GARY A. CONDIT, California
CAROLYN B. MALONEY, New York
THOMAS M. BARRETT, Wisconsin
ELEANOR HOLMES NORTON, Washington, DC
CHAKA FATTAH, Pennsylvania
TIM HOLDEN, Pennsylvania
ELIJAH E. CUMMINGS, Maryland
DENNIS KUCINICH, Ohio
ROD R. BLAGOJEVICH, Illinois
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
JIM TURNER, Texas
THOMAS H. ALLEN, Maine

BERNARD SANDERS, Vermont (Independent)

KEVIN BINGER, *Staff Director*
DANIEL R. MOLL, *Deputy Staff Director*
JUDITH MCCOY, *Chief Clerk*
PHIL SCHILIRO, *Minority Staff Director*

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

STEPHEN HORN, California, *Chairman*

PETE SESSIONS, Texas
THOMAS DAVIS, Virginia
JOE SCARBOROUGH, Florida
MARSHALL "MARK" SANFORD, South Carolina
JOHN E. SUNUNU, New Hampshire

CAROLYN MALONEY, New York
PAUL E. KANJORSKI, Pennsylvania
MAJOR R. OWENS, New York
ROD R. BLAGOJEVICH, Illinois
DANNY K. DAVIS, Illinois

EX OFFICIO

DAN BURTON, Indiana
HENRY A. WAXMAN, California

J. RUSSELL GEORGE, *Staff Director and Chief Counsel*
MARK UNCAPHER, *Counsel*
JOHN HYNES, *Professional Staff Member*
ANDREA MILLER, *Clerk*
DAVID MCMILLEN, *Minority Professional Staff Member*

CONTENTS

	Page
March 20, 1997:	
Bruce Hall, Research Director, Gartner Group, Stamford, CT	4
Ann Coffou, Managing Director, Year 2000 Relevance Service, Giga Information Group, Norwell, MA	10
Vito C. Peraino, Attorney, Hancock Rothert & Bunshoft, Los Angeles, CA	25
Harris Miller, President, Information Technology Association of America, Arlington, VA, accompanied by Marc A. Pearl, General Counsel and Vice President	32

YEAR 2000 RISKS: WHAT ARE THE CONSEQUENCES OF INFORMATION TECHNOLOGY FAILURE?

THURSDAY, MARCH 20, 1997

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

Washington, DC.

The Subcommittees met jointly at 1:05 p.m., in room 2318 of the Rayburn House Office Building, Hon. Constance Morella and Hon. Stephen Horn, Chairpersons of the Subcommittees, presiding.

Mrs. MORELLA [presiding]. I'm going to call to order the meeting of the Joint Subcommittees dealing with the Year 2000 risks.

The question that we're going to be looking at today at this hearing is what are the consequences of information technology failure.

And I'm joined by the Chairman of the Government Reform and Oversight Subcommittee that has looked into this, Steve Horn, and the members who are with us as we begin the proceedings today are Congressman Davis and Congressman Ehlers.

Welcome to an on-going series of hearings held by the Government Reform and Oversight Committee and the Science Committee on the Year 2000 Challenge.

I'm pleased to once again, as I mention, join with my colleagues here to address the very critical issue which will literally affect virtually every human on the planet.

As everyone in this room knows, we're all competing in a race against time to avoid an impending computer catastrophe. Unless it's corrected, when we're in the Year 2000, computer applications that touch our lives across the world may fail.

Amazingly enough, though, despite our best efforts in Congress to educate the private sector on the potential for great operational and fiscal disaster, if they are still non-compliant by the Year 2000, some companies have yet to address the problem.

The deadline we face is unforgiving and time is running out.

Even though there are just 144 weeks or 33 months from today to get the job done, it appears as if these companies are not acting expeditiously enough to be fully Year 2000 compliant by the close of the decade.

And indeed this fact is borne out in the Gartner's Group's recent prediction that more than one-half of all organizations worldwide will not fully complete their Year 2000 effort.

This is startling, because when Chairman Horn and I began investigating this problem at the beginning of last year, our focus was to ensure timely and effective action by our Nation to meet the tremendous challenge of solving the Year 2000 problem, both in the public and the private sectors.

Now it appears as if we must recategorize our thinking, embrace the risks of failure and discuss its consequences. That's the purpose of this afternoon's hearings.

Appearing before us today is a very distinguished panel of witnesses.

Our first witness is Mr. Bruce Hall, who will discuss the Gartner Group's long-term forecast for the Year 2000 problem, the realization of failure and the strategies that must emerge from the realization.

Following Mr. Hall will be Ms. Ann Coffou of the Giga Information Group who will be discussing the scope of the Year 2000 problem.

Initially represented as just a computer software program problem, the scope of the Year 2000 challenge now seems to have the potential to impact more than just computers. This problem seems to be endemic to not just computer software or programs but in any product which contains a computer chip.

Ms. Coffou will discuss this potential problem.

Did I pronounce your name correctly?

Coffou.

Following Ms. Coffou will be Mr. Vito Peraino, an attorney from Los Angeles, who has written extensively on the legal aspects of the problem before us. It seems clear that if in fact programs do fail, liability will be a major issue.

Our final witness will be Harris Miller, President of the Information Technology Association of America, who is accompanied by the ITAA counsel, Mr. Mark Pearl.

Mr. Miller has appeared before us before because ITAA has been very much in the forefront on the Year 2000 issues.

And both Mr. Harris and Mr. Pearl will discuss these initiatives, including ITAA's voluntary certification program as well as the related issue of liability.

It's clear that our Nation still has much to do in addressing the Year 2000 problem.

Congress has taken the lead in pushing for immediate action to solve the problem. We'll continue to do all we can to quickly implement necessary solutions in the Federal Government and to continue encouraging our Nation's businesses and state and local governments to create immediate corrective measures.

I look forward to working with my colleagues, new and old, to correct this millennium bug, and I look forward to engaging in a constructive dialogue with our witnesses on this issue in the hopes that we can also come to a resolution to expedite it.

Right now, I'd like to recognize Chairman Horn for his comments and opening statement.

Mr. HORN. Thank you, Madam Chairwoman.

We're here today to continue our joint investigation into the hazards of failing to address the Year 2000 software date conversion problem. The dangerous fact is that it is as simple to explain the

Year 2000 problem as it is difficult to comprehend its repercussions. Much of our technology is unable to recognize the difference between the Year 2000 and the year 1900, but exactly how much our technology will be affected and what damage will result are critical questions that remain unanswered. Today's hearing should provide some very important, perhaps very disturbing answers.

In past hearings, we've learned about some potential consequences of this problem for the Federal Government. Corrupted date information will affect everything from the processing of social security checks to the safety maintenance of our missile systems.

Today, however, we're going to take a slightly broader perspective. How might the Year 2000 problem affect individuals and private organizations directly? The question is terribly relevant to the government not only because it is made up of individuals but also because it interacts with and depends upon other organizations and individuals.

We're going to hear testimony today about automated devices with embedded microchips. These turn out to be rather important. Consider how many technologies with such chips touch our daily lives. Everything from fax machines to sprinkler systems, from pacemakers to elevators, and from manufacturing process control systems to military messaging systems. The fact is that every one of these technologies must keep track of dates in order to operate.

We're also going to hear about what technology failure might mean in legal terms. Just as technology is ubiquitous in our society, so are legal obligations. Your bank must accurately perform and record innumerable transactions everyday. What if it could no longer do this? Then take it a step further.

Suppose your bank prepares its computers for the Year 2000 but another company on which your bank relies does not. Once again, corrupted information, a failure of services, and legal action would be likely to follow.

The theme here, it seems to me, is the interconnectedness of our society. We're all in this together. Technology forms an amazingly intricate web, not only within large organizations, such as the Federal Government, but between organizations and individuals around the globe.

A tremendous number of our social, governmental, and commercial relationships depend on this web. Failure cannot be isolated.

The risks and consequences we're talking about today are of immediate and overwhelming concern to everyone including those who are responsible for the operation of the Federal Government and the employees whose work depends on effective, efficient computers.

We must understand and address the pervasive nature of this problem.

Our witnesses today are surely going to help us do that. They bring here an expertise in a variety of areas, and we look forward and we thank you for your testimony.

Mrs. MORELLA. Thank you, Chairman Horn.

I'd now like to—you know we have two Mr. Davises here? And so in terms of the bipartisan quality of these Subcommittees, I'm going to recognize Mr. Davis from Illinois and welcome you, and if you have any comments you'd like to make.

Mr. DAVIS of Illinois. I don't have any comments I'd like to make at the moment.

Mrs. MORELLA. Thank you for being here.

I now recognize the other Mr. Davis from Virginia.

Mr. DAVIS of Virginia. I'll also be brief. I serve on both Subcommittees and I appreciate both Chairwoman Morella and Chairman Horn's leadership on this issue and look forward to hearing from our distinguished panel today.

Mrs. MORELLA. Thank you, Mr. Davis.

Ms. Stabenow from Michigan? You're going to find that she will be followed by someone else from Michigan too.

Ms. STABENOW. We're doing our best to surround the Chair on the Subcommittee. I would pass as well. I'm anxious to hear from the folks that are here to testify.

Mrs. MORELLA. Thank you, Ms. Stabenow.

Mr. Ehlers.

Mr. EHLERS. Thank you, Madam Chairwoman. I have no desire to enter an opening statement, but I do want to thank both of the Chairs for holding this hearing. It's an extremely important issue. It's very important for the Congress to be on top of it. It's even more important for the entire Nation to understand the dimensions of it and what has to be done.

Thank you.

Mrs. MORELLA. Thank you, Mr. Ehlers.

What we'll do is we'll progress then with the statements from each of you hopefully not to exceed 5 minutes, and then we'll open it to questions by all of the members of the panel here.

And so we'll start of then with you, Mr. Hall. I just want you to know that I have often, in comments, quoted the Gartner Group, so now we have you here to talk to us about what is happening.

STATEMENT OF MR BRUCE HALL, RESEARCH DIRECTOR, GARTNER GROUP, STAMFORD, CONNECTICUT

Mr. HALL. Thank you. Can you hear me okay?

We'll try to give you some quotable statements today then.

Chairman Horn and Chairwoman Morella, Gartner Group is honored to be given the opportunity to testify today regarding the Year 2000 computer date change crisis.

Gartner Group is an information technology advisory and consulting firm working with the majority of the largest users of information technology, both public and private, worldwide.

We'd like to first applaud the efforts of both your Subcommittees in bringing the Year 2000 issue to light. Your work has helped to illuminate a crisis of unprecedented proportions that must be addressed to avoid business and government service failures.

I'd like to first discuss the role of mainframe processing systems in society today and the proliferation of the Year 2000 problem.

Approximately 80 percent of the computer code to be remediated for the Year 2000 problem is on large mainframe systems. A common misperception, however, is that mainframes are outdated and near the end of their useful life, and in fact mainframe processing power increased in 1996 by 20 percent and is projected to increase again in 1997 by another 20 percent.

Most efforts to retire or downsize mainframe systems have been less than successful and these large systems remain at the heart of information technology processing for virtually all larger organizations, and they continue to run software infected with the Year 2000 virus.

The bottom line is that there is no time to retire or replace a significant amount of mainframe systems, and we are left with a massive repair effort that will be virtually all-consuming of our key information technology resources over the next 3 years.

The Year 2000 problem also extends to other technologies that employ any kind of programming due to the use of two digits to represent years becoming a programming habit and not an enforced standard.

All computer platforms, including many modern client server systems employ the two digit year habit as do microprocessors, embedded firmware and other systems typically found outside of the data center.

In 1995, more than 3 billion microcontroller chips were shipped and are used in telephone systems, bar code readers, bank cash machines, civilian and military avionics and process control equipment.

Organizations cannot afford to ignore these systems whose failures may have possibly dire impact.

Next I'd like to address the concept of time horizon to failure, or THF. Many Year 2000 compliance plans, both in public and private organizations, call for achieving Year 2000 compliance on January 1, 1999, allowing the year of 1999 for testing.

This timetable wrongly assumes that the technology only performs calculations that look back into the century when the next one arrives.

One example of such a calculation is an age calculation where the current year is used to derive age, based on birth year. Unfortunately, the problems we face are not all looking backwards; they're also looking forwards.

For example, mortgage companies faced Year 2000 problems in 1970 when calculating 30-year mortgages, and we've seen failures in credit card expiration dates and other forward-looking situations already.

There is a point in time called the time horizon failure or THF when the number of forward-looking calculations increases to the point where they become impossible to fix through the normal course of maintenance.

This is the date by which repair, replacement, or retirement of affected systems must be done and fully tested. Many systems work in a one-year forward projection mode and thus have THFs of January 1, 1999.

So to allow for adequate testing, these systems may need to be remediated by July 1, 1998, less than 16 months from today.

In the case of the U.S. Government, October 1, 1999, the first day of the 2000 fiscal year will be the THF for some systems.

Year 2000 remediation plans that fail to recognize THF are incomplete and we urge that all project teams work to determine each technology's THF and build it into their planning time line.

Lastly, I'd like to discuss the idea of planning not to finish. A medium-sized organization is looking at a Year 2000 project a little over 100 and possibly multi-hundreds of work years to complete, easily the largest project ever undertaken. This combined with other complicating factors regarding the project causes us to prudently accept the fact that we may not finish it.

Given this, we need to stop trying to just fix dates but endeavor to ensure continuing of the key processes that the organization is chartered for and to remediate the technology that supports those key processes first.

These processes may include partners external to us and their Year 2000 failure could interrupt our service delivery.

If our key technical and project management experts desert us or are reallocated in the middle of a project, we risk failure. And we must plan not just for what will be done for the Year 2000 and who will do it, but we must also understand what will be left undone.

We might also consider rethinking the project step of assessment. The Year 2000 project can be likened to an old house that needs remodeling. We know it's a big job and we're trying to figure out how much it will cost and how long it will take. But we are trying to predict the cost of a job while standing on the curb across the street.

As usual, the contractor thinks the job will cost more than the homeowner thinks it should.

For the Year 2000, our enemy is time, not cost. So why don't we get a crew together and begin the remodeling work on the first, most important room of the house right away. Given that we likely will not finish and that certain rooms must be done, we can choose the rooms in which we will begin, watch that work closely and use it to predict the rest of the job.

We aren't discounting the need for world class planning but our message is to do the planning in parallel to the remediation work of the most critical systems. And the sooner we get crews with experience dealing with the problem, the sooner they are productive on subsequent remediation projects, having learned the tricks of the trade.

I hope this testimony has shed further light on the Year 2000 problem, and I look forward to the question and answer session.

Thank you.

[The prepared statement of Mr. Hall follows:]

GARTNER GROUP, INC.

TESTIMONY OF BRUCE H. HALL

RESEARCH DIRECTOR, APPLICATIONS DEVELOPMENT METHODS AND MANAGEMENT

BEFORE

THE SUBCOMMITTEE ON TECHNOLOGY

AND

THE SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION AND TECHNOLOGY

MARCH 20, 1997

Chairman Horn and Chairwoman Morella:

Gartner Group is honored to be given the opportunity to testify today regarding the year 2000 computer date change crisis. Gartner Group is an information technology advisory and consulting firm working with the majority of the largest users of information technology, both public and private, in North America and around the world. Our role in the year 2000 crisis is to: work with our clients to help estimate the size and scope of the effort; increase awareness and help to gain sponsorship for the project; provide input on technological, remediation, and organizational strategies; and to advise on tool and outside services buying decisions. To date, Gartner Group has worked with over 2,500 organizations facing this crisis.

We would like to first applaud the work of both the Science subcommittee and the Management, Information, and Technology subcommittee in your efforts to bring the year 2000 issue to light both in both the public and private sectors. Your work has helped to illuminate a crisis of unprecedented proportions that must be effectively addressed to avoid worldwide business and government service failures.

In our testimony today, we would like to address three areas regarding the year 2000 crisis. First, we would like to "restate" the problem in terms of the systems that are affected and their role in society today. We would next like to address a concept called Time Horizon to Failure (THF), critical to understanding and planning for this crisis.

Lastly, since the year 2000 project is so large and because of other factors, we must embrace the very real possibility that we will not finish the project, and we'd like to discuss strategies that emerge from this realization.

THE ROLE OF LARGE INFORMATION PROCESSING SYSTEMS IN SOCIETY TODAY AND THE PROLIFERATION OF THE YEAR 2000 PROBLEM

When the year 2000 issue was first introduced, in was termed by many as "just a mainframe problem." Indeed, approximately 80% of the computer code to be fixed is in fact on large mainframe systems. A common misperception, however, is the role these systems play in worldwide information processing, and their expected life spans. Many people believe that mainframes are outdated and near the end of their useful life. This leads to the belief that the year 2000 crisis might be significantly overstated since most older technology that is rife with the problem will be retired or replaced prior to experiencing failures. This is not the case.

The fact is that large, mainframe systems remain at the heart of information technology processing for organizations both public and private worldwide. A small minority of these larger systems have been "downsized" to client/server or otherwise modernized. However, the total amount of large, mainframe processing power actually *increased* in 1996 by 20%, and is projected to increase again in 1997 by another 20%. And, for those that think investment in mainframe technology has been slowed or suspended, consider that 55% of large scale systems running today are less than two years old.

So, one might ask, "if 55% of the systems are new, doesn't that help to fix the year 2000 problem?" No, it doesn't, since only the *hardware* has been replaced, and that new hardware continues to run the same *software* still infected with the year 2000 virus. This is analogous to upgrading from a 386 to a Pentium PC, and then watching your favorite game run faster on the new machine. And, as the software running on these large systems is maintained and expanded, it is bound by the original architectures on which it was designed: two digit years. Even with the proliferation of PCs and client/server systems that have certainly increased personal

productivity and taken over a small percentage of traditionally "mainframe" type work, mainframe systems continue to provide much of the data these distributed systems work with. While the PC systems provide a nicer, easier to use presentation to the user, large scale systems remain at the core of information processing today.

The bottom line is that it is a generally accepted fact in the industry that "downsizing" these large systems is not the answer due to time and capability constraints, So, we are left with a massive repair effort of our existing systems that will be virtually all-consuming of our key information technology resources over the next three years.

Compounding our large, mainframe problem is the fact that the year 2000 problem extends to all technologies that employ any kind of programming. The use of two digits to represent years has become a programming "habit," much as we write the date on our checks as using only two digits, such as "3/20/97." This habit has extended to all computer platforms, and indeed, many of the client/server systems in use employ the two digit year standard of the mainframe system on which it was based, and/or take in data from the mainframe and process it using only two digits for the year. Thus, all computing platforms must be inspected and corrected if necessary for year 2000 failures.

The two-digit habit has also extended to programming of microprocessors, embedded "firmware," and other systems typically found outside of the data center. In 1995, Dataquest, a Gartner Group company, estimated worldwide shipments of RISC and x86 microprocessors at more than 200 million units—over half of which were in embedded systems. This figure is itself tiny when compared to the more than three *billion* microcontroller chips shipped in the same period. The average car contains 14 microcontrollers, and some include more than 45. Other uses include telephone systems, video recorders, bar code readers, microwave ovens, bank cash machines, factory machinery, civilian and military avionics, process control and monitoring equipment, and air-conditioning systems. Year 2000 faults in many of these units would be annoying rather than catastrophic; however, organizations cannot afford to ignore the small percentage that have direct business impact.

Identifying and correcting year 2000 errors in embedded systems is expensive (generally requiring significant manual effort). Much factory equipment cannot be shut down or tested trivially. Embedded controllers and microprocessors may be in units that are no longer manufactured, or suppliers may not be able to offer updates. Even when correction is possible, a physical hardware update (such as a new ROM chip) may be required. It is generally difficult and expensive to identify and audit embedded systems. The process cannot be automated and is likely to require physical inspection of hardware distributed widely throughout the organization.

We must accept that risk exists in *any* technology that was ever programmed by a human, examine such technology for possible failures, and form remediation strategies.

TIME HORIZON TO FAILURE (THF)

In many year 2000 compliance plan documents we have seen, both in the public and private sectors and not just in the U.S. but worldwide, the target date for completion of the compliance initiative is January 1, 1999, allowing the year of 1999 for testing. This timetable wrongly assumes that any technology subject to year 2000 date change problems only performs calculations that "look back" into this century when the next one arrives. One example of a such a calculation is an age calculation, where someone born in 1925 would be treated as follows:

Current Year	97	00
Subtract Birth Year	25	25
Giving Age	72	-25

Certainly, there are many, many "looking back" calculations of the type above that will fail on January 1, 2000. In addition, computer operating systems or other underlying technology may fail because it doesn't know what to do when the system's internal clock reads "00" as the year. All these conditions must be addressed.

Unfortunately, the problems we face are not all "looking backward," they are also "looking forward." For example, mortgage companies faced year 2000 problems in 1970 when calculating 30-year mortgages. Five year financial projection calculations failed in 1995. One company's books were altered in 1993 since their financial system couldn't calculate for the year 2000. Because of this their seven year depreciation schedule was changed to a six year schedule, significantly altering the compa-

ny's financial position. We've already seen failures in credit cards, expiration dates, and other forward-looking situations.

The problems already experienced as described above were fixed in the course of normal systems maintenance. However, as the year 2000 approaches, the number of forward-looking calculations increases, and at some point in time it will become impossible to fix the problems through normal maintenance. This point in time is called the Time Horizon to Failure, or THF, and is the point at which we must have systems with the year 2000 problem fixed, retired or replaced once and for all.

The THF must be determined for each technology as part of the planning process. If a system only calculated age, its THF would in fact be January 1, 2000, and we would have until then to fix it (less some reasonable time to shake out problems as described above). However, many, many systems work in a one-year forward-projection mode (for example, reservation systems, manufacturing/order systems, financial systems, and many others), and thus have THFs of January 1, 1999. In the case of the U.S. government, many systems have THFs of October 1, 1999, the first day of the 1999–2000 fiscal year, as calculations look into the next century as part of processing the current fiscal year. Many states systems have a THF of July 1, 1999, the start of many 1999–2000 fiscal years.

As an example of planning for THF, consider a system that in fact has been determined to fail on January 1, 1999. That system would need to be fixed earlier than January 1, 1999, to allow for a reasonable "shakeout" period—let's call that period six months. That means that the system must be fixed by July 1, 1998—less than 16 months from today. An "average" system may take five to ten labor years to remediate. This means that in less than 1.5 calendar years, we must perform five to ten years worth of work. It may be possible to "divide" the system into parts with different THFs and thus different time constraints in order to spread out the work. Still, organizations that perform this type of analysis quickly realize they do not have the internal resources to complete all of this work in the time allotted. This also gives us pause when considering software package replacement strategies since the average time to select, implement, customize, transfer data, retrain users, and retire the existing system at risk averages two years and is often longer.

The bottom line is that Year 2000 remediation plans that fail to recognize THF are incomplete. We urge that all project teams worldwide attacking this issue immediately incorporate THF into their planning and work with their technical experts and users to determine each technology's THF and build it into their planning and resource timelines.

PLAN NOT TO FINISH

The year 2000 date change is likely to be the single biggest project ever undertaken for information technology organizations. Consider the fact that a medium size organization, with an average size technology portfolio, is looking at a project of well over one hundred—and possibly multi-hundreds, of person-years to complete. Some large organizations are facing efforts of over 1,000 person-years. In addition to the sheer size of the problem, we face other challenges as well. The human resources to do the work are scarce and getting scarcer. The people we do have consider the work tedious, complex, and feel it has a negative impact on their career. Many of the systems to be repaired are old and lacking documentation and in many cases the code itself is missing. Managers already faced with a full agenda of other work are reluctant to reallocate precious resources to this project—especially because it has no perceived end-user benefit, and end users for the most part aren't even voicing concern.

These factors lead us to one inescapable conclusion—that there is a high probability that an organization will not finish this project in time and thus experience business process-interrupting failures. In fact, Gartner Group predicts that more than half of all organizations worldwide will not fully complete the year 2000 effort. Once we recognize and embrace this possibility, we begin to alter our thinking in constructive ways. We see that our goal is not to just fix dates, but to ensure continuance of the key processes that the organization is chartered for, and to fix technology that supports those key processes. We begin to think in terms of the organization's very survival being linked to the solution of the year 2000 problem. We recognize that the processes we perform may include organizational partners, and that *their* year 2000 failure could interrupt our key processes, so we begin to ask our key partners how they are progressing. We recognize that the remediation effort ceases to be one of "fix everything" and becomes one of "fix the most important things first." We begin to think in terms of active prioritization and technology "triage." We recognize that if our key technical and project management experts desert us or are reallocated in the middle of the project, we risk failure. Since we

are already up against tight and unforgiving deadlines, we must also put plans in place to keep those key people on the project. And finally, we must recognize that one of the most important planning aspect for the year 2000 in addition to what *will* be done and who will do it, is what projects and other activities will be left *undone*.

Another offshoot of the realization that we very well may not finish causes us to change our thinking regarding "assessment." Typical year 2000 project plans begin by accounting for the components to be remediated, called *inventory,* then applying some industry standard metrics against that inventory to arrive at an initial cost and labor estimate. When management sees this initial projection, they are stunned at the high cost involved in fixing the problem, and so logically ask for a more detailed assessment. This next assessment is often performed by an outside party, and provides a report that usually reiterates what was learned in the first step—there is a large problem and the cost to fix it will be huge. Then, reluctantly, resources might be reallocated to begin the work, and in the mean time 2-4 months have been wasted. Typically, only in the organizations where the top managers were programmers and thus understand the problem is this pattern avoided.

The year 2000 project can be likened to an old house that needs remodeling. We know it's a big job and we're trying to figure out how much it will cost and how long it will take. But, we are trying to predict the cost of the job while standing on the curb across the street. If we were able to walk through the house, our estimate would be more accurate, and only by getting in and actually doing some of the work can we realistically tell what we are up against. And, as usual, the contractor thinks the job will cost more than the homeowner thinks it should.

For the year 2000, our enemy is time, not cost. At Gartner Group, our recommendation is to immediately get a crew together and immediately begin work on the first, most important, room of the house. Given that we likely will not finish, and that certain rooms *must* be done, we must choose carefully the room(s) in which we will begin, watch that work closely, and use it to predict the rest of the job. We certainly aren't discounting the need for world class planning, but our message is to do the planning in parallel to the remediation work of the most critical systems.

The other benefit getting started gives us is to get crews to work on specific aspects of the project, so that they can learn the tricks of the trade and be more efficient in their subsequent remediation projects. Since we have a fixed and immovable deadline, the sooner we get our crews to work, the more projects they can complete sequentially, and the more efficient they will become. The longer we wait, the more "green" crews we will have to use, and the more we will pay for them, thus further increasing cost and risk of delay and resultant failure.

CONCLUSION

I hope this testimony has shed light on the issues of the persistence of large scale computing technology, the risk of risk of year 2000 failures on all kinds of technologies, Time Horizon to Failure, and that we should plan not to finish. At Gartner Group, we hold a cautious optimism regarding the year 2000 problem, but at the same time predict that this crisis will preoccupy many, many of our technology resources for the next two to three years, and that we will in fact experience society-impacting failures as a result of it. How well those failures are contained depends on the steps we take right now.

Mrs. MORELLA. Thanks, Mr. Hall, it has.

Before I turn to Ms. Coffou, I wanted to recognize the Ranking Member of the Technology Subcommittee, Mr. Bart Gordon, from Tennessee.

Mr. GORDON. Thank you, Madam Chairwoman.

I have some stellar remarks but because of my tardiness, I'll just place them in the record.

Mrs. MORELLA. Without objection, so ordered.

Ms. Coffou.

STATEMENT OF MS. ANN COFFOU, MANAGING DIRECTOR-YEAR 2000 RELEVANCE SERVICE, GIGA INFORMATION GROUP, NORWELL, MASSACHUSETTS

Ms. COFFOU. Thank you.

I'd also like to thank both of the Chairs of these Subcommittees for inviting me to testify here, and also for the good work that you're doing in raising the light onto the issue.

I'm with Giga Information Group, which is a research and advisory business looking at the IT issues. My particular responsibility is looking exclusively at Year 2000 issues and their effect around the world.

As you have seen and have discussed up to this point, the Year 2000 issue has really focused the attention of the Year 2000 issue has mostly been focused on computer systems. There is a second dimension to this entire problem that is also going hand in glove with the computer system, and that's a challenge that has to do with embedded microchips and the routine use of embedded microchips in products ranging from the mundane things like VCRs, fax machines, elevators, lawn sprinkler systems, televisions, all the way up to extremely complex types of products such as devices that help control traffic lights, power generation, water and sewer systems, the proper functioning of aircraft, even to the launching and landing of the space shuttle.

In case there's any confusion about what an embedded computer chip actually does, I don't have one to show you but my hat sings because it has an embedded computer chip in the hat. Now my hat obviously is not going to cause any kind of world problem. However, it's the embedded microchips that perform date and time functions that may well not have been designed to be able to function when the year changes to 2000.

It's going to recognize that 00 as in 1900 and then the functions that are controlled by those computer chips may not work properly.

Potential results of this bug are going to greatly affect everyday consumers just like you and me. And those effects and those results can range from being annoying to being aggravating to being debilitating to being life threatening.

Billions of these chips have become standard components in electrical products. Many chips are combined with other chips within these products. Virtually all of these chips contain computer programming to help them provide the functions that they were designed to provide.

Because most manufacturers utilize preassembled components to build or manufacture their products, the knowledge of exactly how those chips were created, put together and programmed is a little sketchy at best.

So what kinds of problems might these non-compliant embedded chips cause?

Well, take a look at an elevator system. Most elevator systems have embedded chips in them that keep track of the last maintenance activity that was performed on the elevator. If the time has exceeded the time for maintenance, the normal reaction is that the elevator itself takes itself out of service, it goes down to the ground level and stays there until maintenance is performed on the elevator.

Annoying? Sure that's annoying.

But what happens if those elevators all go out of service in a high rise building? How are people going to get work? Taking the stairs isn't always an option.

How will your handicapped employees get to their jobs?

What about the person who suffers a heart attack on the way taking the stairs going up?

Annoying then begins to move all the way past aggravating to debilitating, all the way through to life threatening.

Think about programmable thermostats. What's going to happen on January 1st in the Year 2000 if, all of a sudden, the heat won't come back on? Homes will be cold. Who's responsible for the pipes that freeze, burst, and create all kinds of damage?

The insurance claims alone for a situation like this could rival or exceed those from Hurricane Andrew. I don't mean to sound like a prophet of doom here, but I probably do.

There is a solution. The solution is that every device with an embedded microchip must be tested, and the rule for that means that you're guilty until proven innocent. You're non-compliant until proven compliant.

And who should do the testing? The manufacturers. What's the general reaction so far from the manufacturers? Surprise, disbelief, denial, silence.

It's time that we sent a wakeup call. The potential consequences of non-compliance not only threatens the health and well being of individuals, but the repercussions from this also threatens the global economy as well. Thank you very much.

[The prepared statement of Ms. Coffou follows:]

STATEMENT OF HEARING TESTIMONY

SUBCOMMITTEE ON TECHNOLOGY AND SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION AND TECHNOLOGY

TOPIC: YEAR 2000 RISKS: WHAT ARE THE CONSEQUENCES OF TECHNOLOGY FAILURE?

MARCH 20, 1997

PRESENTED BY ANN K. COFFOU, MANAGING DIRECTOR, GIGA YEAR 2000 RELEVANCE SERVICE

INTRODUCTION

Most attention on addressing the problems and challenges surrounding the Year 2000 has been focused on Information Technology (IT) systems—those automated systems that are under the control of the IT department.

Another dimension to the Year 2000 challenge exists that involves automated devices that use embedded microchips and program code to perform timing or date-related functions that invariably transforms the product into a labor-saving, quality-of-life enhancing tool. These chips have become prevalent in virtually everyone's day-to-day life. As a result, there is a great potential for the average consumer to find himself or herself facing problems and mishaps that have been caused by these same products due to their inability to deal with the change in century.

Although most of these problems will not be of a catastrophic nature to the direct consumer, the overall effect on the economy—worldwide—could be monumental. The potential for problems that could lead to legal litigation are abundant.

The objective of this testimony is to raise the level of awareness to the potential problems and the associated liability ramifications—legal, insurance, and financial—from not addressing these embedded systems. Examples of products with embedded microchips from the business and government marketplace and from the consumer marketplace that could potentially cause problems are given within this testimony along with examples of potential follow-on liability issues for both market sectors.

This information was compiled by Giga Information Group, a third-generation information provider of IT advisory services that address a new level of value and relevance for IT decision makers. Giga offers users, vendors, and investors in IT a suite of integrated services that includes a broad range of IT-related content as well

as a knowledge network of independent IT professionals. Utilizing innovative, Internet-based technology, Giga provides a state-of-the-art approach to finding and using information within a business model that promotes customization, usability, strong value, and high service quality to its members. Founded by Gideon Gartner in 1995, Giga Information Group strives to be the best and most cost-effective knowledge provider in the information technology industry. Giga Information Group is headquartered in Cambridge, Massachusetts with offices in the U.K., Germany, France, Italy, Japan, Korea, and Australia.

MAGNITUDE OF THE SITUATION

Globally, society has benefited tremendously from automation. The efficiency of automated devices has been increased through monitoring them with other automated devices. Automated devices now control processes ranging from the mundane to the most complicated. Some processes are so complex that even the most intelligent and highly trained individual could not control them manually. A good example of this is the launching of the space shuttle. It would not be possible to safely and successfully launch the shuttle using people alone to control all the launch processes. Automation and automated devices are required.

Automated devices do not malfunction unless they have a physical defect or the software, microcode, firmware, or program code driving the device malfunctions. Typically, that device encounters a situation that its software was never designed to recognize or act upon.

A situation that some automated devices may not have been designed to recognize is the change of the century. Because most systems view the year using the last two digits only, some automated devices will identify the "00" as being the year 1900, thus corrupting subsequent calculations using that date. The potential result of these erroneous calculations vary in magnitude. Some may cause nothing more than frustration, while others may wreak havoc. The only way to determine what the potential result will be is to test the device.

This test can be accomplished easily for many automated devices, while testing of devices that contain multiple embedded systems—oftentimes acquired from multiple vendors—becomes more of a challenge. A typical fax machine contains at least one embedded system to control date and time stamping of outbound and inbound faxes. With hundreds of brands and models of fax machines on the market, the task of testing each brand and model poses a challenge.

Given the number of automated devices used in all brands and models of airplanes, cars, and ships—all of which need to be tested—and the challenge becomes a daunting and expensive task.

However, ignoring the potential for malfunctions in these automated devices could result in exponentially larger costs associated with damage control and liabilities for manufacturers of these devices.

BUSINESS AND GOVERNMENT MARKETPLACE

Automated devices that are prevalent in the business and government marketplace can be segmented into two categories: Critical and Non-critical Systems. Critical systems are defined as those that are necessary for a business/government to continue to function. Non-critical systems are those that are prevalent but are not absolutely necessary for continued operation of the entity.

A representative sample of potential problems with critical and non-critical systems follows. This is not intended to be an exhaustive or conclusive list of products with potential problems.

CRITICAL SYSTEMS

MANUFACTURING PROCESS CONTROL SYSTEMS

Most manufacturing plants are highly automated. A small manufacturer of industrial liquid solutions found their production line completely stopped on January 1, 1997. It was discovered that their process control systems were not designed to account for a leap year (1996) and subsequently shut down when the changed from 1996 to 1997. Before company personnel could remedy the situation, the liquid solutions that were in the process pipelines hardened and could not be removed. The company was forced to replace the process pipelines at a cost of $1 million. They were unable to manufacture products for several days, thereby, causing late deliveries to customers. In addition to the cost to repair the pipelines, the company believes they lost three new clients because their shipments were delayed.

The legal ramifications of this example revolve around the software that ran the production manufacturing line. This software was purchased from a vendor who warranted that it would operate correctly under "normal" conditions. The battle is now on as to whether a leap year is an implicitly normal condition that should have been addressed within the software.

Software vendors have errors and omissions insurance to cover situations like this. Taken in isolation, the insurance claims that would be filed by the software vendor should it be found liable are not particularly newsworthy. However, what happens when hundreds or thousands of software vendors file claims to handle the errors created from their products?

ELEVATORS

Most elevators have embedded systems that monitor the amount of time between maintenance checks. If these automated devices calculate that the allowable time between maintenance checks has been exceeded, most elevators will go to the bottom floor in the elevator shaft, take themselves out of service, and remain at the bottom of the shaft until maintenance is performed and the clock is reset.

What if this embedded system was not designed to identify the change from 1999 to 2000 and it interprets the "00" as 1900 making the time between maintenance checks exceed the limit and sends the elevator to the bottom floor making it inoperable? This could be annoying in one building and potentially life threatening in another. Using the stairs isn't always a viable alternative.

How will handicapped workers get to their work floors? How does this affect enforcement of the Americans with Disabilities Act? What happens when a worker suffers a heart attack while climbing the stairs to their eighth floor office? Who is liable for the subsequent medical expenses, insurance claims, and disability payments? Or in the worst case, will the company be held responsible if the heart attack results in the employee's death? Multiply these possibilities by the number of high-rise buildings in New York City alone and the potential results are staggering.

TELEPHONE SYSTEMS (INCLUDING PBX, VOICEMAIL, AND SWITCHING)

Some telephone systems may not be able to recognize the century change resulting in improper billing for calls, incorrectly time stamped voicemail messages, and incorrectly routed calls.

If the phone system that malfunctions is the 911 emergency system for a municipality, the very lives of the city's population could be at risk. There could be a multitude of legal litigation due to the damages that ensued from lack of response from emergency personnel.

MEDICAL EQUIPMENT

In a very simplified explanation, every time a heart pacemaker detects an irregular heartbeat it sends a shock to the system and then records the time the event occurred. This information is regularly downloaded to a computer system so it can be analyzed by medical personnel. Whenever the information is downloaded, the pacemaker resets itself. The downloaded information is used by cardiologists to detect patterns and irregularities in the patient's heart rhythms. If the software in the receiving system starts recording faulty times for the shock deliveries, the cardiologist could misinterpret the results and administer improper medical care.

The U.S. Veteran's Administration funded a project to interview the top five pacemaker manufacturers to see if they were aware of this potential problem. One company was aware of the problem and said they would have it corrected by the end of 1997. Two companies said that the problem would be fixed before the Year 2000, one before 1998. Finally, one company flatly refused to acknowledge the problem and when pushed declined to discuss the topic any further.

A physician in a heart clinic in Spartanburg, South Carolina, related that a new shipment of heart defribulators the clinic received recently were recalled by the manufacturer. The defribulators use an embedded device that calculates the time since last maintenance similar to elevators. Like the elevator, if the time since the last maintenance check surpasses a certain time frame, the defribulator will not operate—thereby reducing the possibility of malfunctioning on a patient. The manufacturer voluntarily recalled their products when they discovered they were not designed to handle the change in century.

The legal ramifications for these and other medical system malfunctions have the ability to become enormous, precedent-setting lawsuits, not to mention the backlash effect on physician malpractice insurance.

STOCK MARKETS

On January 3, 1997, trading on the Brussels Stock Exchange was halted for three hours because the trading system was unable to function after the date changed from 1996 to 1997. Orders that were placed on December 30, 1996 (the last trading day in 1996) were recognized as December 1997 orders. This prevented investors and brokerages from changing their orders to reflect Wall Street's plunge on December 31, 1996, when the Dow Jones industrial average lost 101.10 points, leaving it up 26 percent for the year after a rise of 33.5 percent in 1995.

Liability issues are still being sorted out over this failure. The opportunity cost to many companies from the closing of the exchange is the basis for several legal actions.

MILITARY MESSAGING SYSTEMS

Three employees of Prudential Securities wrote about the potential for disaster should military message warning systems malfunction. Their scenario:

Dateline: December 31, 1999

You are piloting an F-22 above the Pacific Rim. It is one second to midnight and the foreign craft tracking you is so close you're obliged to send a warning signal as a New Year's greeting.

The other pilot has two seconds to respond. Your on-board strategic systems are now calculating the time difference between when you sent your message and when a reply will reach you.

You wait. The interval seems interminable. To your equipment, though, it is extremely short: 1.5 seconds to be exact! Because you sent your signal in the year "99," and received the reply in the year "00," the difference is negative, and your weapons system is arming!

Who takes the responsibility for the potential loss of life associated with this scenario? The liability issues could potentially span the globe.

RADIOACTIVE MATERIALS WASTE TREND ANALYSIS

Radioactive material waste tanks are monitored and some are controlled by automated sensors and other devices. They all work on date-sensitive trend analysis. What will happen to trend analysis when there is perceived to be a 99-year span between two measurements? Who is responsible?

ATOMIC/NUCLEAR SITES (EXAMPLE FROM THE U.K.)

Software on nuclear sites is subject to stringent quality controls. However, experienced software industry professionals already grappling with the Year 2000 have expressed doubts about how reliable these design-based reassurances are. Hard and fast test data to back up these assurances has not been provided.

The first area of concern is the radiation exposure system.

The program for the control of radiation exposure is called ALARA (As Low As Reasonably Achievable). Nuclear facility personnel wear dosimetry devices that measure the amount of whole body exposure that the employee receives while in the plant. These dosimetry devices are analyzed on a regular basis and the data (exposure amounts) are maintained on a computer system that control personnel access. To meet Nuclear Regulatory Commission (NRC) and The Institute of Nuclear Power Operations (INPO) regulations the exposure amounts are monitored on a daily, weekly, monthly, quarterly, and yearly basis.

Second, a "Training Records Tracking System" computer controls access and actual work assignments to ensure that the Reactor Operators, Second Assistant/Auxiliary Operators, Maintenance Technicians, Radiation Protection Personnel, and Plant Management employees have completed the required initial and requalification training for their work assignments.

The third area of concern related to the Year 2000 is the computer system that tracks various plant commitments for hardware and operation procedure improvements.

When considering the impact of the Year 2000, the following questions arise.

1. Will all plant personnel risk exceeding radiation exposure limits because the ALARA computer system is inoperative?
2. Will unqualified employees be allowed access to the plant and work assignments because the Training Tracking computer system is inoperable?
3. Will plant personnel be at risk because of expired respiratory protection qualifications?

4. How will the Department of Energy (DOE) control, track and inventory uranium 235/238, plutonium, tritium, or americium with Year 2000 problems?

5. Will plant commitments be delayed or not completed on time because the commitment tracking computer system is inoperative?

6. Will unqualified operations personnel be operating the reactor in the control room without the required initial classroom training, on-the-job training, qualification card sign off or requalification training?

7. Will personnel be wearing respirators with expired qualifications (e.g. annual physical examination, medical screening, annual radiation protection requalification training, mask fit process)?

8. Will there be any clearance requirements for the computer professionals to correct the Year 2000 problems at DOE facilities? Is there enough time for the computer professionals to obtain the DOE (Top Secret "Q") security clearance and still have the time to fix the computer systems prior to January 1, 2000?

9. Will the maintenance schedules on plant hardware be carried out properly if computer based records fail?

OTHER CRITICAL SYSTEMS

There are many other critical business/government systems. A partial list of those that have been identified includes:

- Security systems for badge readers, surveillance systems, parking lot gates, and vaults.
- Time-dependent controls such as parking lot lighting, and programmable thermostats controlling HVAC. Some devices work only during certain times of the day and/or only on certain days of the week.
- Power-management functions for HVAC usage and control, UPS (uninterruptable power supply) backups and related components, off-hour power availability for lighting the building.
- Power plant process controls
- Environmental safety systems for detecting changes in humidity, temperature, CO2 levels. Extreme changes are monitored. Some changes are based on duration or spike measurements.

NON-CRITICAL SYSTEMS

FAX MACHINES

Some fax machines may malfunction and put incorrect dates on incoming and/or outgoing faxes. Still others, when tested, ceased to work altogether.

Legal implications could be great if incorrect dates are recorded on faxes that are needed to show actual dates and times as evidence in a legal case. The incorrect dates could negate efforts at due diligence.

If the fax machine ceases to work, warranty issues could come into play, resulting in massive repair and/or replacement costs for manufacturers.

ELECTRONIC TIMECLOCKS

Labor suits could result from malfunctioning timeclocks that did not record employee time correctly resulting in erroneous wage payments.

LANDSCAPING SYSTEMS

If unable to accurately determine the date, sprinkler systems and/or fountains could potentially turn on January 1, 2000—the middle of winter in many locales. The potential for damage caused by the water to property could be eclipsed by the personal injury damages claimed by people who fell on the ice created by the influx of water.

VENDING MACHINES

Some vending machines have direct interfaces with the vendor to indicate low-on-stock and stale-dated items. If the change of century is not recognized, these systems could conceivably continue to order more items that it immediately identifies as stale. The cycle could repeat several times before the problem is identified. Who is responsible for paying for the overstock? These types of date failures have already occurred.

CONSUMER MARKETPLACE

Automated devices will affect the average consumer as well. Below are examples of common, everyday consumer products that could have problems handling the century date change.

THERMOSTATS

Several companies manufacture varieties of programmable thermostats. If not designed to recognize the change in century, it is possible that consumers could awake on January 1, 2000 to a very cold house. In a test of three different examples of programmable thermostats, two of the three stopped working when the year was changed to 2000. One recorded the date as 1900. Of the two that stopped working, one could not be restarted.

If pipes freeze and burst, the resulting damage both inside and outside could be immense. The volume of insurance claims alone could exceed those associated with Hurricane Andrew. The potential for follow-on litigation against thermostat manufacturers, building contractors, and heating contractors for building, selling and installing "faulty" thermostats could also reach large proportions.

To compound the problem, what if the telephone systems are also malfunctioning so calls to the local heating contractor cannot be completed. The results continue to snowball. How many homeowner insurance companies will be able to survive the avalanche of claims?

MICROWAVE OVENS

A brand new microwave oven in a company cafeteria was reprogrammed to December 31, 1999 and allowed to let the date rollover to January 1, 2000. As a result, the microwave ceased operating. The display went blank and could not be brought back to life. The microwave was taken into the local service shop and left for repairs without telling the service technician how the problem occurred. The service company replaced the computer circuit board in the microwave and returned it to the company.

If replacement of the circuit board to handle the century date change is required, will manufacturers recall all models that will not handle Year 2000 properly? Will they even know which models are Year 2000 compliant?

Many consumers purchase extended warranties for their appliances. Will this be covered under the warranty? Or is the warranty actually misleading? Is the manufacturer selling a product with limited function? Should the FTC be involved? Is this false marketing?

The same questions apply for digital watches, cameras with date features, televisions, VCRs, and many more appliances.

WHO WILL TAKE RESPONSIBILITY?

The intent of this testimony is to raise the level of awareness to the potential problems with embedded systems and the potential consequences from those problems. The issue of embedded systems in airplanes, automobiles, ships, and weapon systems was purposely not discussed in detail. These systems represent a huge risk to the life and well-being of the global population. However, the manufacturers of these products, on the whole, are taking the Year 2000 situation very seriously and have programs underway to address their issues. It is the manufacturers of the lesser-publicized products that employ embedded systems that must be given a wake up call regarding the seriousness of Year 2000 issues. Anything with an electrical component should be suspect. The rule should be guilty until proven innocent.

The amount of legal litigation associated with Year 2000 has been estimated by Giga Information Group to be $2 to $3 for every dollar spent fixing the problems. With the estimated size of the market for Year 2000 ranging from $200 billion to $600 billion, the associated legal costs could easily near or exceed $1 trillion. It is improbable to believe that these immense costs will not adversely affect the economy on a global scale. Many companies will simply not be able to continue operating when faced with these legal costs.

Be aware that no legal precedents have been set as yet. There is still time for manufacturers to step forward and take responsibility for fixing their products.

Pressure should be put on manufacturers to voluntarily take action to identify their potential problem areas and fix them. If this doesn't happen by the end of 1997, mandatory regulations imposed by governmental and regulatory bodies should be imposed. Company executives and board members must be held responsible if the company fails to protect consumers from hazards caused by their faulty products.

The true danger is in the domino effect of business failures on the global economy. Competitive advantage will definitely be gained by companies ensuring that their products are Year 2000 compliant. This message must be made loud and clear to businesses worldwide.

A copy of a Giga Planning Assumption titled: Year 2000 Issues: Executive-Level Accountability is attached.

PLANNING ASSUMPTION

Stephanie Moore

Year 2000 Legal Issues: Executive-Level Accountability

PA FORUM
SUBMIT INQUIRY
SAVE PDF FILE
PDF HELP
SEARCH

Statement

Most IT managers are focusing on Year 2000 solutions: how to bring information systems into the 21st century with a minimum of risk and at a reasonable cost. Unfortunately, many companies still risk system failures and subsequent business interruptions as time runs out and system conversions are not completed or are ignored entirely. While the majority of legal actions will be directed at vendors and service providers, the first lawsuits will come from shareholders and be directed at the corporations themselves. Although legal issues relative to the Year 2000 problem are still in their infancy, and precedents will not be set before 1998 [.8p], securities laws and accounting standards are already established, which will govern much of this type of litigation. Organizations should act now to minimize potential litigation against themselves and, at the same time, prepare for litigation against parties that are liable. This Planning Assumption is one of a pair that focuses on Year 2000 legal issues and covers executive-level accountability.

Catalyst

A client inquiry: A CIO is concerned that he may be held legally responsible for his company's Year 2000 problem. He asks, "Are CIOs and IT managers being sued for negligence because of Year 2000 failures?"

Alternative View

Worldwide, the cost to fix the Year 2000 problem will be well in excess of a trillion dollars. Legal fees associated with these expenditures could dwarf this figure. The US government should move to limit damages in order to protect the economy.

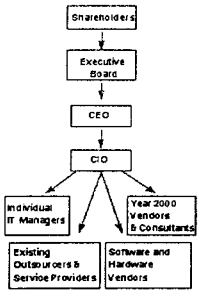
Related Topics

Legal Issues and IT # 4130
Year 2000 Conversion Problem # 5071

Notes

Figure 1 illustrates a Year 2000 chain of liability. Shareholders will provide the first impact on this chain and the blame will eventually trickle down to negligent IT managers, vendors, and service providers.

Figure 1
Year 2000 Chain of Liability



Source: Giga Information Group

Discussion

To date, much of the activity surrounding the Year 2000 problem has focused on proactive solutions for repairing non-compliant systems. However, as IT managers and executives begin to realize the significance of Year 2000 costs and the potential for business interruptions or failures due to insufficient Year 2000 efforts, they will need to take a more reactive stance in order to protect themselves and their organizations. Accountability will be an issue at all levels within the organization, and legal liability will be an issue for the directors and officers of a company, including the CEO, the CFO, and, in some instances, the CIO [.8p].

Definitive answers to Year 2000 legal questions are premature--precedents will not be set before 1998 [.8p]. However, established Securities and Exchange Commission (SEC) rules, securities laws, and accounting principles will be used to set Year 2000 precedents as they pertain to directors' negligence and financial accounting and reporting. Capers Jones of the Software Productivity Research has estimated that the average Fortune 500 company that does not fix its Year 2000 problems can expect to pay $100 million in litigation costs [.7p]. By paying attention to the relevant legal issues early on, corporate executives and technology managers can help to defray the chances and costs of potential litigation.

A Chain of Liability

Shareholders, Executive Boards, Directors, and Officers

While the bulk of Year 2000-related litigation will be focused on product liability and breach-of-contract actions, the first impact on the Year 2000 chain of liability will be shareholder law suits (user organizations will not and should not begin to invest time, resources, and money in litigation until after their Year 2000 problems are addressed). Shareholders that see their investments devalued due to the Year 2000 issue will hold the directors and officers, and possibly relevant lawyers, external auditors, and investment bankers accountable. The basis for shareholder complaints will be:

* Deficient or non-existent Year 2000 efforts causing business interruptions, damages, or failures.
* Incorrect or misleading financial reporting that omits Year 2000-related costs. If the costs are of a material nature, they could cause earnings reports to be significantly below projected earnings which could result in poor stock market performance (see PA, "FASB's Ruling Is a Year 2000 Call to Action"). Alternatively, such misleading reports could cause an investor to invest in a company that it otherwise would not have if it had know the extent of the Year 2000 risks.

In the case of a company's failure or damage, shareholders can argue that the directors of a company did not take reasonable measures to safeguard the company from pending Year 2000 risks. This will be easy to prove if there is evidence that the executive board or any of its members--especially the CEO--were notified of the Year 2000 problem and the associated business risks, and opted not to exercise due diligence

FASB's SFAS 5

The Financial Accounting Standards Board (FASB) promulgates GAAP standards and is empowered to regulate public companies' financial accounting and reporting practices by the Securities and Exchange Commission (SEC). All SEC registrants are required to follow FASB standards. FASB's Statement of Financial Accounting Standards Number 5 (SFAS 5) requires that contingencies that are reasonably possible must be disclosed in a note in the financial statements, even if the amount of the contingency cannot be calculated. SFAS 5 defines a contingency as an existing condition or situation involving uncertainty as to the potential losses or gains to a company that will eventually be resolved when a future event occurs or fails to occur. Year 2000 problems can be construed as such a contingency in many instances.

Directors & Officers Insurance (D&O)

D&O liability insurance is to protect the directors and officers of a company from being personally liable for things such as shareholder lawsuits. In the case of the Year 2000 problem, D&O policies will provide coverage as long as the company can prove that it was making some effort to remedy the problem--another important reason that Year 2000 remediation efforts must be well documented. Unfortunately, some insurance companies may begin to exclude Year 2000-related liabilities from their policies because of the likelihood and copiousness of Year 2000 litigation [.7p]. Some may sell a separate Year 2000 policy, but they will vigorously qualify companies' Year 2000 readiness before they underwrite them.

External Auditors

Under the Securities Act of 1933, auditors are considered to be experts with regard to a client company's financial statements. As such, auditors have securities law liability for material misstatements or omissions in a company's financial

in assessing and fixing the problem. It will be easier to disprove if the executive board has documented evidence of an attempt to fix the problem. Executive management that *is* attempting to solve its Year 2000 problems should thoroughly document its efforts to protect itself from legal actions.

Faulty financial reporting will be an easier charge to substantiate as there are Generally Accepted Accounting Principles (GAAP) and securities laws that govern and regulate this area. If a company fails to disclose relevant Year 2000 information on appropriate financial reports and subsequently fails or is damaged, federal and state securities laws will be the basis for shareholder lawsuits against the executive board. While technically the CEO is only as liable as other officers, the officers will be able to use the CEO as a defense if, in fact, he or she has not informed the board of relevant risks.

To be on the safe side, executive boards should demand immediate action on Year 2000 issues and disclose the company's exposure to shareholders and external auditors for financial and SEC reporting, even if the size of the exposure is unknown. Such executive disclosure will become even more important if Directors and Officers (D&O) insurance policies begin to exclude Year 2000 litigation (see related sidebar), thus increasing the chances of the directors and officers becoming personally liable for Year 2000 debacles.

The CIO and IT Managers

The Year 2000 problem is primarily in the domain of the CIO. The IT organization is most affected by the problem and is responsible for fixing it. So, as systems begin to fail and the company begins to suffer financially, senior executives may attempt to blame the CIO or IT management. The CIO will be the most likely scapegoat, and certainly the correct scapegoat if he or she has neglected the issue.

While CIOs are not generally legally liable (unless they are officers of the company or their behavior was criminal in nature), they should protect their present and future employment by: (1) directing Year 2000 conversions efforts in order to ensure compliance and (2) acting as a liaison between the Year 2000 project office and the executive board. The CIO must keep the executive board informed of all Year 2000-related activities and risks. Further, the CIO should meticulously document and disclose all conversion and awareness efforts. Those CIOs that cannot get internal approval for Year 2000 projects should alert executive boards directly to protect themselves from future blame. CIOs may well end up as the plaintiff's star witness in shareholder legal proceedings [.8p].

In addition, CIOs should work with legal staff to determine which vendors, outsourcers, and service providers are liable and therefore obligated to contribute to the Year 2000 effort. In this role, CIOs can be instrumental in recouping losses incurred from Year 2000 problems as well as in ensuring that contracts with Year 2000 service providers are

reports. To protect themselves against shareholder and executive board litigation, external auditors will begin to require Year 2000 disclosure from their clients in order to limit their liability [.8p]. They will begin to insist on conducting their own assessments or reviewing one from a Year 2000 specialist. Directors and officers should make sure these assessments are as accurate as possible to protect the company and avoid violating securities laws.

If an auditor is concerned that the company, against its recommendation, fails to note a potential Year 2000 hazard according to SFAS 5 in its financial reports, it may include a qualified opinion which states that reports are all accurate except that the possible effects of the Year 2000 problem have not been included or covered. This again will put the directors of the company at risk, especially if the auditors recommended such a disclosure and the organization objected.

foolproof. The second Planning Assumption in this pair, "Year 2000 Legal Issues: Vendor Contracts and Liabilities" deals specifically with these issues.

Accounting Standards and Securities Laws

The SEC has yet to specifically require Year 2000-related disclosure in financial reports. However, certain disclosure requirements already exist to which Year 2000 exposures, if large enough, are subject. The Financial Accounting Standards Board (FASB) already requires that companies disclose in a note to the financial report any contingencies that may reasonably occur that may be detrimental to the business (see sidebar, "FASB's SFAS 5").

Furthermore, federal securities laws require that public companies include a similar disclosure in the annual 10-K reports that they are obligated to file with the SEC. Every 10-K report must include a section called Management's Discussion and Analysis of Financial Condition and Results of Operations (MD&A). This section is for declaring and explaining material events and uncertainties known to the company that might impact the company's future financial condition or operations. This includes expenditures that would significantly impact future operations (e.g., Year 2000 costs), but that have not had an impact in the past.

Recommendations and Findings

Legal issues relative to the Year 2000 problem are still in their infancy, and precedents will not be set before 1998 [.8p]. However, securities laws are already established and will govern some types of Year 2000 litigation.

The basis for shareholder complaints will be devaluation of their investment due to deficient or non-existent Year 2000 efforts causing business interruptions, damages, or failures and/or incorrect or misleading financial reporting that omits Year 2000-related costs.

Accountability will be an issue at all levels within the organization, while legal liability will primarily be an issue for the directors and officers of a company, including the CEO, the CFO, and, in some instances, the CIO [.8p].

CEOs or officers that are made aware of the Year 2000 problem but refuse to allocate budget or take action will be held liable for the damage to the corporation [.9p]. Even if Directors and Officers (D&O) insurance exists, the company would have to be able to produce documentation showing efforts to remedy the situation in order for the company to be covered.

Due to the likelihood and copiousness of Year 2000 litigation, insurance firms will start to exclude Year 2000 litigation from D&O insurance policies--making it possible for a company's officers to be personally liable for such litigation [.7p]. Some firms may offer a separate Year 2000 D&O policy, but it will be extremely expensive and candidate companies will be vigorously qualified before they are underwritten.

CIOs will generally only be liable for Year 2000 disasters if they are officers of the company or if their behavior toward the issues could be construed as criminal (e.g., attempting to cause the business to fail). However, CIOs that neglected Year 2000 issues risk their present and future employment [.9p].

Giga Recommends:

Shareholders should demand Year 2000-compliance information from the executive board in order to protect their investment before it is too late.

Executive boards should demand Year 2000 compliance information and *action* from the CEO and CIO if necessary.

CIOs and IT managers should assess their Year 2000 exposure, document it, and disclose it to the CEO, as well as to the executive board.

Directors and officers should examine their existing D&O policy to make sure that they are covered for Year 2000 litigation costs.

CIOs and IT managers should examine the liability of existing vendors

Other Giga Research

PA, I-96-00029, "Are You Ready for the Year 2000?" Stephanie Moore

PA, I-96-00047, "Using Systems Integrators for Year 2000 Conversions," Liz Barnett and Stephanie Moore

PA, P-96-00061, "Automated Solutions for Year 2000 Conversions," Stephanie Moore

PA, C-96-00039, "CA's Legacy Becomes Year 2000 Business," Stephanie Moore

PA, I-96-00056, "Setting Priorities for Year 2000 Consultants," Stephanie Moore and Liz Barnett

PA, C-96-09075, "Let Data Dimensions Plan Your Year 2000 Projects," Stephanie Moore

PA, I-96-09098, "Do Not Underestimate End-User Computing Year 2000 Issues," Stephanie Moore

PA, I-96-10106, "FASB's Ruling Is a Year 2000 Call to Action," Stephanie Moore

PA, I-96-10114, "Year 2000 Vendor Management Is Critical," Stephanie Moore

PA, I-96-10110, "The Year 2000 Project Office," Liz Barnett

PA, I-96-10107, "Estimating Year 2000 Projects," Liz Barnett

PA, I-96-12120, "Year 2000 Resources: The Third Wave," Stephanie Moore

Background Articles

"Legal Issues Concerning the Year 2000 'Millennium Bug,'" The Year 2000 homepage, http://www.year2000.com

and service providers in order to recoup some of the costs of the Year 2000 project.

GIGA
copyright
Gartner Group

Planning Assumption
Year 2000 Legal Issues: Executive-Level Accountability
Stephanie Moore
12/27/96 Ver: 1 Doc. No.: I-96-12130

PA FORUM
SUBMIT INQUIRY
SAVE PDF FILE
PDF HELP
SEARCH

Mrs. MORELLA. Thank you very much, Ms. Coffou. I'd like to now turn to Mr. Peraino.

Ms. Coffou kind of frightened us, so let's see what you can do.

STATEMENT OF MR. VITO C. PERAINO, ATTORNEY, HANCOCK ROTHERT & BUNSHOFT, LOS ANGELES, CALIFORNIA

Mr. PERAINO. We'll keep the good news rolling here with my testimony. Thank you, Ms. Chairwoman, and you, Mr. Chairman, and the members of the Committee, for asking me to testify today.

My name is Vito Peraino. I'm an attorney with the California law firm of Hancock, Rothert, and Bunshoft. I'm a trial lawyer who has represented business entities in catastrophe litigation.

Over the years, I have been a lawyer in billion dollar cases that have gone to trial. I've been involved in environmental litigation, the S&L crisis, securities litigation, asbestos litigation, and other major areas of litigation.

I raise these points to say that I know a litigation catastrophe when I see one. For better or for worse, the Year 2000 problem is a litigation catastrophe waiting to happen.

Equally important, it is a catastrophe to which most companies and most lawyers are completely blind. Hancock, Rothert, and Bunshoft is one of maybe three firms in the country dedicating assets to addressing the legal aspects of this problem. That's far too few.

I hope my comments today help to start raising awareness on the legal aspects of the problem. I think to understand the legal threat posed by the Year 2000 problem, one has to appreciate what I think is the most serious aspect of the problem.

At its most basic level, the Year 2000 problem threatens the integrity of financial information. It does so because so much financial information is date-dependent.

Leaving aside the social and political ramifications of that statement, a threat to the integrity of financial data presents significant, and, I believe, potentially staggering liability exposures for companies. I'd like to highlight for you today, five main points about legal problems associated with the Year 2000 bug.

After outlining these points, I'd like to offer a couple of suggestions where I think we may be able to take some action to limit the potential litigation catastrophe. Those five points are as follows:

Number one, companies that don't solve this problem in time are certain targets of mass suits that will threaten the viability of their organizations. Doing nothing is not an option from a legal perspective.

Number two, directors and officers will face particularly close scrutiny and the potential of mass shareholder class action litigation for failing to act.

Number three, if the litigation hits because of a significant Year 2000 problem, it's going to hit like a fireball. It's going to be fast, it's going to be pervasive, and it's going to come from all directions.

Number four, companies that installed non-compliant software, or which provided software consulting services will face potentially significant liability exposure, because their conduct will be examined.

Number five, the potential liability associated with the embedded chip issue we just heard about is under-reported and potentially an avenue of mass product liability exposure.

As I said, doing nothing is not an option. A company's first order of business is to service its customers. And when we turn to any sector of industry, be it utilities, telecommunications, insurance, banking, we know that a company that cannot fulfill its obligations to its customers isn't likely to stay in business very long. And from a legal perspective, they are almost nearly certain to be sued.

Let me turn in detail to the problem that directors and officers face. For publicly traded companies, directors and officers are going to face particularly close scrutiny.

The first challenge they're going to face is whether they need to disclose the costs that their company will incur for fixing the Year 2000 problem. It will turn on the determination of whether the cost is, quote/unquote, material, and turn on the factors set forth in Financial Accounting Board Rule 5.

Of course, what is material is going to vary from company to company, but I can say this, directors and officers who do not disclose material information will face shareholder class action litigation. This is a dangerous problem.

In my work, I do a lot of speaking on the Year 2000 circuit, and I have had the opportunity to come across literally thousands of dedicated IS professionals who are attempting to raise management's awareness. But far too many report a similar story, and that story is, management just won't listen.

Part of it is an education problem, a view that the problem can't be real. Part of it is a funding problem, that there just aren't enough dollars in what's already a tight budget for many companies.

Part of it is just old fashioned denial. If we ignore the problem long enough, it will go away.

But for companies that fall into this category, they're going to be sued and their directors and officers will face liability. I believe the problem may be even deeper.

A company must produce an audited, certified financial statement in order to trade on a regulated exchange. Going back to my premise, the Year 2000 problem, I believe, threatens the integrity of financial information because so much financial information in a financial statement is date-dependent.

Take a two or three financial statement and you think of accounts receivable figures, notes payable, lease obligations, debt figures. If a company's computers cannot assemble a financial statement that can withstand audit scrutiny, their ability to trade on a regulated exchange will be undermined, and their credit rating will degrade.

Speaking as a lawyer, this is a profound legal risk. Many people believe that litigation risk is still far off. It's still 3 years away. This is dead wrong.

Leaving aside the fact that companies are already experiencing Year 2000 failures, scores of companies are incurring fund today to fix their problems. Some of these companies are looking to sue those who advised them to put in their non-compliant systems.

Because the statute of limitations is running on these claims, because damages are being incurred today, I anticipate that these claims will begin to be filed very soon. These claims will raise interesting and largely unresolved issues of law.

What is the standard of care owed by a computer consultant? What was the state of the art?

If there was a state of the art, when was it no longer the state of the art to use a 2-digit date code? Will consulting contracts prove to have warranted their ability to address this problem, or will they have enforceable warranty disclaimers? These and other issues are going to consume the courts.

Turning to the embedded chip problem, as I said, I think one of the least publicized and most legally significant aspects of the Year 2000 problem is the embedded chip problem. As you know, this problem arises from the fact that microchips that have hard coded date logic are incorporated into larger products that we use today.

And we've heard about how date-sensitive chips are incorporated in things like security systems and heating and air conditioning systems and communications equipment. For the manufacturers of these goods and for the manufacturers of these chips, product liability suits will be in their future.

Businesses need to be aware of these problems, and to assure that their mission-critical devices will operate at the turn of the century. Manufacturers need to be up-front and disclose whether they have a date-related problem, and to state what they intend to do about it.

What can Congress do? The Year 2000 problem will become a litigation fire storm unless this problem comes out of the corporate closet and is dealt with affirmatively. One step that I believe Congress should consider is to mandate that all sizable companies disclose publicly, their Year 2000 problem and their plan to fix it.

We recommend that Congress require companies to disclose three broad categories of information. Number one, whether they have undertaken a Year 2000 assessment, and if the company has undertaken an assessment, what is their plan to fix it? What is their time table for completion, and what will it cost?

Number three, if they haven't undertaken an assessment, when do they intend to begin it? These simple disclosures, I think, will have several beneficial effects.

It will bring public pressure to bear on companies to address the problem. It will allow consumers and businesses to make informed decisions about which companies to do business with. It will bring market forces to bear against companies that are not addressing the problem.

Finally, it will give Congress a tool to use to cut through some of the mythology that surrounds the Year 2000 problem, and to gain a better sense of how critical sectors of our economy are addressing the problem.

Congress can also help regarding the accounting for these costs. Currently, FASB's Emerging Issues Task Force has indicated that the Year 2000 costs must be taken in the year incurred, rather than allowing companies to amortize the costs over a longer period of time.

Because so much of these costs will be back-loaded to 1998 and 1999, due to the fact that companies are taking their time addressing the issue, Congress may wish to consider giving these companies an option of spreading those costs over a longer period of time to avoid attendant bottom line impact.

Finally, I believe Congress should consider creating an independent body to assure that critical sectors of industry are responding to the Year 2000 challenge. The UK has created a Task Force 2000 which has done a remarkable job of raising private sector awareness in a short period of time.

There is no similar singular spokesman in this country who is tasked with galvanizing the private sector to action. This will help with the number one problem, which is, doing nothing is not an option. Getting companies to step up and take action is the best medicine to avoid litigation.

In closing, as I said, I believe the Year 2000 problem may present the biggest litigation wave our country has ever seen. Prudent companies are acting now to take steps to avoid liabilities; others will fail to act and will be sued.

I hope I've been able to raise a little bit of awareness on the legal aspects of the problem. I'll be happy to answer any questions members of the Committee may have for me.

[The prepared statement of Mr. Peraino follows:]

WRITTEN STATEMENT OF VITO C. PERAINO

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY AND THE SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION AND TECHNOLOGY

U.S. HOUSE OF REPRESENTATIVES

MARCH 20, 1997

I'd like to thank you Mr. Chairman and Ms. Chairwoman for asking me to testify today on this important topic.

My name is Vito Peraino and I am an attorney with the California firm of Hancock Rothert & Bunshoft. I am a trial lawyer who has represented corporations and business entities in catastrophe litigation. Over the years I have been a lawyer in billion dollar cases that have been tried to verdict. I have been involved in environmental litigation, asbestos litigation, insurance coverage litigation, the s & l crisis and several other areas of major litigation. I raise these points to say that I know a litigation catastrophe when I see one; and, for better or for worse, it is my view that the Year 2000 problem is a litigation catastrophe waiting to happen. Equally important, it is a catastrophe to which most companies and most lawyers are completely blind. Hancock Rothert & Bunshoft is one of maybe three firms in the country that are dedicated to addressing the legal issues associated with the Year 2000 problem. I hope that my comments today help raise awareness in the legal community regarding just a few of the many legal issues presented by the Year 2000 problem.

As you have heard from the Gartner Group, the worldwide cost of the Year 2000 problem is estimated to be $300 billion to $600 billion exclusive of litigation costs. In the history of mankind, there has never been a $300 billion to $600 billion dollar problem that has not attracted significant legal attention. Some might say that there has never been a $300 to $600 problem that hasn't attracted significant legal attention.

To understand the legal threat posed by the Year 2000 problem, one must appreciate the most serious aspect of the problem. At its most basic level, the Year 2000 problem threatens the integrity of financial information. Let me say that again. At its most basic level, the Year 2000 problem threatens the integrity of financial information. It does so because so much financial information is date dependent. Our

system of contract law, the basis of our securities law, the premise of accounting and the functioning of federally regulated businesses all are premised to a significant degree on the fact that accurate and reliable financial information underlies transactions.

Remember that computers were first introduced to our businesses to alleviate the repetitive and costly accounting functions that consumed thousands of man hours. Billing, collection, payroll, tax calculations and the construction of a general ledger and financial statement all left the realm of manual calculation, and were automated in the 60's and into the 70's. These functions all rely on date dependent calculations and form the backbone of most computerized financial applications for companies. Leaving aside the political and social ramifications of the problem, a threat to the integrity of financial information presents significant and potentially staggering liability exposures.

I would like to highlight for you today five main points about the legal problems associated with the Year 2000 bug. After outlining these points, I would like to offer some suggestions for helping to lessen the litigation impact.

1. Companies that do not solve this problem in time are certain targets of mass suits that will threaten the viability of the organization. Doing nothing is not an option.

2. Directors and officers face particular scrutiny and the potential of shareholder class action litigation.

3. If the litigation hits because of significant Year 2000 failures, it will hit like a fireball—fast and pervasive.

4. Companies that installed non compliant software or which provided software consulting services potentially face significant liability exposure.

5. The potential liability associated with the imbedded chip issues is under-reported and potentially an avenue of massive liability.

DOING NOTHING IS NOT AN OPTION

When companies wake up on January 1, 2000 the first order of business will be to service their customers. No matter what sector of industry we imagine—utilities, telecommunications, banking, transportation, securities, insurance, retailing—a company that cannot fulfill its obligations to its customers is not likely to stay in business very long. From a legal perspective, they also are nearly certain to be sued. Let me give one example. A bank that cannot open because of a Year 2000 failure could face huge liabilities. A bank needs to track a customers deposits; it needs to service loans; it needs to track payments and receipts; it needs to clear checks; it needs to maintain trust accounts; and, it needs to report to state and federal regulators. Let's consider how my business—a law firm—might be affected by a Year 2000 bank failure. Hancock Rothert & Bunshoft needs access to funds to pay our employees. We need to pay our vendors. We need a credit facility. We need to have our clients' settlement checks cleared to pay litigants. We need to maintain trust accounts or we can be sued and we can be disciplined by the State Bar of California. If my bank can't open for several weeks, our firm is out of business. We will sue and we are no different than millions of other businesses in the Country.

But the problem isn't limited to banks and it isn't limited to law firms. It pervades virtually every sector of our Country and every business sector in the World.

But even companies that do the right thing by fixing their Year 2000 problem may not be protected from litigation. To the extent that we rely on other institutions to perform critical services for our business, we may still face liability. As I just pointed out, I need to assure my clients that monies maintained in trust are segregated and accounted for. The Year 2000 problem poses a liability problem not only for companies that fail to address their Year 2000 problem, but also for companies that fix their problem if their trading partners fail. Even if my internal Year 2000 problem is fixed, if our bank fails us, our firm will be sued. This is a problem for every business.

This problem will take the form of mass breach of contract actions, consumer fraud actions and in some instances, mass tort actions. In certain instances, they may even give rise to criminal liability.

DIRECTORS AND OFFICERS FACE PARTICULAR SCRUTINY

Moving to the realm of publicly traded companies, directors and officers will face close scrutiny for their handling of Year 2000 risks. The first challenge they face is whether to disclose the Year 2000 costs that their company will incur. This will turn on a determination of whether the cost is "material" and will turn on the factors set forth in FASB 5. Of course what is "material" will vary from company to

company. Directors and officers who do not disclose "material" Year 2000 costs will face shareholder class actions.

This problem is a dangerous one. In my work on the Year 2000 speaking circuit I come across thousands of dedicated IS professionals who are attempting to raise their management's awareness on this problem. Far too many report a similar story: management just won't listen. Part of it is an education problem—a view that the problem can't be real. Part of it is a funding problem—a view that the problem is too expensive to fit into an already tight budget. Part of it is old fashioned denial—a view that if the problem is ignored long enough it will go away. For companies that fall into this category, they will face directors and officers liability. Shareholders and customers will sue.

The problem may be deeper, though. A company must produce an audited certified financial statement with the Securities and Exchange Commission and must maintain accurate financial records in order to trade on a regulated exchange. Going back to my premise, the Year 2000 problem undermines the integrity of financial information. So much of a financial statement is based on date related calculations—accounts receivable, notes payable, lease obligations, debt reporting, inventory calculations, tax obligations. As one traverses a financial statement, it is readily apparent that date based calculations form many of its essential elements. If a company's computers cannot produce a financial statement that can withstand audit scrutiny, their ability to trade will be undermined and their credit rating will degrade. Speaking as a lawyer, this is a legal risk that is profound.

Directors and officers may have duties that go beyond their internal operations. Under a recent decision in Delaware, a board may have an affirmative duty to investigate problems presented to the company. This may obligate directors and officers not only to ferret out their Year 2000 problem, but also to assure that their trading partners are compliant. This may place an affirmative obligation on boards to assure that essential services will remain intact—e.g., banking, insurance, securities trading, etc.

Accordingly, boards of directors should insist that three activities are undertaken to protect their companies. First, they must undertake a comprehensive assessment of information services. This must receive the backing of the highest corporate officers and directors. Second, they must audit outside service providers to assure that essential services will be maintained through the turn of the Century. Finally, they should undertake an internal legal audit to assure that proactive steps are underway to avoid liability as well as to assure that all avenues of cost recovery are being aggressively pursued.

A LITIGATION FIREBALL

Because the Year 2000 problem is so pervasive and affects virtually every sector of our economy, if the litigation hits, it will hit like a fireball. It will hit several industries and it will come from all directions.

Today, March 20, 1997, the overwhelming majority of attorneys remain completely unaware of the legal implications of the Year 2000 problem. That will not last. Suits will be filed by consumers and businesses alike. Too much money is being spent for a basic computer error for it not to generate disputes that will end up in court. If companies think that the cost of the Year 2000 fix is expensive, they haven't begun to consider the cost of Year 2000 litigation.

Considering the likelihood of litigation, companies need to undertake steps in anticipation of litigation to assure that their operations will not be unduly disrupted by the inevitable suits. Several steps can be taken to inoculate the company against certain suits and to protect information developed to help avoid litigation.

CONSULTANTS WILL FACE RIGOROUS SCRUTINY

Many people believe that the litigation risk is still three years off. This is dead wrong. Leaving aside the fact that companies are already experiencing Year 2000 failures, scores of companies are incurring funds today to fix their problem. Some of these companies are looking to sue those who advised them to put in their non-compliant systems. Because the statute of limitations is running on these claims, I anticipate that these claims will begin to be filed soon. These claims raise several interesting and largely unresolved issues of law. What is the standard of care that is owed by a computer consultant? Was there a state of the art? If there was, when was it no longer the state of the art to use two digit date fields? Will consulting contracts prove to have addressed this problem, to have warranted software's performance, or will it have enforceable warranty disclaimers?

The issue of warranties and disclaimers will be a central issue. Two points require emphasis. First, implied warranties often supplant written warranties and provide

a basis for businesses—and the government—to claim against consultants that may have caused the problem to exist. These particulars of the enforceability of such warranties varies from state to state. Second, it must be remembered that warranty disclaimers are disfavored in the law. Technical requirements regarding the placement of warranty disclaimers and the wording of such disclaimers are essential to enforceability. Any ambiguity in the disclaimer is likely to be construed against the drafter of the document. Accordingly, the enforceability of disclaimers may consume courts facing this problem.

THE IMBEDDED CHIP PROBLEM

One of the least publicized and most legally significant aspects of the Year 2000 problem is the imbedded chip problem. As you know, this problem arises from the fact that microchips that have hard coded date logic reside as a component of many products which we use today. There are reports that date sensitive chips will fail in certain elevator systems, security systems, heating and air conditioning systems, automobiles, communication equipment, waste water treatment facilities, the global positioning system and many other devices that permeate our lives. Do we want supertankers navigating our shoreline with a global positioning system that will not function? Do we want 911 systems to operate in the case of emergency? For the manufacturers of these goods and for the manufacturers of these chips, products liability suits may well be in their future. Businesses need to be aware of these problems and to assure that their mission critical devices will operate at the turn of the Century. Manufacturers need to be up front and disclose whether they have a date related problem and to state what they intend to do about it.

The products liability issues may turn on the question of whether there is actual damage to property or bodily injury. Typically, there is no relief in the law of products liability for economic injury alone. However, many states' consumer protection laws and consumer fraud laws supplant the common law of products liability to give consumers a remedy in these instances. Furthermore, courts will be tempted to stretch the definition of "property damage" to provide an avenue of relief should the Year 2000 problem become as disruptive as its potential suggests.

WHAT CAN CONGRESS DO?

The Year 2000 problem will become a litigation firestorm unless this problem comes out of the corporate closet and is dealt with affirmatively. One step that Congress should consider is to mandate that all sizable companies disclose publicly their Year 2000 problem and their plan to fix it. We recommend that Congress require companies to disclose three broad categories of information: 1. Whether they have undertaken a Year 2000 assessment. 2. If they have, what is their plan to fix the problem, what is their timetable for compliance and what will it cost. 3. If they have not, when do they intend to begin such assessment.

These simple disclosures will have several beneficial effects. It will bring public pressure to bear on companies to address their problem. It will allow consumers and businesses to make informed decisions about which companies to do business with. It will bring market forces to bear against companies that are not addressing their problems. Finally, it will give Congress a tool to use to cut through some of the mythology that surrounds the Year 2000 problem and to obtain a better sense regarding how critical sectors of industry are addressing the problem.

Congress can also provide help regarding accounting for these costs. Currently, FASB's Emerging Issues Task Force has indicated that Year 2000 costs must be taken in the Year incurred, rather than allowing companies to amortize the cost. Because so much of the costs will be backloaded to 1998 and 1999, the accounting impact will be most pronounced in those years, with attendant bottom line impact. Congress may wish to consider giving companies the option of spreading those costs over a longer period of time.

Finally, Congress should consider creating an independent body to assure that critical sectors of industry are responding to the Year 2000 challenge. We might consider taking a page from the book of Parliament. The UK has created Task Force 2000 which is charged with raising awareness in British Industry. The United Kingdom's Robin Guenier has effectively used the power of his bully pulpit to cajole industry to action. While Britain probably remains behind the U.S. in its response to the Year 2000 problem, it has made remarkable progress in a short period of time. No similar singular spokesperson exists in our Country to galvanize the private sector to action. We recommend that the Task Force be comprised of a spokesperson and high ranking executives from each sector of industry and that the body be tasked to report to these committees regarding each industries' Year 2000 effort.

In closing, the Year 2000 problem may present the biggest litigation wave our Country has ever seen. Prudent companies are acting now to take steps to avoid liabilities. Others will fail to act and will be sued. My comments today are meant to highlight a handful of the problems we have seen. I urge companies to consider their risk and to adopt a proactive strategy to solve the problem and to avoid liability. I urge Congress to adopt the modest measures I have outlined to prod industry to action and to help avoid a storm of litigation.

I would be happy to answer any of your questions.

YEAR 2000 CURRICULUM VITAE OF VITO C. PERAINO, ESQ.

Mr. Peraino has been a partner at Hancock Rothert & Bunshoft since 1989, when he founded the firm's Los Angeles office. Mr. Peraino has practiced law since 1981 and has specialized in complex commercial and insurance litigation. In addition to chairing the firm's Year 2000 Working Group, Mr. Peraino chairs the firm's technology committee.

Mr. Peraino joined Hancock Rothert & Bunshoft in 1984 in their San Francisco office. He has tried to verdict some of the largest cases in California history and has lectured widely on complex case management and trial techniques.

Mr. Peraino has spoken widely on the Year 2000 problem. He has addressed the Electronic Banking Economics Society of New York, the DCI Issues and Answers Conference on Year 2000 Problems in Chicago, the Data Processing Management Association, Underwriters at Lloyds, London, the Orange County CIO Organization and the Bank Administration Institute. He is currently scheduled to address the San Francisco Chapter of the Risk Insurance Management Society, the International Municipal Lawyers Association, the California Bankers Association, the 45th Annual Corporate Accounting and Financial Reporting Institute, GIGA World and the DCI Year 2000 conferences in Toronto, Phoenix and Boston.

Mr. Peraino also has published articles on the Year 2000 crisis in Director's Monthly, the Daily Journal, National Underwriter, Underwriter's Report, Bankers' Review, Bank News, Bank Securities Journal and other publications. He will be published in several upcoming publications. He has been quoted as a Year 2000 legal authority in the Washington Post, the Los Angeles Business Journal, the Los Angeles Daily News, the BNA Banking Law Reporter and many other publications.

Mr. Peraino is a graduate of the University of Michigan Law School.

Mrs. MORELLA. You certainly have, Mr. Peraino. I can just see this as a kind of an economic boom for lawyers.

But it's really very serious. I'd like to recognize, also, having joined us for a while, Mr. Sessions from Texas, is here, and Mr. Sununu from New Hampshire.

Now, Mr. Miller.

STATEMENT OF MR. HARRIS MILLER, PRESIDENT, INFORMATION TECHNOLOGY ASSOCIATION OF AMERICA, ARLINGTON, VIRGINIA, ACCOMPANIED BY MR. MARC A. PEARL, GENERAL COUNSEL AND VICE PRESIDENT

Mr. MILLER. Thank you, Chairwoman Morella, and Chairman Horn. I'm Harris Miller, President of the Information Technology Association of America, representing approximately 11,000 information technology companies from around the country.

I'm accompanied by Mr. Marc Pearl, who is ITAA's General Counsel and Vice President for Government Affairs.

Our association applauds the leadership of Chairwoman Morella and Chairman Horn on the Year 2000 issue. The challenge we face in the coming years is enormous, a challenge which, frankly, was not helped by the Administration's failure to set a strong, positive example for the Nation and the world.

The Office of Management and Budget's recent estimate of $2.3 billion for federal-wide Y2K fixes fails to pass the laugh test. A

clear signal that even now our government has not made this issue a top priority.

Today, I've been asked to testify about ITAA's Year 2000 certification program called ITAA*2000. I'm delighted to do so, because we have a very positive story to tell.

Let me give you some brief background. When we set this program up last year, our goals were threefold: First, to give the marketplace a mechanism to identify the best-of-breed companies in addressing the Year 2000 issue; secondly, to respond to a growing sense of concern within agencies, and a viewpoint articulated by the government Interagency Working Group, that IT companies themselves are not doing enough to respond to the Y2K concerns of their customers; thirdly, to take a proactive, industry-based stance on the Year 2000 issue, in response to a request made by Congressman Horn in the first Congressional hearing in April, 1996.

We developed the ITAA*2000 Program last summer in conjunction with the Software Productivity Consortium of Herndon, Virginia, an organization with great expertise in software process improvement. They provide the technical manpower to staff our program.

We conducted a pilot to get the bugs out of our program last summer, and publicly announced the program October 1, 1996. The program has begun to achieve critical mass.

Today, 11 organizations have received certification. IBM's AS400, S390, and TPF Business Units; IBS conversions, Cap Gemini, NCR, CACI, Into2000, Objective, Inc., BDM, and Lawson Software. And we'll announce another certification tomorrow.

Another 18 companies are currently undergoing technical evaluation, with most of those expected to be completed in the next few weeks. Several other companies have told us they will be submitting completed applications in the next few days.

In total, 189 companies have requested a questionnaire necessary to become certified. The program requires all applicants to respond to an in-depth technical questionnaire, provide extensive backup documentation and respond to followup questions from the software engineers at SPC.

The focus of the program is on the processes and methods that organizations use to develop Year 2000 compliant software and services. As the list of our certified companies indicates, applicants can be information technology companies, but we have designed the program to apply to any company, organization, government agency, or any entity involved in a Y2K conversion.

The certification can involve organizations which sell products or services commercially, but is of equal interest and value to those developing systems for their own internal use. It provides an independent, third party review of their Y2K processes and methods.

Our thinking is, if you get the processes and methods right on the front end, you dramatically reduce the chance of failure down the road. This concept of reviewing processes and methods is similar to the International Standard Organization 9000 process, ISO9000, which is widely used in our industry.

I will confess, this is not a perfect program. We've heard from some potential customers of Y2K services and products who say,

because the program does not test software, per se, in every environment in which they use it, it fails to meet their needs.

We understand and respect their point of view, but we believe there is still a substantial value in a program which provides an independent analysis of processes and methods.

The fact that IT industry leaders such as IBM, NCR, Cap Gemini and others have been certified and endorse our program, speaks volumes. Moreover, members of the Subcommittee, no single industry program could hold itself out as the ultimate arbiter of Year 2000 compliance.

There are simply too many platforms, systems, languages, interfaces, and other date-dependencies to check, and not enough time. Every organization's computing environment is sui generis. Attempting to recreate such environments on a customer-by-customer basis is just a bridge too far.

The complexity and multiplicity of environment interfaces is one reason we so strongly emphasize the need for testing of any Year 2000 conversion. The Year 2000 so-called solution that works very well in one computing environment may not work well in another environment.

It simply would be impossible for our program to test even a limited set of software products in all possible environments and interface situations. Speaking as an IT industry executive, I feel proud that IT has stepped up to the Year 2000 certification challenge.

It is just one of our many initiatives, including seminars, a directory, a buyers guide, and a weekly Internet-based newsletter. I recently presided over a series of Y2K seminars in the Peoples Republic of China, and had an excellent opportunity to brief Chinese Government officials and business executives about this critical issue.

I was very pleased that one of the companies that joined me in the Chinese seminar presentation proudly displayed its certification insignia, indicating it places great value on the program.

I've given similar education seminars around the country and around the world, including Singapore, Canada, France, and Spain. Next week I will travel to Brazil.

I also serve as President of the World Information Technology and Services Alliance, which consists of 25 IT associations around the world. My colleague who heads the UK association is currently drafting a Y2K white paper that we will adopt in May and then present to global leaders and organizations such as the OECD and European Union, to ask them also to rise to the Year 2000 challenge.

We are meeting also with many organizations in the customer markets, such as banking and the securities industry, and we will be briefing a group which includes the Big Three auto makers. I am particularly gratified that the State of Texas has selected to make ITAA*2000 a source selection criteria for its IT solution providers.

The Commonwealth of Virginia cited our program in a recent Y2K Request for Proposal. We have also briefed many Federal Government officials about our program, including people at the General Services Administration, SSA, and the Department of Defense.

We hope that one day federal agencies will ask for the ITAA*2000 label when buying Year 2000 products or services. The program continues to grow and offer important benefits to certified organizations. It enables commercial companies to set themselves apart from the competition by making a strong, positive statement about their Year 2000 readiness.

It allows customers to distinguish among many vendors offering them products and services, and it permits organizations to validate their own internal Year 2000 conversion process. We also hope it will help companies mitigate risk by demonstrating that they took appropriate steps to deal with this unprecedented situation.

Thank you very much. I'd be happy to respond to any questions.

[The prepared statement of Mr. Miller follows:]

STATEMENT OF HARRIS N. MILLER

PRESIDENT, INFORMATION TECHNOLOGY ASSOCIATION OF AMERICA (ITAA)

SUBMITTED TO THE SUBCOMMITTEE ON TECHNOLOGY AND THE SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION AND TECHNOLOGY

U.S. HOUSE OF REPRESENTATIVES

ON YEAR 2000 RISKS: WHAT ARE THE CONSEQUENCES OF TECHNOLOGY FAILURE?

MARCH 20, 1997

Good afternoon. I am Harris Miller, president of the Information Technology Association of America, representing 11,000 direct and affiliate member companies in the information technology (IT) industry. ITAA members are the marketplace leaders in a host of critical IT areas, including product and custom software, telecommunications, Internet, systems integration, and outsourcing.

Chairwoman Morella, Chairman Horn and other distinguished members of the Subcommittee, ITAA applauds your outstanding leadership on the Year 2000 issue. The challenge we face in coming to terms with this issue is enormous—a challenge not helped by the Administration's failure to set a strong positive example for the nation and the world. The Office of Management and Budget's (OMB) recent estimate of $2.3 billion for federal Y2K fixes fails to pass the laugh test, a clear signal that even now our government has not made this correction a top priority.

Today I have been asked to testify about ITAA's Year 2000 certification program, called ITAA*2000. I am delighted to do so, because we have a very positive story to tell. Let me begin with some brief background.

ITAA has been engaged for several years to educate governments at all level, the private sector, and the international community about the actions necessary to address the Year 2000 and the very real risks of inaction. Last year, our Year 2000 Task Force approved the idea of a Year 2000 certification program. Our goals were three fold:

- To give the marketplace a mechanism to identify the "best of breed" companies in addressing the Year 2000 issue
- To respond to a growing sense of concern within federal agencies and a viewpoint articulated by the Interagency Working Group that IT companies are not doing enough to respond to the Y2K compliance concerns of their customers
- And to take a proactive, industry-based stance on the Year 2000 issue, partially in response to a request made by Congressman Horn in the first Congressional hearing on this issue in April, 1996.

We developed the ITAA*2000 program last summer in conjunction with the Software Productivity Consortium (SPC) of Herndon, VA, an organization with great expertise in software process improvement. The Consortium provides the technical manpower to staff the program. We conducted a pilot to "get the bugs" out in August and September, and publicly announced the program on October 1, 1996.

The program has begun to achieve critical mass. Today eleven organizations have received Certification: IBM's AS/400, S/390 and TPF business units, IBS Conversions, Cap Gemini Transmillennium Services, NCR Professional Services, CACI, Into2000, Objective, Inc., BDM and Lawson Software. We have another 16 compa-

nies currently undergoing technical evaluation, and the SPC expects to complete most of those reviews by the end of March. Several other companies have informed us they expect to submit completed applications in the next ten days.

One hundred and eighty-five companies have requested the questionnaire necessary to submit to become certified. We are somewhat puzzled why more completed questionnaires have not yet been submitted. Let me hazard some guesses. First, the applications process is rigorous, perhaps more rigorous than some companies are willing to go through. Completed applications are often several inches thick. We do not issue these certifications lightly. Perhaps some organizations start the process assuming it will be pro forma, and have second thoughts when they realize the challenge of becoming certified.

Secondly, many companies are extremely busy talking to or servicing potential or actual Y2K customers. They simply may not have adequate staff and time to complete the questionnaire, or it may just inadvertently fall to the bottom of the "to do" list. We have talked to many companies which have assured us they are poised to submit their applications, yet do not do so, probably because of time pressure.

Our program requires applicants to respond to an in-depth technical questionnaire, provide extensive documentation, and respond to follow-up questions. Our focus is on the processes and methods that organizations use to develop Year 2000 compliant software. As the list of certified companies indicates, applicants can be information technology companies. But more generally, we have designed this program to apply to any company, government agency or other entity involved in Y2K conversion. The certification can involve organizations which sell products or services commercially; it can be of equal interest to those developing systems for internal use only. The certification process provides an independent, third-party review of Y2K processes and methods. Our thinking is that if you get the processes and methods right on the front end, you dramatically reduce the chances of failure down the road. This concept of reviewing processes and methods is similar to the ISO 9000 process, widely used in our industry.

This is not a perfect program. We have heard from some potential customers of Y2K services and products who say that because the ITAA*2000 program does not test software *per se* in every environment in which they use it, it fails to meet their needs. We understand their point of view, but we believe that there is still substantial value in a program which provides an independent analysis of processes and methods. The fact that industry leaders such as IBM, NCR, Cap Gemini, and others have been certified and endorse our program speaks volumes.

Moreover, no single industry program could hold itself out as the ultimate arbiter of Year 2000 compliance. There are simply too many platforms, systems, languages, interfaces and other date dependencies to check—and not enough time. Every organization's computing environment is *sui generis*. Attempting to recreate such environments on a customer by customer basis is just a bridge too far. The complexity and multiplicity of environments and interfaces is one reason we emphasize so strongly in our general presentations on the Year 2000 that the most time consuming and important element of the conversion process is the testing phase. A Y2K "solution" that works very well in one computing environment may not work well at all in another environment. It simply would be impossible for us or any organization to test even a limited set of software products in all possible environments and interface situations.

Speaking as an IT industry executive, I feel proud that ITAA has stepped up to the Year 2000 certification challenge. ITAA*2000 is one of several Year 2000 initiatives we have underway, including seminars, a Year 2000 directory, buyer's guide, and weekly Internet-based newsletter. We have been very active in trying to get other industries and industry groups informed about the Y2K challenge and to embrace the ITAA*2000 program. I recently presided over a series of Y2K seminars in the People's Republic of China and had an excellent opportunity to brief Chinese government officials and business executives about this critical issue. I was very pleased that one of the companies that joined me in the China seminar presentations proudly displayed and discussed its Certification insignia, indicating it places great value on the program. I have given similar educational seminars across the country and around the world, including Singapore, Canada, France and Spain. Next week, I will take our Year 2000 message to an industry meeting in Brazil.

I also serve as President of the World Information Technology and Services Alliance (WITSA), comprising 25 IT associations from around the world. My colleague who heads the UK association is currently drafting a Y2K white paper that WITSA will adopt in May as policy calling for an increased global focus on the Year 2000 challenge. ITAA also is talking to several of our global sister associations which are interested in implementing the Certification program in their countries.

Closer to home, our past Y2K discussions have included U.S. trade organizations representing the banking and securities industries. We will be briefing the ITAA*2000 program to a group which includes the Big Three auto makers later this month. I am particularly gratified that the state of Texas has elected to make ITAA*2000 a source selection criteria for its IT solution providers. The Commonwealth of Virginia cited our program in a recent Y2K request for proposal (RFP). We have also briefed many federal government officials about our program, including officials from the General Services Administration (GSA), Social Security Administration (SSA), and the Department of Defense (DoD), as well as the government-wide Y2K task force. We hope that one day federal agencies will ask for the "ITAA*2000" label when buying Year-2000 products or services.

The ITAA*2000 program continues to grow and to offer important benefits to certified organizations. Today, the program enables commercial companies to set themselves apart from the competition by making a strong positive statement about their Year 2000 readiness. It allows customers to distinguish among the many vendors offering them products and services. It permits organizations to validate their own internal Year 2000 conversion processes. Tomorrow, ITAA*2000 certification program will help companies of all types mitigate risk by conclusively demonstrating that they took appropriate steps to deal with this unprecedented situation.

Thank you very much. I will be happy to respond to any questions you have about my testimony.

Mrs. MORELLA. Thank you, Mr. Miller. Mr. Pearl, you are here on a consulting basis, okay, great, good. We've also been joined by Ms. Rivers from Michigan.

I'm going to turn now for questioning to Chairman Horn.

Mr. HORN. Thank you very much, Madam Chairwoman. Mr. Miller, I congratulate you and your fine organization on taking an idea and putting it into implementation. I must say that idea got worked on faster than a lot of the ideas I give my other 434 colleagues. [Laughter.]

So maybe you should be the Congress for a week. We thank you for what I called originally the "Good Housekeeping Seal of Approval."

Mr. Hall, I can't help but ask you and remind you of the testimony of the Gartner Associates. The estimate was that this was a $600 billion world-wide problem. We have half the computers, so it's a $300 billion domestic United States problem, and it is a $30 billion federal problem.

As you know, the Administration in its budget has said it's a $2.3 billion problem, and when we had General Paige over before us, who handles communications matters in the Pentagon, he noted that they hadn't even begun really going down the highway to solve all the problems. And $1 billion of that $2.3 billion estimate is from the Pentagon.

My guess is, we've got a $5-10 billion federal problem. We'll never know till the end, and anything we estimate now just always multiply it by three, and that will be about where the Federal Government comes out.

So, I'm just curious. Have you got any new numbers you'd like to give us? Do we have any new numbers that Gartner might be thinking of that gives us some feel for what the magnitude of the problem is?

Mr. HALL. Well, I'd like to first respond and say that all the bets that I made that would be the first question, I'm going to go collect on. [Laughter.]

I thank you for illuminating the history and background of the $30 billion number. I think it's a number that has been used, and in many cases, abused.

I'd like to first clarify the $600 billion number. There is actually a range in that prediction. It's $300-600 billion.

That's our prediction. And we arrived at that, based on a survey that was taken earlier in the decade on the total lines of code that exist in the commercial world.

And that came out to be about 250 billion lines of code, commercially. And the number for COBOL stands at somewhere in the range of 180 billion. Just to give a sense of people thinking about getting into the remediation business, there's plenty to do.

From there, we extrapolated what it's going to take to do a Year 2000 project, and then added in the tremendous wild card of government. That 250 billion does not include the public sector anywhere in the world.

So we arrive at the $300-600 billion, and from there we can extrapolate down to the $30 billion number, which really, by rights, ought to be then expressed as a $15-30 billion number in that kind of range, given that thinking.

But the reality is, and I think you alluded to it, is that I can guarantee one thing about any number that anybody says today and it will be wrong.

Mr. HORN. Yes.

Mr. HALL. And the reason I say that is that I will go back to the analogy I drew in my opening statement of this old house scenario. If we imagine a street with 27 houses that need to be remodeled, you know, that is the Federal Government.

And we are standing across the street with the homeowner, and in this case, several contractors who are all weighing in on what we anticipate to be the cost of remodeling this house. And we've yet to ascertain the square footage. We've yet to understand even how many rooms there are, or even how extensive the modeling job needs to be to achieve minimum requirements.

And we're standing across the street trying to make predictions. And sure enough, there's an argument between the contractor and the homeowner. And the homeowner doesn't think it's going to cost as much, and the contractor thinks it's going to cost a tremendous amount, and so forth.

And as soon as we take our first walk through the house, I would align that with the concept of inventory, meaning as soon as we collect and understand the size and breadth of the systems to be repaired, we can apply some industry standard metrics to that.

We've published some numbers to that effect at $1.10 per line of code, which is on its way up because the labor will be going up, as well as 100,000 lines of code anticipated for a work year. So you can use that number.

Mr. HORN. That's very helpful. It seems to me the unit here is the lines of code and the labor cost of dealing with the line of code.

Mr. HALL. That's right.

Mr. HORN. Frankly, the Administration never convinced me that they even asked for the lines of code. I don't know. Maybe you've got better information.

Mr. HALL. No, I don't. In fact, few of the agencies are prepared to deliver that number at this point. They are in the midst of collecting it, which is the logical first step to the process.

Mr. HORN. Sure.

Let me move to want I want to regard as the major information I'm interested in. Much of the attention, as we all know now, with this problem is centered on computer software used by older mainframe computers.

The testimony, of course, of Mrs. Coffou and Mr. Peraino suggests we need to become a lot more worried about microchips and these small little chips that act as electronic brains controlling so many everyday products in our lives, such as VCRs and telephones.

Ms. Coffou, I wonder, how can people or organizations know if they are using products with date-sensitive embedded chips, and whether those products have the potential for failure in the Year 2000?

How does one go about dealing with that?

Ms. COFFOU. Well, as I had said, guilty until proven innocent needs to be the way that is initially approached. Things like televisions and, let's say, fax machines, microwaves, those kinds of things, you can test on your own, where you can take and advance the date on there. Have it roll over.

Many, many people have done this, and unfortunately, the results have not been very promising. Several people that I know that did this with fax machines, the results ranged from the machine backing off and resetting itself at 1980. Other machines have just given up the ghost and stopped, and they could not be restarted.

The same thing with microwave ovens, interestingly enough. A number of people that I know of that restarted their microwaves and moved the dates ahead, they were unable to bring the microwave back to life at all, wound up taking it into the repair shop where the whole circuit board within the machine had to be replaced.

So, it's things like that you need to do to just take a look and see what's going to happen. I would recommend for the general public to start putting the pressure on manufacturers. Call and find out. Ask questions.

A friend of mine just recently went to buy a camera that has the automatic dating feature that puts the date on the pictures so that you know when you took it. She asked the question, what happens if I buy this camera and it has this warranty on it, what happens when this goes past the Year 2000? Will this still work?

There was no answer. She was not given an answer. She said they at the store did not know how to respond, so she called the manufacturer, and the manufacturer could not respond, as well.

You start looking at so many people that buy extended warranties on their appliances, and are we selling appliances and equipment that are supposedly warranted to keep working? Now, are we marketing falsely? Should the FTC be involved in something like this as well?

A number of questions need to be asked. Above all else, we need to start putting the pressure on the manufacturers.

Mr. HORN. You're creating plenty of work for Mr. Peraino, and I'm sure this whole area—one more thought to my friends in the Information Technology Association of America. You might want to think about a 900 number which would generate a little money. [Laughter.]

For people that don't want to wreck their refrigerator, their fax machine, and all the rest of it, of course, you might have the trial lawyers who would have you in court the next day. But you know that's your problem.

Let me ask the last question I have, and that is: Mr. Peraino, you suggested that there are likely to be substantial numbers of product liability cases resulting from these problems. If you could just elaborate on the types of cases that may emerge?

It seems to me that the sky is unlimited here. Give me an example that the average citizen we talked about in that last exchange—and we've talked about what the directors and officers' liability is in making the information known.

What else can you speculate on?

Mr. PERAINO. The products liability area really is—the mind kind of reels, because there are a lot of examples of potential exposure. Let me give you some things that I have heard in my travels on Year 2000.

I was told that there was one municipal agency that discovered that they had an embedded chip that ran the waste water treatment plant for the city. And it was an old chip. It was a 286 chip, and every so often, the waste water has to be moved in order to assure that it's properly aerated.

And it's eventually discharged back into a bay. I was told that chip was discovered to be non-compliant, and had they not discovered it, raw sewage would have been discharged into the local bay area.

That's an example of a product liability failure. On the one hand, it's an example of how that can snowball into actual physical damage and injury to citizens and people in the area.

We hear reports that there are problems with the Global Positioning System. I shudder to think about supertankers navigating in and out of major ports, unable to utilize the Global Positioning System as part of their navigation controls.

We've heard reports that there may be problems in everything ranging, as I said, from security systems to 911 systems, to communications systems. So there are a lot of ways that the problem can arise.

Again, a lot of this isn't hard data, because a lot of this is underreported, and manufacturers, I think, simply are not aware that they may have a problem on their hands.

Mr. HORN. That's all I have. I'm sure we've got plenty of talent here. They've got a million questions.

Mrs. MORELLA. Absolutely. I'd just ask a couple of questions, and then turn it over to my colleagues for any questioning they may have.

Ms. Coffou, it almost sounds like, from what you said, a slogan from Brave New World would be appropriate, and that is, ending is better than mending. And I'm just wondering, is this kind of like an easy solution to so many of those products that we have around the house, just plan to get rid of them before January 1, 2000?

Would that not be less expensive, quite seriously?

Ms. COFFOU. For the individual consumer, it could very well be. However, to think about ending your relationship with you programmable thermostat within your house, that's part and parcel of

the whole infrastructure of your home, it could be a very, very pricey situation, indeed, different from replacing your microwave oven type of a thing, your camera, your digital watch.

Quite frankly, I think planned obsolescence is something that many manufacturers are certainly hoping is going to happen. The problem is that there continuing to manufacture new products that still are not compliant.

Mrs. MORELLA. What should we do about that? That just seems so frustrating to think that people could buy new thermostats that should last 15 or 20 years.

Should we be doing something about that?

Ms. COFFOU. I think we should definitely be doing something about that. As I said, I think we need to be making the manufacturers wake up, send a call to action out to them to wake up and step up to this entire situation.

If you try as a private citizen myself, calling and researching this, and trying to talk to manufacturers, they won't even talk to me. I believe it's going to take some movement from the government to bring this issue up to the level at which it needs to be before appropriate action is taken.

Mrs. MORELLA. You don't think this would be unnecessary government interference into business? Should it be done by a business entity?

Ms. COFFOU. I honestly think it needs to be done through the government. Awareness programs need to be put together.

Mrs. MORELLA. Mr. Peraino, on the same line, you mentioned that you thought that we should require that there be disclosure by companies.

Again, do you see Congress requiring that? Would you explain? Could that be done reasonably?

Mr. PERAINO. Let me respond to that. I think it can be done reasonably, and I think it can be done simply.

And I think Congress can do that. Part of the problem is, right now companies are left to a decision about whether to disclose this, based on an assessment of whether the problem is material or not.

Because the problem is so pervasive, and because the problem can affect the way a company operates, I think we need to take that judgment call out of the hands of the companies, and put it as an absolute requirement that everybody step forward and make a statement about what they're going to do.

The reason I think that's important is because it will force companies who currently aren't looking at the issue, to take a look at their systems, take a look at their internal structures, and make the assessment. Half the battle is realizing you have the problem.

Once that's done, we can make all sorts of, I think, intelligent decisions about how we might proceed from that point forward. But right now, companies simply aren't making those disclosures in a universal way.

Mrs. MORELLA. Thank you.

Mr. Hall, is there—what would result if you have a compliant computer or whatever it might be, connect with one that is not? Is that a big fiasco?

Mr. HALL. It could be, absolutely. I think a way to look at that is in the concept of a transaction. If we think about the notion of,

say, going to your automated teller machine to get money. Okay, there is, in fact, a computer staring at you right as you do your work locally.

There are chips within that machine that take in your card and figure out whether or not your card has expired. That is actually done locally, and there are banks that are going to have to replace their teller machines, because they don't know what to do with the card that says 00.

They're going to have to either swap out the board or replace the entire machine, and that's not a trivial amount of money. From there, is connected to some mid-range system that's probably either local to the bank, or regional, which processes that information and then sends it on to some mainframe somewhere for that bank.

Then the bank sends it on to VISA who says, is it okay to give this money? And you see how the chain is all connected.

And when we talk about making our systems compliant, you know, we think about a virtual organization, because we have to deal with these transactions from cradle to grave, and if the transaction fails at any point, we don't get our money.

And the transaction fails and it's no good to us. So, absolutely, you know.

And when we talk about a compliance certification, and when we talk to clients about defining what certification means, we talk about upstream and downstream interfaces for systems, and how do they connect together, both to outside organizations and within systems within our own organization.

Unless we provide compliance all the way through, the transaction drops. What I mean by that is, it will either deliver you the wrong amount of money, or it will give you no money, neither of which are very attractive options, unless, of course, it's too much money, in which case, maybe——

Mrs. MORELLA. You factored that into your speculation of your fiscal amount?

Mr. HALL. We factored that in actually in a couple of ways. When we've laid out the project plan, you know, for the Year 2000, which a lot of organizations have adopted, we first lay out a project management percentage of that plan at 25 percent, which is very high.

If you look at the average project, it uses only about 8 to 10 percent of the resources of the project for project management, and we've raised that dramatically for precisely this reason. The fact that you've got interconnectivity of all these systems that you have to worry about, and the fact that you have such high change volumes in a typical system that you'll have to worry about.

And it's also reflected in testing. If you look at testing the systems—and I think it was alluded to earlier—you're talking about something like half the effort in trying to initiate testing for these systems. And it's challenging, not just because you have the connectivity, you have to see if the transaction will work.

But you have to see if the transaction will work in multiple time dimensions. You have to see that you didn't break it today, that it will still work when you reenact it. You have to make sure that it works as you go through the time horizon.

The failure that I discussed, when does it first break in time, like January 1, 1999, and then 2000, 2001? So you have to repeat these tests through time, and it's very, very difficult.

And there's mention of Wall Street-wide tests to actually do financial tests in future time dimensions of transactions as they move around the Street, and in other places.

Mrs. MORELLA. Mr. Miller, are you frustrated that more companies aren't looking towards certification or aren't aware?

Mr. MILLER. The certification program is only one element. Our frustration is a more general frustration about the failure to deal with the Year 2000. I just received some data yesterday from Dr. Howard Rubin, who is with Hunter College of the City University of New York, and a well known expert on this Year 2000 issue.

His survey last year, 1996, showed that only 11 percent of the companies he surveyed had completed a full fledged strategy. So he went out and did the survey again, and his initial results for 1997 shows that percentage has jumped to a whopping 13 percent. So that's of great concern.

I'd like to address and perhaps respond to the question you directed to Mr. Peraino a few minutes ago, and give a slightly different perspective.

We believe that, number one, the top priority must be the government using its role as a bully pulpit. I agree with what Mr. Peraino said about what's happening in the United Kingdom, where the United Kingdom government has taken a very vocal lead, just in the last few weeks.

For example, they sent a letter to all 156,000 publicly traded companies in the UK, indicating that this was a high priority for the country and for every one of the industries in the country. I think that would have about as much impact as any law that this Congress tried to pass.

Certainly, if the government stepped up to the real numbers to fix the Year 2000 problem that Congressman Horn and Mr. Hall discussed a few minutes ago, I think that would send a signal. Secondly, we would suggest that there are already a tremendous number of powers that the Securities and Exchange Commission has regarding publicly traded companies, and Mr. Peraino discussed some of those implicitly in his testimony.

We believe those should be used, as, for example, the Office of the Comptroller of the Currency already has sent a letter to all the banks. It did this several months ago, telling them they must be compliant.

Similarly, we believe the SEC could notify all publicly traded companies that this is a critical issue in terms of their public disclosure to their shareholders and stockholders.

Another example is the insurance industry. It is a very heavily regulated industry in our country already. The insurance industry, not just in terms of their use of the Year 2000 solutions for their own computers, but as an insurer of businesses, they could play a critical role in getting companies to pay more attention.

Their regulators should be looking to them to ask, are you really insuring companies, understanding the liability they have on these issues? That would be a spur to get more companies to get active.

Another set of existing laws and regulations that are relevant for both federal and, more primarily, state agencies are those that regulate things like consumer fraud. To go back to the questions you were discussing with Ms. Coffou, one could argue that if one sells a product that doesn't work beyond a couple of years, that is a form of consumer fraud. States should be using the existing state consumer fraud laws to move against companies.

What I am suggesting is that there are already a lot of statutory mechanisms out there to convince the business community to respond. Coupled with the bully pulpit of the Congress and the President of the United States, these would have a major impact in getting this issue much more aggressively dealt with in this country.

Mrs. MORELLA. Mr. Horn.

Mr. HORN. Madam Chairwoman, I got convinced about 40 minutes ago with Mr. Peraino's testimony that we ought to be doing something.

I think you've given an excellent list in this area. I told the Chairwoman we'd be glad to have our joint staffs explore those and put in the necessary legislation or write letters with all members of the Committees signing it—I think this is a nonpartisan thing—to the various regulatory authorities that already have the power to alert people.

Just as you noted, I think it takes a combination. I remember my hearings with the government officials. I have been upset at the lack of leadership in the Executive Branch on this. I think they are finally getting the message, but it's just a matter, as you say, of educating people.

Britain has a lot less firms than we do, and you've got to assume that a lot of people have never heard of the problem. We found that when we surveyed Cabinet officers, two of them had never heard of it.

Yet we learned one year later that one of the two had been pioneers in one of the divisions way down in that bureaucracy from which the current Secretary comes, and just had never escalated to the top. And I think that's true in a lot of firms.

They might well be working at it, but nobody's got a focus on it.

Mrs. MORELLA. Thank you, Mr. Horn. I wanted to also have included in the record, a letter that was sent to Chairman Alan Greenspan and a number of other people who are, for instance, the FDIC Chairman, Director of the Office of Thrift Supervision, National Credit Union Administration, the Department of Treasury, and SEC by Chairman D'Amato in the Senate and Bob Bennett in the Senate, both chairing separate Committees, asking for the response to whether or not people have been advised what they're doing, again, the kind of thing you mentioned that we should do with companies—have companies do, a disclosure about what their plans, time table, and costs would be.

[The letter referred to follows:]

UNITED STATES SENATE,
COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS,
Washington, DC 20510–6075, February 27, 1997.

Alan Greenspan,
Chairman,
Board of Governors of the Federal Reserve System,
20th St. and Constitution Ave., NW,
Washington DC 20551

Dear Chairman Greenspan:

The Committee on Banking, Housing, and Urban Affairs is concerned about the so-called "Year 2000 Problem." This problem will arise in those computer systems that employ only two digits to represent the year when processing date information. On January 1, 2000, such systems will reset the year to "00," which in many cases will be misinterpreted to mean "1900" or another incorrect date. This pervasive error could severely damage the wide range of accounting and management operations that lie under the control of these computer systems. As a result, the "Year 2000 Problem" may pose a serious threat both to the federal agencies and regulatory bodies under the Committee's jurisdiction, and to depository institutions and the financial services industry in general.

The U.S. Office of Management and Budget is working with Federal agencies to assist them in their own Year 2000 preparations; however, the status of efforts among financial institutions and organizations regulated by federal agencies is not clear. Experts believe that solutions to the Year 2000 Problem will be time-consuming and costly, yet will become far more difficult and costly as January 1, 2000 approaches. Experts also strongly recommend that reprogramming be completed before December 31, 1998, in order to allow a full year for system testing. Therefore, every institution should already have efforts under way to (1) assess the scope of the problem by identifying and prioritizing vulnerable computer systems, (2) develop a plan for action, including a timetable for completion of work, and (3) implement solutions by fixing computer code and testing the new systems.

We therefore ask that you respond to the following questions regarding your oversight of Year 2000 preparations in the institutions that you regulate:

(1) Have you prepared an overall plan for ensuring Year 2000 compliance in the institutions that you regulate? What are the elements of this plan?

(2) Have you advised senior executives of the regulated institutions of their need to initiate and fully support Year 2000 preparations?

(3) What procedures or systems have you put in place to ensure that all of these institutions (or the vendors that supply their data processing services or equipment):

(a) Have begun an inventory of computer systems that may be affected?

(b) Have developed, or are developing, a plan for making essential repairs?

(c) Are on a schedule to complete planned reprogramming before December 31, 1998?

(4) If you are including Year 2000 issues within your regular examinations of these institutions, is the timing of the examinations adequate in all cases to ensure a vigorous Year 2000 effort in which essential reprogramming will be complete before December 31, 1998?

(5) Have you prepared an overall assessment of the general status of Year 2000 efforts among these institutions? If so, please provide a copy of this assessment.

(6) If no such assessment exists,

(a) Is such an assessment under way, and when do you expect completion?

(b) Do you currently perceive a high degree of awareness and preparation for the Year 2000 Problem in these institutions?

(c) How great is the risk that some will not achieve Year 2000 compliance on a satisfactory schedule? Are some types of institutions at particularly high risk?

(e) Are you aware of any special obstacles that interfere with or preclude industry readiness for 2000?

(7) Who within your agency is responsible for oversight of the Year 2000 preparations of the regulated institutions?

It would be most helpful to this Committee if you could provide your responses to these questions by March 21, 1997. Please direct any questions regarding this matter to Steve Hagen on our staff at (202) 224-7391.

Sincerely yours,

ALFONSE M. D'AMATO, *Chairman*

ROBERT F. BENNETT, *Chairman,*
Subcommittee on Financial Services and Technology

RECIPIENTS OF YEAR 2000 LETTER, SIGNED BY CHAIRMAN D'AMATO & SEN. BENNETT

Alan Greenspan,
Chairman,
Board of Governors of the Federal Reserve System,
20th St. and Constitution Ave., NW,
Washington DC 20551

Ricki T. Helfer,
Chairman,
Board of Directors,
Federal Deposit Insurance Corporation,
550 Seventeenth St. NW,
Washington DC 20429

Nicolas P. Retsinas,
Director,
Office of Thrift Supervision,
1700 G St. NW,
Washington DC 20552

Norman E. D'Amours,
Chairman,
National Credit Union Administration,
1775 Duke St.,
Alexandria VA 22314-3428

Eugene A. Ludwig,
Comptroller of the Currency,
Office of the Comptroller of the Currency,
Department of the Treasury,
250 E. St. SW,
Washington DC 20219

Arthur Levitt,
Chairman,
Securities and Exchange Commission,
450 Fifth St. NW,
Washington DC 20549

Mrs. MORELLA. And we will follow through as Chairman Horn has said. I notice that we have been joined by Mr. Ewing from Illinois. But I now wanted to turn to this side and recognize Mr. Davis for any questions that he may have.

Mr. DAVIS of Illinois. Thank you very much.

Mr. Peraino, in listening to your testimony, I gather that you are projecting that in all probability, there is going to be a flurry of lawsuits, lots of legal action, and that our judicial system will not have had experience with these kinds of lawsuits to some degree, is that correct?

Mr. PERAINO. Factually, that's correct. We've never had a Year 2000 type problem arise before. The actual context, the legal principles, of course, will be based on legal principles that we're all familiar with.

But factually and technically, our courts haven't seen something like this on a mass scale.

Mr. DAVIS of Illinois. Then I guess it would have impact. I mean, we could project that not only will we be impacted in terms of the

technical systems, but also impacted in terms of the judiciary and the legal system.

I guess my question is, is there a way to perhaps forestall or prevent the occurrence of this?

Mr. PERAINO. I've tried to give some thought to that, and tried to give some thought to steps that might be taken to simply limit or eliminate litigation altogether. I have to tell you that, in all honesty, I can't come up with anything that I think could pass constitutional muster or in any way be realistic in terms of such a massive limitation.

The problem is that these lawsuits have the potential of arising in so many different ways, from so many different sectors, under so many different legal theories, that it's very difficult to put limits on it. But I think you are correct in pointing out that we can anticipate it's going to put a strain on the judicial system, both in terms of the number of lawsuits.

There are projections that there will be a significant bankruptcy rate that will result from companies that simply fail, due to the costs involved, which, of course, will put a strain on the bankruptcy court system as well.

Mr. DAVIS of Illinois. I guess this particular question, another member of the panel could perhaps address it. Are we suggesting that there is a tremendous amount of need for us, our government, now, to place more emphasis in this area to try and not only be ready to meet the crisis, but to try and get ahead of it, perhaps a little bit?

Mr. PERAINO. If I can just make one quick comment on that?

I think the Committees are to be commended for what they've done with the Federal Government by hauling people before the Committee and asking them to commit as to their timeframe, the cost, and what they plan to do.

I would encourage you to think about ways in which you can do the same thing with the private sector, and assure that the critical sectors of our economy, the critical sectors of our business, are addressing the issue, and that they are having that same sort of accountability, public accountability.

And I think that will avoid a lot of litigation, and it will utilize your efforts as public figures, and utilize the bully pulpit that you have to prod industry to action, and to make a decision as to whether you need to do more than that.

Mr. MILLER. I would like to echo what the previous speaker said, but also emphasize that one of the fundamental challenges we find—and this was referred in some of the other testimony—is getting people at the top of companies to understand this issue.

The technical people know about the issue and have understood it very well. What they can't seem to do is get their bosses or get their CFOs or get the COOs to understand that this is a fundamental business problem.

This isn't an IT issue. This is a question of whether you stay in business. Or if you're a government agency, this is a basic issue of whether you can continue to deliver the service.

I would suggest, Congressman Davis, that CEOs in your Congressional District will listen to you a lot quicker than they'll listen to their IT people. And if you and your colleagues go out and ad-

dress this issue in public fora, you will get their attention in a way that no matter how competent the information technology manager in a company may be, won't get their attention. If a Member of Congress says, this is an important issue and we expect business leaders in your Congressional District and in the 434 other Districts to pay attention to this, I think that would send a wonderful message to the business leaders of this country.

That's fundamentally what the UK government has done by putting the bully pulpit in motion and using the tremendous respect that business leaders have for our political leadership as a way of working together to get the job done.

Mr. HALL. If I can just add to that, briefly, and echo it again?

We talked to the majority of the large organizations grappling with this problem, mostly at the project manager level. The organizations that are farthest along are the ones where senior managers are programmers, and they know what the issue is.

There is no translation of the risk here to business terms, and that's the challenge; is trying to achieve that translation. Until we do that, we're facing never-ending frustration.

And the typical mechanisms of pushing back on a project, solving for the variable of cost, and all the time when we come back and we talk about what the Year 2000 will be, we're trying to solve for cost. And what we need to be solving for is time when the reality is, we don't have enough time left to finish, even if we devoted all the resources we had to it, even today.

And to further echo the comments, I think that there hasn't been—and all of us, I think, on the panel, and in the industry are watching for this—there hasn't been that one single global failure that has made headlines worldwide that says, here is the smoking Year 2000 gun. We haven't seen that yet.

And I think, you know, that would be the thing that would have hordes of people walking into banks and saying, you know, daily, please guarantee that my money is safe. And I think you will see that slowly accelerate.

We need that motivation. We need that external voice to provide the catalyst to get management out of the coma of denial that they are in, to get this moving.

Mr. DAVIS of Illinois. Thank you very much. I have no further questions.

Mrs. MORELLA. Thank you, good questioning, Mr. Davis. Now we turn to the distinguished Mr. Davis from Virginia.

Mr. DAVIS of Virginia. As opposed to the distinguished Mr. Davis from Illinois, I just want to put that on the record.

I see Mr. Pearl sitting here, and, Mr. Miller, I didn't want you to bring your General Counsel and not have him consult with us. So can I ask him questions? You're paying him by the hour, so I want to make him earn it.

Mr. PEARL. I wish. [Laughter.]

Mr. DAVIS of Virginia. I noticed recently in the UK that the new VISA cards had come out, that 10 percent of them were kicking out if they had the expiration date, 00, and they were having members certify or put up some money, that the cards would be compliant, members who were using it.

What I want to ask is, if you could explain to us the general legal liability standard for information technology vendors when they're products don't perform as anticipated, and what can their customers expect? Do you have any thought on that?

Mr. PEARL. This is not a tort issue. This is a contractual issue that we're dealing with in this particular situation.

First and foremost, it ultimately must rest, unlike a product liability issue that has been discussed here, in the IT arena, the ultimate responsibility rests with the user.

Mr. DAVIS of Virginia. What if somebody's credit is ruined because things are kicking out? That could be a tort issue, couldn't it?

Mr. PEARL. If you are the consumer using a particular card, that's where we're talking about in terms of the bully pulpit and the things that Ms. Coffou said, which is asking the questions. Whatever you are holding and dealing with in your life, be it your bank account, your credit cards, your drivers license, you need to ask: Are these things Year 2000 compliant?

And we haven't even gotten to the point of getting the users of our society to ask that question, simply picking up the phone and saying, will this work?

From a user standpoint, it is a contractual relationship that you are in. When you're using the computer, when you're using anything that is time-, date-, and data-sensitive. First of all, it is the awareness question from the liability questions.

In many respects, we're simply asking the questions from a liability standpoint in terms of, was an inventory in the first place even taken? Do you know what you're holding, as a business, as a consumer, as a customer, that is, in fact, time-, date-sensitive?

And what, in fact, has been identified as time-, date-sensitive, and how important it is to you? What action have you taken? Do you have a contract that's in force.

Part of what we're talking about, for example, a 286 chip at a waste treatment plant; is there a reasonable expectation that piece of equipment that you bought 20 years ago was supposed to last to and through the 21st Century?

Did you maintain a maintenance contract? Is that contract in force? Is there a reasonable expectation that, in fact, the product was going to last up and to and through that time?

So, the issues that we're looking at and the questions that we're asking are contractual questions that deal with the subject, not just what, in fact, who should the finger of blame be pointed at, but, in fact, who is asking the right questions?

Mr. DAVIS of Virginia. So the job opportunities have been increased for COBOL programmers for the next couple of years, and then after that, it looks like the lawyers will take charge.

Mr. PEARL. Our hope is that we won't.

Mr. DAVIS of Virginia. Unless something is done. Does anybody want to comment?

Mr. MILLER. To answer that question and Congressman Davis's question is, the way to mitigate the problem is to solve the problem. What we believe, Congressman Davis, is that it is in the best interest of both the IT industry vendors and their customers to solve the problem.

It is interesting. No disrespect to my colleague to my left here, but when I've done seminars across the country, and I've done probably several dozen at this point, the legal liability questions rarely come up, much less often than I would think. Most of the people attending those seminars seem to be interested in solving the problem, not pointing blame.

Interestingly enough, I had more questions in the eight seminars I did in China last week about liability than in the several dozen I have done in the United States. For some reason, the Chinese were fascinated with the issue of legal liability.

But in this country, I find both the vendors and the customers, whether they be private sector or people in government, asking how can we solve the problem? At the end of the day, a bank or an insurance company which can't deliver services because a Year 2000 problem arose is not going to be able to turn to its millions of customers and say, "We were so busy filing lawsuits to determine liability here, we forgot to fix the problem." That's not an answer.

Similarly, the vendors are not going to want to be in a situation where their customers see them as adversaries. So, it's mutual economic self interest which is driving people to solve this problem and not get hung up in the questions of liability at this point.

Not to say that the issues are not legitimate, but I don't see most people focusing on them because they're trying to solve the problem.

Mr. PERAINO. Just a couple of quick comments on that, so we're clear. I'm in no way suggesting that I advocate that litigation is the answer here; in fact, just the opposite.

I'd like to see steps be taken to avoid litigation. I do think we have to be realistic though. This much money, this many potential failures, there is no way that there isn't going to be a lot of litigation, if I can use several negatives in a sentence there.

In other words, it's inevitable. There's going to be litigation on this, and it's going to be pervasive.

In terms of how to avoid it, I think Mr. Pearl is quite right. This will oftentimes be a question of contract and implied warranty, but there will be some federal liability questions coming up.

There may even be potential criminal liability in certain instances.

Mr. DAVIS of Virginia. There are certainly going to be some political liability if we don't get this solved.

Mr. PERAINO. There may be political liability, but so far you can sue for that, I think.

Mr. DAVIS of Virginia. I just want to ask one other question.

In last month's hearing on the Year 2000 problem, I remember having a representative from the FAA here. It looks like we heard testimony that the FAA only began its Year 2000 efforts in July of last year.

The Chief Information Officer of the Department of Transportation only first learned of the Year 2K problem last August, and that the FAA still has not completed its assessment phase of the problem.

Any reaction about the risks the FAA and the general public would face? Does anyone want to comment on that?

Mr. PERAINO. From a liability perspective, the transportation industry really needs to take a hard look at what the potential liabilities are. From the FAA perspective, to assure that our air traffic systems are operating correctly, I think is a first critical component, not only to avoid a mass disaster, but to avoid significant economic dislocation if it's not able to operate.

Mr. MILLER. Of course this issue of transportation is truly a global issue. All of these transportation systems are interconnected, whether you're talking about reservations systems, whether you're talking about fees for landing at airports, whether you're talking about inspection processes for airplanes and related equipment, whether you're talking about interconnecting the air traffic control systems around the world.

I personally don't plan on flying anywhere on New Year's Eve of the Year 2000.

Mr. DAVIS of Virginia. Mr. Horn established, I think, in the last meeting, that he wasn't going to be on the first couple of planes out.

Mr. MILLER. Again, I hate to keep going back to my trip to China, but since I'm still on Chinese body time, we did have a very long meeting with the Minister of Aviation, and they are as far behind as the FAA. But I was very pleased that they actually sent a Minister, a very high ranking government official, to come to our presentation.

The Chinese clearly have now decided that this is a high priority issue. And China is very much a part of the global aviation system, and must also deal with its Year 2000 problems in its aviation system.

Mr. DAVIS of Virginia. Thank you. Just as a note, we talked to some of these groups celebrating the millennium who are planning on flying around the world so that they can, every hour, as it turns, they can be somewhere in a huge jumbo jet. If we don't get this fixed, they won't be able to land anywhere.

Thank you.

Mr. HALL. Congressman, may I respond to that point?

Mr. DAVIS of Virginia. Please.

Mr. HALL. You used the words earlier, they haven't even completed their assessment. I wanted to weigh in on that, because we talked to a lot of organizations about their project progress and how to think outside the box to get this done more quickly.

And our message to many of these organizations is, in fact, to bypass the assessment step for all practical purposes. What we heard from the other witnesses here, what are the key processes that the FAA needs to continue to do?

I mean, they need to continue to supply ATC. They need to continue to supply regulatory information and other kinds of systems to keep airplanes flying. I mean, this is not a hard thing to figure out.

We know these systems have to be remediated. We're not in a position to be able to readily replace them. We know they have to be repaired.

Why go through a 3-to-6-month or whatever time period you want to pick, assessment period for these things? We know they have to be fixed.

Let's get a crew, let's get them to work on the systems tomorrow, and begin the work. You know, there's enough public information published by Gartner and other organizations about methodologies, about tools, about remediation methods. Why are we doing an assessment?

Let's go through and get a crew to work on our most important systems. Let's use the metering of that work to see how productive they are, and use that to extrapolate and see what the rest of the project might be looking at. But let's get going.

Let's plan not to finish and remediate our most important systems first.

Ms. COFFOU. I'd like to just add that I don't want to be again the bearer of bad news, but the FAA is one piece of the puzzle. I have spent numerous days discussing the embedded chip issue with aerospace manufacturers, and, quite frankly, from the number of the companies that I have been working with, they're planning to do exactly what Bruce was saying here, with going—knowing that they have to fix their systems, what their biggest concern is right now are the embedded chips, the embedded systems that they can't follow the audit trail back very successfully as to who put those together, and how they put them together, how they've been programmed to absolutely, positively guarantee that they will not malfunction.

Mrs. MORELLA. We've been joined by Mr. McHale from Pennsylvania. Mr. McHale, did you want to question any of our testifiers?

Mr. MCHALE. Thank you, Madam Chairwoman. I apologize to you and the witnesses. I have just arrived in the room, so I'm confident that at least one or two of the questions that I was going to ask have been previously presented to you.

If that's the case, then a very brief answer will suffice. I'd like to follow up on what was just said a moment ago by Ms. Coffou.

With regard to the embedded chips, I received a briefing yesterday from an industry source on this issue, which, frankly, increased my awareness of that challenge, very substantially.

A few moments ago, Mr. Davis from Virginia raised the issue of FAA implications arising out of the Year 2000 challenge. What about the actual safe operation of aircraft and automobiles and elevators arising out of the use of embedded chips?

A moment ago, a reference was made to those who would celebrate the Millennium by flying around the globe. I guess my basic question is, beyond issue of controlling transportation vehicles, relating more specifically to the safe operation of those vehicles, do we have a problem in the Year 2000 in terms of the ability of the public to fly with safety and security on aircraft, commercial and private; the ability to get in an automobile and have security that it will function effectively and safely after the Year 2000 deadline is reached?

I am told that many elevators now have such embedded chips, and that those chips contain maintenance information that will cause those elevators to safely, I am told, go to ground level in wait of maintenance, if the chips are not modified before now, in the Year 2000.

Could you generally address that issue of safe operation of transportation vehicles?

Ms. COFFOU. Yes, the same type of chip mechanism that you alluded to in the elevator systems are very, very prevalent in a number of other types of products, such as airplanes, large ships.

You know that most automobiles now have very significant and sophisticated electronic systems within them. Everybody's probably had that little engine light come on in their car, those types of things.

Mr. MCHALE. Twice last week.

Ms. COFFOU. It's the same type of a situation. I can tell you from the aerospace manufacturers that I have been working with over the last few months, they're scared to death.

This presents a very, very significant threat to the health and well being of people all over the world. One mistake from an airline manufacturer can result in loss of life.

As Mr. Hall said, we really need to get a smoking gun perhaps to get the attention of the world to this problem. Hopefully it will not be a situation such as this that will be the smoking gun.

The issue is extremely important and it's an issue that is being addressed within, I know within the large aerospace manufacturers, as well as within the automobile manufacturers. They're not going to talk about it. They haven't been talking about it very openly. They are aware of it.

But it is definitely something that because of the proliferation of the products will affect everyone.

Mr. MCHALE. Any comments from other witnesses?

Mr. PERAINO. If I can make one comment on the point. I think those are fair comments and I think those are similar to the comments that I've heard. But it raises another question I think, which is that question probably is best addressed to people in the aerospace industry, the transportation industry, which I think kind of illustrates why we need some mechanism to get industry in front of a panel like this or a similar panel to assure that you're getting the kinds of information that's accurate, the kind of information from people that understand the problem in a very deep and technical way, not to diminish the comments being made here which I think, as again I said, are consistent with what I'm hearing from people in industry.

But I urge you to consider having some mechanism to assure that you're talking to people in the right industries.

Mr. MILLER. Mr. McHale, let me make an observation which I think addresses your question at a slightly more general level. A hundred years ago, if you turned on a light switch, people thought it was a wonderful thing. It was something new and different.

Over a period of time, electricity became something that we all began to expect. Now it's so fundamental to the operations of our everyday lives, if the electricity system went down tomorrow, it would shut down lots and lots of activities, including the operation of this hearing.

Electricity became part of everybody's life; therefore we expect it work all the time.

Over the last 20 years, information technology has become something that people have begun to expect as part of their lives. They

don't even think about the fact that there's more computing power in the average automobile than there was in Apollo 13.

The tremendous developments associated with the silicon chip and the ability to get software processing costs down means that information technology is ubiquitous, and people have come to expect it to be there all the time.

They have not realized that if there is a flaw in it, it affects everything. They include the items you mentioned, as well as the other items that have been detailed with the other witnesses.

That's the level of realization of the import of computers that we have to get people to understand.

Computers don't mean just the mainframe that you see in the movies. It's not just the PC on your desk. It is everyday life. It's part of everyday life.

And if you don't make sure that computers are taken care of across all these consumer and business products, then it's like losing electricity all of a sudden. It would be a disaster.

Mr. MCHALE. Let me ask an ethical, a question raising ethical and legal concerns that directly follows upon the statement that you made, Mr. Miller.

Recognizing that embedded chips are now used in a wide range of products and also recognizing that under foreseeable circumstances, the failure of a product to perform as originally intended can produce dangerous consequences for the user or consumer.

In light of the fact that these products are now on the market, that they are known to contain embedded chips that may fail or perhaps will fail when the Year 2000 deadline is reached and where it is foreseeable that the failure of that product to perform will endanger human life and certainly public safety.

Is there a duty to disclose that product, with a life expectancy known to be beyond the Year 2000 contains such an embedded chip? Is there a duty to disclose to the prospective consumer of that product that it contains such a chip, so that consumer can be forewarned of a possible failure.

Or are we in fact, in the alternative, without legal reservation, selling products without notice to consumers where it is foreseeable that the product may fail when the Year 2000 deadline is reached, particularly in the case of a product that, through its failure to perform as designed, would be unreasonably dangerous to a user or consumer?

I mean it's one thing where we would not anticipate that a failure of that product would produce an adverse effect on safety or life, but where it would be unreasonably dangerous in the event of a failure, is there a duty to disclose?

Mr. MILLER. I can't comment on the legal questions. I'll leave that up to the lawyers, Congressman.

But in terms of business practices, obviously a business person wants to treat the consumers and the customers in the most positive way, not just because of ethical but for business reasons.

You don't want to make airplanes that are going to crash. You don't want to make cars that aren't going to run. You don't want to make microwaves that are going to shut down. It's not just an ethical issue, it's a fundamental business issue.

You can't stay in business if you're producing products that the customers come to know don't work.

To use an example, any microwave manufacturer that had products out there on the market that Consumer Reports put in one of their issues that these will all fail in the Year 2000, you can be sure that manufacturer will suffer a big hit in the marketplace.

We think that's what really drives these decisions.

Mr. MCHALE. Could somebody address the issue? I truly don't know the answer to the question. This is not one of those questions where I know the anticipated answer or have an anticipated answer.

Is there a duty to disclose?

Mr. PERAINO. Maybe I can give you some insight from the legal perspective on that.

It's certainly fair to say that the hypothetical you've outlined raises a liability concern on behalf of the manufacturer of that product. It may turn on questions of what the state of the art was, whether it really was or was not foreseeable, the product would be used for 30 years or 20 years or 10 years, as the case may be.

And those are the kinds of questions that will be asked in a product liability lawsuit. Should that failure result in more than economic injury, in other words, should that failure result in an injury to a person or an injury to property.

So you're on the right track I think from the legal point of view in terms of outlining the potential liability and some of the issues that would arise.

Does that answer your question?

Mr. MCHALE. It does. I think what it says is that the ethical obligation to disclose, at least in my view, is clear. The legal liability that might arise for a failure to disclose is somewhat in doubt. But frankly, if I were advising a manufacturer under these kinds of circumstances, I would very clearly, in writing, warn that manufacturer that a failure to disclose a potential defect, where the defect would have consequences, adverse consequences to public safety and human life, I think a failure to disclose would raise enormous risks of potential liability.

Mr. PERAINO. I think that's right. And a prudent business would take steps, I'm sure, to address that issue responsibly.

Mr. MCHALE. Madam Chairwoman, I thank you.

Mrs. MORELLA. Thank you, Mr. McHale.

I would like to recognize the very patient Mr. Ehlers.

Mr. EHLERS. Thank you, Madam Chairwoman.

Mrs. MORELLA. And distinguished, of course.

Mr. EHLERS. Thank you. That's the kindest thing anyone has said about me in a long time. I must say, you're really a cheerful group. [Laughter.]

I think we should hand out Prozac the next time we have this panel here. It reminds me of the Prophet Jeremiah. You're in somewhat the same camp.

But I think it's important to remember the function of prophecy is not to predict the future, but to scare people so that they change their behavior, and I hope that you'll achieve that objective.

My first thought was to simply retire in the Year 2000. I'll be 65 then. It suddenly occurred to me, I won't be able to get my money

out of the bank, or my credit card won't work and my social security checks won't arrive. I have no choice but to continue.

The impression I get from the discussion you've given is that, much to my surprise, the government may be in better shape in dealing with the Year 2000 problem than the average business community or business organization.

Is that a correct perception or not?

Mr. HALL. From Gartner's perspective, I would say that's not the case. Indeed, you have to look at different business sectors to make that assessment.

Mr. EHLERS. Let me just add to that my next question, because I'm trying to pin down where the problem is in the business sector.

Is it the large corporation where the CEO is just too far out of touch with the CIO, or whoever might be in charge of information technology? Or is it the smaller business where they just don't know how to handle this? Or in between?

Can you give me some idea of what the spectrum might be?

Mr. HALL. Sure. Indeed, you made an excellent point when you talked about the relationship between the CEO and the CIO.

If you go to the typical large financial institution or financial intermediary, like a brokerage house, a bank, an insurance company, the technical systems, the computer systems drive the functioning of that organization and thus the CIO tends to carry tremendous weight in terms of business decisions.

They are typical organizations. They're at the forefront of technology. They always have the most powerful systems they're running. And in this case, the CIO typically understands the problem and has conveyed it in business terms to the CEO.

Now there are exceptions in every case here, and I can cite examples of insurance companies, banks, and brokerage houses that are way, way behind. But in general, you know, those organizations where the information processing is so central to their business that they simply wouldn't have a business without it are further along.

When you move into some of the other verticals, when you talk about telecommunications, when you talk about manufacturing, when you talk about some of the other verticals of care, other kinds of things, certainly information technology has helped them automate some key processes, and if they were to really be called to the carpet, they do in fact rely on these for their very survival.

But the treatment of those systems is not elevated to board level, if you will, you know. It is a cost center. It's something that is perceived to be economized, you know, something that we can, you know, we'll give them money if they really demand it and they can make a good enough case.

So there is a separation there.

I think in those organizations, there's a higher degree of frustration in trying to get moving.

When you move to the smaller organizations, it's interesting that you mentioned that, because most people think that unless you have a mainframe, you don't have a problem.

We've talked to a lot of organizations that have AS400s, the IBM platform mentioned earlier. We've talked to a lot of organizations

with client service systems that might be from Hewlett-Packard or from Sun or some of the other platforms.

These systems were in fact based on the same programming habit. It was never a standard, it's a habit and there's no date police running around to make sure that's been changed, as I think has been mentioned. They're created under the same premise.

So the awareness and the resources I would claim to resolve the problem in these smaller organizations is even more alarming than you see in some of the larger organizations.

And you typically get the reaction of well, I know that the manufacturer of the computer system will fix it for me when they have a lot of code that simply is not going to be fixed. And they haven't worried about the transaction or their relationships with other organizations and how they communicate with them.

So I think that all through the private sector, awareness continues to need to be increased.

And we talk about the bully pulpit and such. Then you get to government. And I think when you talk about government, you know, a couple of the mandates that have come down, one being no new funding, two being the general perception that what we're trying to do is solve this based on cost efficiency, which is what I sense when I look at OMB documents and other kinds of things, I just do not get the sense of urgency and the sense of capability to reallocate key resources to get this done.

And I'm talking not just about the U.S. Federal Government, I'm talking about many, many States, internationally, and so forth. I think the wheels of this kind of a catastrophe are moving much more slowly, in general, in the government community, and I would invite others on the panel to maybe weigh in on that.

Mr. MILLER. I would echo what Mr. Hall's saying, Mr. Ehlers. And I think another problem that the government has is the government procurement process. There's been some improvement in the procurement process but the government process is usually fairly slow and difficult. Whereas in a major corporation, maybe they wake up late to the Year 2000 problem, but once they wake up, they can throw a tremendous amount of resources into a problem very quickly. Either internal resources or outside vendors and consultants and software tools can be directed quickly at the problem.

And if a major bank or a major airline or a major telecommunications firm, the CEO says go do it, they'll go do it.

Obviously federal agencies are much more constrained in terms of financial resources, particularly with, as Mr. Hall said, this ridiculous notion that they can pay for it with existing resources. And there is the nature of the procurement process.

Also, just to go back to your Jeremiah issue at the beginning, I would note that ITAA publishes a weekly Year 2000 electronic newsletter that covers the issue in great depth. The newsletter author, Bob Cohen, my VP for Communications, is sitting right behind me. Every week we try to feature a success story, an organization that has tackled the Year 2000 problem and has either completed conversion or made great progress, we have featured about 10 of these success stories.

We're going to be compiling these because we want organizations to understand this is not an insurmountable problem. It's a question of commitment and will to deal basically with what is a management issue. Organizations big and small, government or private sector, should not be discouraged. They can do it. We try to outline ways that organizations have actually done it very successfully because we think that's an important part of the message too.

Ms. COFFOU. There's also another little difference, and it's actually quite a large difference when you really think it through, that I have seen, speaking with people in state governments as well as city governments, federal agencies in this country as well as in Europe.

That's the elected official that you do not have in the private sector. There seems to be a number of governmental bodies that have decided not to address the Year 2000 issue because they have elections that are coming up. The magnitude of the cost to fix the situation is something and the lack of full acceptance of the problem itself is something that many politicians don't want to be saddled with as being the politician that spent all that money or is supporting spending all of that money on this particular issue right before election time.

Mr. EHLERS. I can't conceive of a politician being afraid to do that. I simply, Ms. Coffou, while I have you on the mike, do you have any estimate of the percentage of embedded chips that have a problem?

Ms. COFFOU. No. Unfortunately, I do not. We have begun looking into that, Giga, as a company, but we don't have a percentage that we've been able to work up on that at this point.

How about Gartner?

Mr. HALL. We've looked at the problem and laid forth some preliminary percentages of something in the 2 to 4 percent range in that area, but I would submit that there has not been enough discovery done to the chips and certain as Ms. Coffou pointed out earlier, there's different levels of severity of these kinds of issues.

And I think you certainly want to prioritize those that are life-threatening first, and a very, very small percentage of those are going to be like that. If they happen, they happen.

Somewhere under the 5 percent range here is what we're talking about.

Mr. EHLERS. That makes me feel better because that would have been my estimate before coming in the room. After hearing the discussion, I was beginning to be afraid you're talking about 40 or 50 percent.

Mr. HALL. Make no mistake. We are talking about 100 percent inspection, so it's a remediation issue that we're talking about here.

Mr. EHLERS. Right.

One other question. Well, I have a host of technical questions. I probably shouldn't take the panel's time. If I'm still here at the end, I'll ask you then, but I'm afraid we're going to have a vote in just a few moments.

Just one quickie. When you talk about the 286 and the waste water treatment plant, are you talking about the problem of the software that's being used, or are you talking about the ROM or the built-in memory?

Mr. PERAINO. As I understand it, that was a 286 generation chip, that was a hard, embedded chip issue.

In the waste water treatment plant, as it was described to me——

Mr. EHLERS. I guess my feeling is anyone who is still using a 286 should be replacing it anyway.

A related question, however, is I assume you raised the issue, Mr. Hall, of the small business with the smaller computers.

Isn't it likely that virtually all the operating systems being developed by now have taken care of the problem, and that virtually all the shrink wrap you buy in the latest version will have taken care of the problem? It's received so much publicity.

Bill Gates assured me that Microsoft had taken care of it.

Mr. HALL. I think it depends on how liberally you want to use the word virtually. The reality is there are many products, either operating systems or commercial off the shelf products that will not achieve compliance until at least the end of this year.

If you look at the operating systems and the systems that have addressed it first, they are the ones that began from the legacy side and came down. For example, IBM has addressed it earlier I think than probably just about anybody else.

Again, when you talk about compliance in these particular systems, there is no substitute for testing. Unfortunately, the whole progress and the whole time lines of when we're going to receive the upgraded operating system, when we're going to receive the upgraded version of the software is not enough time for us to do integration of the customizations we may have made to that software.

Has the vendor adequately tested it, and can we get it implemented and up and running before you hit our time horizon to failure, which in many instances might be as soon as next summer or even already may have passed in some cases?

I think the whole issue of timing is one that I don't think we should take for granted on any platform or for any technology.

Mr. EHLERS. I'll reserve the rest of my questions for later.

Thank you very much.

Mr. HORN [presiding]. I thank the gentleman.

I now yield to the Ranking Democrat on the Subcommittee on Management, Ms. Maloney of New York.

Mrs. MALONEY. Thank you very much, Mr. Chairman.

I would like to request that my opening statement be placed in the record as read.

Mr. HORN. Without objection, so ordered.

[The prepared statement of Ms. Maloney follows:]

STATEMENT OF HONORABLE CAROLYN MALONEY

GOVERNMENT MANAGEMENT SUBCOMMITTEE HEARING

ON

SOLVING THE YEAR 2000 COMPUTER PROBLEM

MARCH 20, 1997

Thank you, Mr. Chairman. This morning I introduced the Millennium Computer Act of 1997. I know that you disagree with me that there is a need for legislation on this issue, but I hope you will give my bill a fair hearing.

This bill requires all agencies to renovate and test all computer systems to ensure that they will not fail solely because of an inability to correctly account for the years after 1999. It further requires that agencies certify to Congress not later than July 1, 1999, that all critical systems have been renovated and tested. To assist us in monitoring this renovation, I have included several reporting requirements.

First, all agencies are required to report to the Committee on Government Reform and the Senate Committee on Governmental Affairs, not later than August 1 of this year, an inventory of all computer systems; an identification of which systems are critical; and a detailed schedule for renovation and testing.

A second set of reports are required on July 1, 1998. In these reports the agencies must identify the procedures adopted for renovation and testing; the percent of critical systems that have been renovated and tested, and the results of those tests; and the percent of all systems that have been renovated and tested, and the results of those tests.

This bill will send a clear message to the executive agencies that the millennium bug must not be allowed to cause their systems to fail. The reports in this bill will give us the information necessary to monitor agency progress, and to sound an alarm about those agencies that are failing to address the problem well in advance of January 1, 2000.

Mrs. MALONEY. I unfortunately had a conflict with the Banking Committee today.

I'd like to ask Ms. Coffou on your testimony about the embedded chips in our weapons systems. How can Congress be sure that the Defense Department is correcting all of the embedded chip problems in our weapons systems that you pointed out?

How can we be sure that they're correcting it? Or anybody on the panel.

Ms. COFFOU. You've got to ask them. You need to find, we've been speaking about this, you need to find out, again, make the request as to what are you doing, what is the plan, where are you right now in the status of that plan. What are you finding out? How are the manufacturers working with you? Which ones are cooperating? Which ones are you having more difficulty with? What is your plan? Let's take a look at your plan. How are you as far as action and activity, actual tool plan.

It has to come as far as it's an awareness, you have to ask and be told.

Mrs. MALONEY. Mr. Chairman, since the defense of our country is very important, I'd like to recommend that the Committee place in writing a series of questions to the Defense Department as outlined by Ms. Coffou and we can work on it with the appropriate staff between the Minority and the Majority, so that we can get a direct answer from the Defense Department.

Mr. Chairman, I'm asking you a question. I'm asking if we can send a letter to the Defense Department outlining the problems that she mentioned, a series of questions to get a breakdown of where they stand on this problem she's pointed out?

Mr. HORN. We have worked out, with the Office of Management and Budget, on a regular basis, that the staffs of the respective Committees involved in OMB will send a questionnaire to the Department, so we've got one voice in the hymnal here. Then we will ask the relevant Chairs and the relevant Ranking Members to sign the various individual letters that will be prepared based on the testimony we heard today.

Because what we want is action under existing authority. If existing authority doesn't exist, we'll then deal with that legislatively, as I mentioned earlier.

My staff will work with all relevant staff to get their appropriate legislation drafted. We're going to do this as a team effort. You will be asked to sign a series of letters.

Mrs. MALONEY. Very well. At our last hearing, the representatives of the State Department told us they have no direct computer links with other countries. And of the agencies that testified, they were the ones that appeared to be more really in control of the problem and taking the necessary steps to correct it.

What about our interaction with foreign countries? Even though we don't have direct computer links, there could be emergencies where we have to exchange information rapidly with foreign allies. There could be emergencies that develop that we need to communicate with a computer, relevant data.

What is taking place now to make sure that our allies and maybe people that are not our allies that we're communicating with, that the problem is being addressed internationally?

Mr. MILLER. I think you've hit something, Congresswoman, that's of great concern. It's not only what we're doing but what other countries are doing. Because as far behind as we are in this country, I think most of the analysts would agree that most other countries are even further behind, not just in terms of government to government links, but industry to industry links.

Just to take your hypothesis one step further, perhaps the U.S. Government is saying they don't have formal links with other countries, but we do have outposts in those countries which may be dependent on the telecommunications systems of those other countries.

If their telecommunications systems don't operate because of the Year 2000 problem, we've lost our links with our own outposts in those other countries. So it's not enough to say that we don't have a direct link with another country's government, our own State Department employees abroad, or other agency's employees abroad. If the communications are not on some private network which is totally immune to the Year 2000, which is unlikely, there could be a problem there.

Mrs. MALONEY. I believe they indicated, if I understood them correctly, that there were, as far as our embassies are involved and our personnel, and our outposts, that the problem was being corrected and the computer system was separate.

That was my understanding. Maybe the Chairman had a different understanding from the conversation we had with the State Department.

The problem is with the country itself, is what they're saying.

Mr. MILLER. Again, I don't want to debate them, because I wasn't here for the hearing unfortunately. But I think there is some question about their dependency on other telecommunications systems. Telecommunications systems, to the average consumer, appear to be seamless, but the reality is they're so wonderful because they appear to be seamless. But, in fact, there are seams and there are interconnections.

If in fact our government is so independent of all the telecommunications systems that it's able to tell you that it has no problems, then I guess they can tell you that. I think I would probe that a little further if I were in your position.

Mrs. MALONEY. I think you have come up with an excellent suggestion. We intend to follow up.

This may sound like rather a silly question, but I'd just like to ask you. Last year we passed legislation requiring agencies to buy software that was Year 2000 compliant.

What guarantees can we have that the software works? I mean, we have a whole computer system that doesn't work now. How will agencies know if the software that they are purchasing is compliant? We never dreamed we'd have the problem we confront now. How do we know that the software that they tell us that they're buying that they are putting into the system works?

Mr. HORN. Well, if I might interject, the General Services Administration has the responsibility to certify that they are Year 2000 compliant. And if they aren't certified, the government cannot buy it. That's my current understanding.

Am I wrong, staff?

I don't see any heads nodding that way. They seem to be nodding that way.

Mr. HALL. I think if I could just respond. I think there's an issue of what Year 2000 compliance means and how we can prove it. And I think when you talk about a given product, or a software package or other kind of technology, you know, has it been in fact tested up into the next century.

In fact, I've talked to certain software vendors who shall remain nameless who are talking to the effect that their software will in fact be Year 2000 compliant, and they have not tested it into the Year 2001. They have gone through and they have validated it, and they said it looks good to us, but we haven't gotten through a full systems test.

But they're claiming that, so I think the message is we need to probe to the next level to see if for any of the technology, we can excuse ourselves from a complete test of that technology in order to validate the vendors' claims of compliance. I think that's what we're trying to achieve.

When we asked questions, you know, and Gartner has published information and the ITAA 2000 program is aimed at similar goals, is to say to vendors, will you share with us your proof of testing. Will you share with us what you did to make it compliant. How much money you spent, how many people it took. Because we have a sense of what that ought to be and I think when vendors will come clean with that information and not only that, what help do you have to help us get to the new model, new version or whatever it is that we need to get to to make sure this thing is compliant, but lets not lose sight of the fact that liability and responsibility for that product working lies within our four walls.

And so the decision we have to make is, are we going to test this thing ourselves through a full system test, or aren't we. And I think you'd have a hard time pushing the fact that you'd experienced a failure of a particular technology and we can deal with the legal aspect of it, you know, back to a specific vendor.

I think we need to take on that responsibility ourselves.

Mrs. MALONEY. Okay. I'd like to ask Ms. Coffou a question, and if you've answered it, I can just read the testimony and the record.

You testified, or in your statement you mentioned really several critical systems that could fail from elevators to military equipment because of the date logic embedded in the chips.

Is there any systematic investigation underway to really determine the extent of the problem?

Ms. COFFOU. You mean worldwide systematic methods?

Mrs. MALONEY. U.S.

Ms. COFFOU. In the United States, as well as worldwide, I'm afraid the answer is no. There are independent bodies such as Giga Information Group, Gartner Group that are looking at this, but there, from a worldwide, US-wide basis, there has been nothing but forth at this point.

Mrs. MALONEY. Thank you very much, Mr. Chairman.

I yield back my time.

Mr. HORN. Thank you.

I now call on the distinguished gentleman from Illinois, Mr. Ewing.

Mr. EWING. Thank you, Mr. Chairman and to the panel members.

I was a little late coming in today and I ask your indulgence in that. But also I would admit to you that I'm a new member of this panel and so the whole subject matter today is new to me, and very interesting and somewhat alarming.

I probably am maybe a good example of what the American people are like in how we go blissfully on our way looking forward to a big celebration in the Year 2000 and not thinking much about whether our clocks or radios or weapons systems or anything else will work the next day.

Do we have an estimate of the cost to our economy to bring us into compliance in the Year 2000?

Mr. HALL. I think the most popular number that's been bandied about has been a Gartner number which we talked about it being between $300- and $600 billion worldwide.

Now that you mention it, I think it's worth expounding on that point which is what we refer to with that number is just the cost to remediate affected computer software. That's all we're addressing with that number.

And on top of that are additional costs to be considered, such as what about computer hardware and that 286 machine we have to replace. What's going to be our cost that maybe we were going to replace it anyway, but there's some catalyst due to the Year 2000.

What about embedded chips. There are certain banks staring at bills of over $100 million to replace their ATM machines because they do local credit card validation processing, and the ATM machine will become useless when they go to the 00 credit card.

We've also heard extensive testimony earlier about embedded firm ware chips in consumer devices, in process control systems, in defense systems. None of these are in our estimate.

I have not seen, and I think both Giga and Gartner are undergoing some kind of analysis here to try to put a price tag on that, but to say that the number, the impact to the worldwide economy will be over a trillion dollars just to remediate the technology that's affected I think ends up being a pretty conservative statement ac-

tually. And if you add to that the legal issues, you're into multi-trillions of dollars here.

Mr. PERAINO. My point was that the Gartner numbers, as I understand them, are also exclusive of litigation costs and my point would be, if people think it's expensive to fix the Year 2000 problem, they haven't begun to consider how expensive it will be to litigate the Year 2000 problem.

Ms. COFFOU. On that, Giga has actually done some research. We predict that for every dollar spent to remediate the problem, there's a potential of two to three dollars to litigate.

Mr. EWING. Is there time left? I mean we are in 1997. Have we run out of time? Is it too late? Should all of us in the legal profession be getting our knives sharpened up?

Mr. HALL. Thank you for asking that question. The answer is, it's not too late in our belief. We're not gloom and doom mongers. We certainly want to make everyone aware of the issue, but it is too late if we continue the debate of how much it will cost.

And what I'd like to see, and whatever I hear, is it $2.3 billion or is it $30 billion, the debate I'd much rather hear is, is it 2 years or is it 4 years, you know, to get through the remediation of our critical systems.

And our message from Gartner, and this was in my opening statement and my written testimony is, can we please bypass this assessment step that we're all going through and agree that we have mission critical processes that have to be maintained.

For an example of such a process is communications with foreign bodies. In the event of crisis, that's a process that has to be maintained.

Along that process, what technology supports it. Whether it's computer technology, whether it's embedded chip technology, whatever it might be, let's get crews to work today remediating that technology, meter their progress, and then from there extrapolate total cost.

And if we adopt that strategy right now, then we believe that we can avoid the kind of systemwide failures we're talking about.

Unfortunately, there's a lot of us on the panel here seeing the pattern of denial, particularly from the managers who have to authorize such activity is causing us, I think, and I don't want to speak for others, but myself I'm very concerned about that, that mentality will not shift soon enough.

Mr. MILLER. Mr. Ewing, not to be defensive, but just simply to elucidate the cost issue a little bit more, let me re-emphasize this is a maintenance problem. The country, the world has been able to save billions of dollars over the years because computer programs were not written with four digits for the year.

When I took computer programming courses back in college, there were only 80 columns on that punch card be used. My computer professor said, use one column for the date, don't you dare use any more because you need to use the rest of those columns for other fields. And as for storage space, don't use up any more storage and memory. There were premiums on all of those.

So like the school house that doesn't fix the roof for 25 years, or like the Chevy of 1964 which is still running in 1997, the mainte-

nance bill is coming due. I'm not downplaying or denying the cost estimates.

But I think it's important that the American people also understand that this wasn't some malicious intention by the computer industry to try to create a giant windfall in the Year 2000. What this was was using the technology to save money and to make it as cost efficient as possible. The law of unanticipated consequence is that many of these technologies have continued to be used like the 1964 Chevy running in 1997. It doesn't have airbags because no one had airbags back in 1964. If you want airbags today, you have to go out and pay for them.

Similarly, if you want to get your programs still running into the Year 2000, you're going to have to spend some maintenance money to do so.

Mr. EWING. I'm glad you made a comment about malicious intentional whatever it might be. There's a lot of talk about the legal cost. We don't know. I guess I can't quite fathom that the government's going to allow our legal system to throw us into economic chaos over what maybe was not malicious and intentional in this situation.

I think it's a very good point to make to the business world, to everyone out there that this needs to be fixed, but it's not a fear that I am absolutely sure that won't have long-range effect for our legal system as well.

Mr. PEARL. I was just going to say, Mr. Ewing, that issue that we're missing also is not just the legal costs, because that's down the road. But the administrative costs, the economic costs to our country, the business interruptions that are going to take place, the fact that checks may not be able to be issued by the government or the fact that a business can't go on. That kind of administrative cost is going to have an economic effect long before there's litigation.

That's the kind of thing that all of us can do, and what we've said throughout this whole panel is what the Congress can do in terms of making people aware so that the administrative costs are going to be lessened and that will be mitigated so that we might not have to rise to the level of as much litigation as has been discussed.

Mr. EWING. I have a question that I didn't make up, so I want you to know that I'm not responsible. But time is running out. I will read it and if you can give a quick answer that would be appreciated.

I understand there is an alternative solution to the Year 2000 problem which involves the modernization of software using object-oriented technologies. Some say that if this approach is effective, the Federal Government and American businesses would save hundreds of millions of dollars.

Apparently this technology is already being considered by the Department of Defense, specifically the Air Force.

What are your thoughts?

Mr. HALL. If I could weigh in on that one, object-oriented technology is a means to an end. And the end is to take an existing system that may have in it many, many points of function, in other

words, things that it performs that's expressed in lines of computer code.

Let's take an average size system of say one million lines of computer code. That may have 50 points of function, as we call it, 50 things it does, right?

Calculations that it does or rules that it enforces. The question is how long will it take in total calendar time to take that system, understand what it does in full, take a new technology such as object-orientation, transpose the work that the existing system does into the new technology, test it, train the users on it, take the existing data that exists in the existing system, cut it over to the new system, and ultimately shake out the bugs that are inevitably going to be there, and retire the existing system.

It's a hypothetical example, but let me tell you that the average wall clock time to do a job like that is between 2 to 4 years. And sometimes it's even longer.

And I would make the same case for attempting to replace, with an off-the-shelf vendor package. There's time when you have to adapt that package to the specific needs of an individual situation.

So I think if you look at just the mechanics of saying how long does it take when you use object-oriented technology to deploy a single point of function, that's not very long. But if you look at the entire project from beginning to end, including testing, including working out and shaking out the bugs, including understanding what the existing system does, which is a challenge in itself sometimes, you are going to blow out the back end your timing. You do not have time to initiate on a massive scale this kind of transition.

In fact, the organizations we've talked to and there are companies out there that will do just this, their whole positioning for the Year 2000 is we will re-engineer your system in object-oriented technology and retire your existing system.

You ask them their track record and how many lines of code have you converted and remediated for the Year 2000 so far. The answer is zero. So they don't know the full load of what that total calendar time will be.

So, you know, the current thinking in the market is that about 40 percent of the existing systems will be remediated. They'll just be fixed because we can't replace them, we can't rewrite them, we can't redeploy them.

Our estimate at Gartner is up in the 60 percent or even higher range of those systems that will have to be repaired because there's simply no time to deploy these new kinds of technologies once you account for the entire project.

Mr. EWING. Thank you, Mr. Chairman. Thank you, panel members.

Mr. MILLER. Mr. Chairman, can I address one other quick technical issue and maybe Mr. Hall and Ms. Coffou will also jump in.

Another thing we're concerned about with the Federal Government, at least the last time I talked to officials at OMB, is that they were going to use field date expansion to solve all Year 2000 problems across the board.

I think most industry analysts and most people doing this job think that is the wrong way to go. There isn't time, there aren't

the resources to do that. Maybe Mr. Hall and Ms. Coffou wanted to comment on that.

Mr. HALL. Well, yes. Let me just weigh in on that very quickly.

I think the debate here is, I'll speak quickly, the debate here is——

Mr. HORN. We've got about 10 seconds. Go ahead.

Mr. HALL. There is no one answer for any given system. The preferred way to go is what's called windowing which is the simpler, patchwork type fix as opposed to data expansion, but there are characteristics of each system that may force us to choose one way or the other, and I don't think we should enforce a single standard but make the right choice for each system.

Mr. HORN. We thank all of you. It's been an excellent hearing. I congratulate the staff that put the hearing together, and I congratulate each of you giving us a new perspective on some of the problems, both legal and actual, in terms of getting about remedying and fixing things.

I want to thank the staff that has worked on this.

J. Russell George, the Staff Director for our Government Management Subcommittee. Richard Russell, the Staff Director for the Technology Subcommittee of Science. Mark Uncapher, Counsel for the Subcommittee on Government Management, Benjamin Wu, Counsel for the Subcommittee on Technology. John Hynes, Professional Staff Member, and Andrea Miller, Clerk, for the Subcommittee on Government Management, and Kathi Kromer, Technology Staff Assistant. For the Minority, David McMillen, for the Government Management Subcommittee, and Mike Quear, Professional Staff Member, and Marty Ralston, Staff Assistant, for the Technology Subcommittee.

Our official reporter was David Hoffman.

We thank you. I think you had the toughest job in here. We need some new technology there to save his breath.

So thank you very much.

With that, this hearing is adjourned.

We have a vote on the Floor which will be over in 5 minutes.

[Whereupon, at 3:15 p.m., Thursday, March 20, 1997, the hearing was adjourned.]

○