YEAR 2000: BIGGEST PROBLEMS AND PROPOSED SOLUTIONS

HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

OF THE

COMMITTEE ON GOVERNMENT REFORM AND OVERSIGHT HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTH CONGRESS

SECOND SESSION

JUNE 22, 1998

Serial No. 105–199

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

U.S. GOVERNMENT PRINTING OFFICE

54–585 WASHINGTON : 1999

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-058448-5

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
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 B. SHADEGG, Arizona
STEVEN C. LATOURETTE, Ohio
MARSHALL "MARK" SANFORD, South Carolina
JOHN E. SUNUNU, New Hampshire
PETE SESSIONS, Texas
MICHAEL PAPPAS, New Jersey
VINCE SNOWBARGER, Kansas
BOB BARR, Georgia
DAN MILLER, Florida
RON LEWIS, Kentucky

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
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
ROD R. BLAGOJEVICH, Illinois
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
JIM TURNER, Texas
THOMAS H. ALLEN, Maine
HAROLD E. FORD, JR., Tennessee

BERNARD SANDERS, Vermont
(Independent)

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

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

STEPHEN HORN, California, *Chairman*

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

DENNIS J. KUCINICH, Ohio
PAUL E. KANJORSKI, Pennsylvania
MAJOR R. OWENS, New York
CAROLYN B. MALONEY, New York
JIM TURNER, Texas

EX OFFICIO

DAN BURTON, Indiana
HENRY A. WAXMAN, California

J. RUSSELL GEORGE, *Staff Director and Chief Counsel*
ROBERT ALLOWAY, *Professional Staff Member*
MATTHEW EBERT, *Clerk*
BRIAN COHEN, *Minority Professional Staff Member*

CONTENTS

Page

Hearing held on June 22, 1998 1
Statement of:
DeSeve, Edward, Deputy Director for Management, Office of Management and Budget 6
Grabow, Dennis, president, Millennium Corp 35
McCabe, Tom Sr., chairman, McCabe & Associates 74
Simpson, Alan, president, ComLinks.Com 59
Steinberg, Dan, president, Synthesis: Law & Technology 44
Stillman, Rona, Chief Scientist for Computers and Telecommunications, General Accounting Office, accompanied by Joel Willemssen, Director, Accounting and Information Management Division, General Accounting Office 15
Webster, Bruce F., chief technical officer, Object Systems Group and director of the Washington, DC Year 2000 Group 68
Letters, statements, etc., submitted for the record by:
DeSeve, Edward, Deputy Director for Management, Office of Management and Budget:
Colloquies and statements 94
Prepared statement of 9
Grabow, Dennis, president, Millennium Corp., prepared statement of 38
Horn, Hon. Stephen, a Representative in Congress from the State of California, prepared statement of 4
McCabe, Tom Sr., chairman, McCabe & Associates, prepared statement of 76
Simpson, Alan, president, ComLinks.Com, prepared statement of 62
Steinberg, Dan, president, Synthesis: Law & Technology, prepared statement of 47
Stillman, Rona, Chief Scientist for Computers and Telecommunications, General Accounting Office, prepared statement of 18
Webster, Bruce F., chief technical officer, Object Systems Group and director of the Washington, DC Year 2000 Group, prepared statement of 70

YEAR 2000: BIGGEST PROBLEMS AND PROPOSED SOLUTIONS

MONDAY, JUNE 22, 1998

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION, AND TECHNOLOGY,
COMMITTEE ON GOVERNMENT REFORM AND OVERSIGHT,
Washington, DC.

The subcommittee met, pursuant to notice, at 1:03 p.m., in room 2154, Rayburn House Office Building, Hon. Stephen Horn (chairman of the subcommittee) presiding.

Present: Representatives Horn, Davis, and Kucinich.

Staff present: J. Russell George, staff director and chief counsel; Bob Alloway, professional staff member; Matthew Ebert, clerk; Faith Weiss, minority counsel; Brian Cohen, minority professional staff member; and Ellen Rayner, minority chief clerk.

Mr. HORN. The Subcommittee on Government Management, Information, and Technology will come to order.

I begin today with an organizing concept on the year 2000 problem. We can break the year 2000 problem into five stages: Startup, easy work, hard work, final preparation, and aftermath.

The subcommittee helped initiate the first startup stage with the first congressional hearing on the year 2000 subject in April 1996. We moved into the second stage of easy work during 1997 and made some progress, implementing fixed and tested systems. By May 15, 1998, the Federal Government was up to 39 percent compliant for mission critical systems.

As of today, we are moving into the third stage of hard work. This stage will last about 1 year, until the spring of 1999. Then, we will move into the fourth stage of final preparation.

I characterize these stages because they represent different types of tasks and priorities, as well as solutions. In the first awareness stage, the task was convincing people that this was a real problem and they should take it seriously. In the second easy work stage, the task was developing processes for progress reporting, determining which systems are mission critical, code remediation, contracting, and automated tools.

Now, as we move into the third stage of hard work, the tasks, priorities, and solutions will shift once again. We have gathered a group of expert witnesses to look forward to this next stage to discuss what will be the highest priorities and, hopefully, get some insight into their solutions.

There is not enough time to do everything. There are too many problems contending for top priority. We must be careful in the se-

lection of the most important problems. We cannot afford to work on second-tier problems when first-tier problems are being simply ignored. We must be careful in the selection of the most realistic solutions. We cannot afford to make matters worse with unintended consequences.

So today we have gathered together expert witnesses from different perspectives, from the public and private sectors, policymakers, project managers, legal and financial experts, and domestic and international perspectives. We will discuss the same question across all these perspectives: What are the highest priority problems for the next stage of the year 2000 problem?

As I have said many times, and I think everybody is saying it now, this is not a technical problem, it's a managerial problem leading to practical actions. There is no doubt that the year 2000 problem is real. It isn't a figment of someone's imagination. There is no doubt that all systems will not be compliant in time. Our responsibility as a congressional oversight committee is to decrease the impact on the American people. We must cut the number of system failures in half and, then, cut that in half again.

From a legislative point of view, the year 2000 problem is unique. For most issues, Congress has the luxury of refining legislation again and again, over the course of decades. For the year 2000 problem, Congress will not be able to pass legislation, see how it works for a couple of years, and then, amend as necessary.

Identification of top priority year 2000 problems will not necessarily result in legislative action. However, any suggested legislative measures from this panel or any other source must be more carefully considered. The normal opportunities to correct unintended consequences are precluded by the short time remaining before the deadline.

This problem has evolved since our first subcommittee hearing on April 16, 1996. At first, it was a few lone individuals explaining the inevitable technical consequences of a two-digit year calculation in the next millennium. Now there is a whole range of voices, from every direction with thousands of anecdotes.

At first, the priority action was simple, raise awareness and start working. Now priorities must be carefully considered. We must distinguish the possible from the likely, rank order by impact, take into account the availability of work-arounds, include the consequences of failures on other systems, and remember practicality and the laws of unintended consequences. This hearing asks some of the leading experts for their carefully considered top priorities and recommended solutions.

Our first panel includes the following witnesses: Edward DeSeve, the Deputy Director for Management, Office of Management and Budget; Dr. Rona Stillman, Chief Scientist for Computers and Telecommunications, General Accounting Office; Dennis Grabow, the chief executive officer of the Millennium Investment Group; Dan Steinberg, president, Synthesis: Law and Technology; Alan Simpson, president, ComLinks; Bruce Webster, chief technical officer, Object Systems Group, and director of the Washington, DC Year 2000 Group; and Tom McCabe should be here, I believe, yes, a little out of order, chairman, McCabe & Associates.

We will go in the order in which we have it on the agenda. As you perhaps know, some of you have been here before, since it is a subcommittee of the Committee on Government Reform and Oversight, you need to stand and raise your right hands, and take the following oath.

[Witnesses sworn.]

Mr. HORN. I will note for the clerk that all seven witnesses have affirmed. We will now begin in the order you are on the agenda.

Mr. DeSeve, the Deputy Director for Management, Office of Management and Budget.

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

DAN BURTON, INDIANA
CHAIRMAN

ONE HUNDRED SIXTH CONGRESS

HENRY A. WAXMAN, CALIFORNIA
RANKING MINORITY MEMBER

Congress of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6143

"Year 2000: Biggest Problems and Proposed Solutions"
Opening Statement, Chairman Horn
June 22, 1998 at 1:00 p.m. in 2154 Rayburn

I begin today with an organizing concept of the stages in the Year 2000 problem. We can break the Year 2000 problem into five stages:

1. start-up
2. easy-work
3. hard-work
4. final preparation, and
5. the aftermath.

This subcommittee helped initiate the first start-up stage with the first Congressional hearing on the Year 2000 subject in April of 1996.

We moved into the second stage of easy-work during 1997 and made some progress implementing fixed and tested systems. By May 15 of 1998, the Federal Government was up to 39% compliance for mission-critical systems.

As of today, we are moving into the third stage of hard-work. This stage will last about one year, until the spring of 1999. Then, we will move into the fourth stage of final preparation.

I characterize these stages because they represent different types of tasks, priorities, and solutions. In the first awareness stage, the task was convincing people that the problem was real and serious. In the second easy work stage, the task was developing processes for progress reporting, determining which systems are mission-critical, code remediation, contracting, and automated tools.

Now, as we move into the third stage of hard work, the tasks, priorities, and solutions will shift once again. We have gathered a group of expert witnesses to look forward to this next stage - what will be the highest priorities and, hopefully, some insight into their solutions.

There is not enough time to do everything. There are too many problems contending for top priority. We must be careful in the selection of the most important problems. We can not afford to work on second tier problems, when first tier problems are being ignored.

We must be careful in the selection of the most realistic solutions. We can not afford to make matters worse with unintended consequences.

We have gathered together expert witnesses from different perspectives - from the public and private sectors, policy makers and project managers, legal and financial, and domestic and international perspectives. We will discuss the same question across all these perspectives: What are the highest priority problems for the next stage of the Year 2000 problem?

This is not a technical discussion, rather, it is managerial, leading to practical actions. There is no doubt the Year 2000 problem is real. There is no doubt that all systems will NOT be compliant in time. Our responsibility is to decrease the impact on the American people. We must cut the number of system failures in half; and then, cut it in half again.

From a legislative point of view, the Year 2000 problem is unique. For most issues, Congress has the luxury of refining legislation again and again over the course of decades. For the Year 2000 problem, Congress will not be able to pass legislation; see how it works for a couple of years; and then amend as necessary.

Identification of top priority Year 2000 problems will not necessarily result in legislative action. However, any suggested legislative measures from this panel, or any other source, must be more carefully considered. The normal opportunities to correct unintended consequences are precluded by the short time remaining before the deadline.

This problem has evolved since our first subcommittee hearing on Year 2000 on April 16, 1996. At first, it was a few lone individuals explaining the inevitable technical consequences of two digit year calculations in the next millennium. Now, there is a cacophony of voices from every direction with thousands of anecdotes.

At first, the priority action was simple - raise awareness and start working. Now, priorities must be carefully considered. We must distinguish the possible from the likely; rank order by impact; take into account the availability of work-arounds; include the consequences of failures on other systems, and remember practicality and the laws of unintended consequences.

This hearing asks some of the leading experts for their carefully considered top priorities and recommended solutions.

STATEMENT OF EDWARD DeSEVE, DEPUTY DIRECTOR FOR MANAGEMENT, OFFICE OF MANAGEMENT AND BUDGET

Mr. DESEVE. Thank you very much, Mr. Chairman.

I am here today to discuss the Federal Government's efforts to address the year 2000 problem. As you know, the seemingly simple problem is one of the great challenges confronting our Nation today. Let me begin by expressing my support for the work of this committee. You have been and are playing a key role in helping to address this critical issue.

By way of background, Executive Order 13073, Year 2000 Conversion, created the President's Council on the Year 2000 Conversion, chaired by Assistant to the President, John Koskinen. The council has a twofold mission: First, to assist Federal agencies as they work to prepare their systems for the new millennium; and second, to increase awareness of the problem among private sector entities, State and local governments, and international organizations.

We at OMB are working very closely with the council. While OMB continues its role of oversight of Federal agency progress on fixing the internal year 2000 problem, the role of the Council has been to increase awareness beyond the Federal Government.

The invitation letter today asks that I discuss practical solutions to high priority activities. Accordingly, I would like to identify our top management priorities and the practical solutions that we are undertaking. This afternoon I would like to describe five of those priorities: First, dealing with mission critical systems; second, data exchanges; third, embedded chips; fourth, continuity of business planning; and fifth, international and national readiness, and discuss each of those briefly.

The first priority I would like to mention is that of fixing mission critical systems. Overall, the Federal Government continues to make progress, but at the rate of some agencies' progress is not fast enough. As you know, OMB has characterized agencies into one of three tiers. Although 71 percent of the mission critical systems of tier 3 agencies are compliant, only 33 percent of those in tier 1 agencies are compliant. It's critical that those agencies most at risk devote more management attention to fixing the problem.

We in the administration are taking practical steps to improve the progress of these agencies. First, for all cabinet agencies that are not making sufficient progress, the chairman of the Year 2000 Conversion Council and OMB staff will personally participate in monthly progress briefings with senior management of each tier 1 cabinet agency. In addition, we have asked the tier 1 and tier 2 agencies to provide OMB their plans for monthly progress toward making their mission critical systems compliant, and that they provide monthly progress reports against those plans.

The plans are due to OMB on Friday, June 26, and the monthly progress reports will be due on the 10th of each month, beginning in August. As a practical matter, Mr. Chairman, as we have in the past, we will make this information available to the committee on a timely basis.

Data exchanges. Another priority is coordinating and managing exchanges of data with those outside the Federal Government. It is essential that exchange partners agree on changes to the format

of exchanges, as well as the timing of such exchanges. Federal agencies have more than 10,000 such exchanges with each other, with foreign, State and local governments and private entities.

In response to this problem, we do hope for a close working relationship with organizations such as NASIRE, the National Association of State Information Resource Executives, and the National Governors' Association.

As a practical first step, we directed agencies to inventory all of their data exchanges by February of this year, and to begin discussions with their exchange partners. The deadline for them to update all of these exchanges is March 1999, however, beginning in July, Federal agencies will incorporate into the inventory the status of each exchange. The status will be reported by State and will include whether the exchanges are compliant or not.

Embedded chips. An additional priority is that of addressing the embedded chip problem. As you know, this is the great unknown about the year 2000 problem. People are finding embedded chip problems in a wide array of unexpected noncomputer places. Last week, for example, I read about a number of chip problems that could affect the operation of cargo tankers. At this point, it appears that virtually any large piece of machinery could have an embedded chip problem. While much of the work in identifying embedded chips and contacting the manufacturers of the product must be done individually by agency, in some cases, a governmentwide approach is more practical.

One solution has been to establish through the Chief Information Officers Council interagency working groups in the areas such as biomedical devices and laboratory equipments, commercial products, telecommunications and building. Each group is chaired by key agency personnel, and listed in my testimony are the web sites to these groups. Once an agency finds that a product is either compliant or noncompliant, in terms of embedded chips, the web site is the mechanism for posting this information.

The next priority I would like to highlight is the continuity of business planning. No matter how well Federal agencies progress between now and January 1, 2000, there is no question there will be some problems. As a practical solution to this problem, the CAO Council's Year 2000 Committee and the General Accounting Office are developing a draft guide on continuity of business planning. Such planning is to address, in addition to the risk of failure of agencies' internal systems, the implication of the year 2000 problem that are outside of the agencies' control. In addition, we will shortly require agencies to provide us with more detailed information on both their continuity of business plans, as well as contingency planning for those systems that are expected to miss the March 1999 deadline for implementation.

National and international preparedness. The Council implemented a practical solution by reaching out to many complex constituencies and groups and by building on existing organizational relationships. The Council has identified roughly 30 economic sectors and enlisted agencies with policy interests or connections to those areas to serve as coordinators. These areas are critical because everyone is dependent on them; thus, the energy group is cochaired by the Department of Energy, the Federal Emergency Reg-

ulation Commission is looking at gas and oil, telecommunications is being worked on by FCC, et cetera. Meanwhile, the State Department is taking the lead overall in raising awareness internationally. For example, Secretary Albright recently sent to all U.S. Ambassadors a cable that designates them as the U.S. Year 2000 Coordinator in their host country and instructs them to determine the Y2K readiness of these countries.

Year 2000 funding. In order to implement these and other priorities, OMB will continue to assist all agencies in assuring that adequate resources are available to address this critical issue. In the fiscal year 1999 budget, the President has requested more than $1 billion for a Y2K computer conversion. In addition, the budget anticipated that additional requirements would emerge over the course of the year and, in a practical way, included an allowance for emergencies and other unanticipated needs.

At this time, we believe the resource levels included in the President's budget will fully address the year 2000 conversion problems governmentwide. However, our experience has been, as we learn more about how to address these problems, we expect that ensuring governmentwide compliance will require flexibility to respond to unanticipated requirements. To the extent such unanticipated requirements are identified, it will be essential to make sure that funding is available quickly and will truly be emergency funding. The emergency mechanism recently approved by the House Appropriations Committee provides such flexibility. We are encouraged to learn the Senate Appropriations Committee is also expected to approve such a mechanism.

As action on the various appropriation bills proceeds, we urge Congress to leave as much as possible of the emergency contingent reserves unallocated so funds are available to address emerging needs. It is our understanding when the House Rules Committee meets on Tuesday to take up the Defense and Treasury/General Government appropriations bills, they will report rules that will strip the emergency funding mechanisms from both bills. This is regrettable action and will not help agencies move forward in addressing the problem. The value of the emergency mechanism approved by the House Appropriations Committee is the flexibility it provides in the event we determine that additional requirements are required. We have only 557 days left. We want to solve the problem as soon as possible. By delaying approval of emergency funding and reopening the issue of the use of the emergency spending authority, the House would create controversy and delay. We hope the House will reconsider.

That concludes my testimony, Mr. Chairman. I would be delighted to take questions either now or at the end of the panel.

[The prepared statement of Mr. DeSeve follows:]

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

STATEMENT OF G. EDWARD DESEVE
ACTING DEPUTY DIRECTOR FOR MANAGEMENT
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE
COMMITTEE ON GOVERNMENT REFORM AND OVERSIGHT
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY
UNITED STATES HOUSE OF REPRESENTATIVES

June 22, 1998

Good afternoon. I am here today to discuss the Federal government's efforts to address the year 2000 problem. As you know, this seemingly simple problem is one of the great challenges confronting our nation today. Let me begin by expressing my support for the work of this Committee. You have been and are playing a key role in helping to address this critical issue.

By way of background, E.O. 13073, *Year 2000 Conversion*, created the President's Council on Year 2000 Conversion, chaired by an Assistant to the President, John Koskinen. The Council has a two-fold mission: to assist Federal agencies as they work to prepare their systems for the new millennium and to increase awareness of the problem among private sector entities, State and local governments, and international organizations.

We at OMB are working very closely with the Council. While OMB continues its oversight of Federal agency progress on fixing the internal year 2000 problem, the role of the Council has been to increase awareness beyond the Federal government. Therefore, today I will discuss our efforts to help Federal agencies fix their internal year 2000 problems while also touching on the national and international efforts of the Council.

The invitation letter asks that I discuss "practical solutions to high-priority activities." Accordingly, I would like to identify our top management priorities and the practical solutions that we are undertaking. This afternoon, I would like to describe five of those priorities -- mission-critical systems, data exchanges, embedded chips, continuity of business planning, and national and international readiness -- and briefly discuss the practical solutions that we have underway.

Mission-critical Systems

The first priority I would like to mention is that of fixing mission-critical systems. Overall, the Federal government continues to make progress in addressing the year 2000 problem -- but the rate of some agencies is still not fast enough. As you know, OMB has categorized agencies into one of three tiers based on evidence of adequate progress. Although 71 percent of the mission-critical systems of the tier 3 agencies are compliant, only 33 percent of those of the tier 1 agencies are compliant. It is critical that those agencies at most risk devote more management attention to the problem in order to ensure that solving it is the agency's highest

priority

We in the Administration are taking practical steps to improve the progress of these agencies First, for all the Cabinet agencies that are not making sufficient progress, the Chairman of the Year 2000 Conversion Council and OMB staff will personally participate in monthly progress briefings with the senior management of each tier 1 Cabinet agency. This way we can provide on-the-spot practical help to Departmental management in addressing any problems that may be slowing their progress.

In addition, we have asked the tier 1 and tier 2 agencies to provide to OMB their plans for monthly progress toward making their mission-critical systems compliant, and that they provide monthly reports on their progress against those plans. The plans are due to OMB on Friday, June 26, and the monthly progress reports will be due on the tenth of each month beginning in August. This is a practical way to monitor the agencies at highest risk more closely, without imposing a substantial new reporting burden on them. We will include summaries of this information in future OMB quarterly reports.

Data Exchanges

Another priority is coordinating and managing exchanges of data with those outside the Federal government. It is essential that exchange partners agree on changes to the format of exchanges, as well as the timing of such changes. Federal agencies have more than 10,000 such exchanges with each other; with foreign, State, and local governments; and with private entities. Of particular importance are data exchanges with the States, because States operate many important Federal programs.

In response to this problem, we have developed a close working relationship with organizations such as the National Association of State Information Resource Executives (NASIRE) and the National Governors Association. As a practical first step, we directed agencies to inventory all of their data exchanges by February of this year and to begin discussions with their exchange partners by March. In their most recent reports to us, all agencies say they have inventoried their exchanges and initiated discussions with their partners. The deadline for them to update these exchanges is March 1999.

In addition, the Chief Information Officers (CIO) Council has been working with NASIRE to assure that these exchanges will work. This spring, Federal agencies provided the States with an inventory of Federal/State data exchanges. The States are in the process of verifying that the inventory is complete. Beginning in July, Federal agencies will incorporate into the inventory the status of each exchange. The status will be reported by State and will include whether the exchange is compliant, whether the fix is permanent or interim, and whether the fix has been tested. This information will be updated monthly and will provide us with useful, practical information about how well agencies are doing in preparing their data exchanges.

Embedded Chips

An additional priority is that of addressing the embedded chip problem. As you know, this is the great unknown about the year 2000 problem. People are finding embedded chip problems in a wide array of unexpected, non-computer places. Just last week, for example, I read about a number of chip problems that could affect the operation of ships. At this point it appears that virtually any large piece of machinery or any complex process needs to be assessed to see if it will be impacted by an embedded chip problem. It is important to note that in these instances the problem occurs in commercial products that rely on computers or have computer chips inside them. Therefore, unlike fixing custom software, these problems, while identified by agencies, usually need to be fixed by the manufacturers of those products.

While much of the work of identifying chip problems and contacting the manufacturers of the products must be done individually by each agency, in some cases a government-wide approach is more practical. One solution has been to establish, through the CIO Council, interagency working groups in the areas of bio-medical devices and laboratory equipment, commercial products, telecommunications, and buildings. Each interagency working group, chaired by a key program agency, is tasked with raising awareness across government and working with manufacturers to assure that products are fixed. Each group is contacting vendors on behalf of the entire Federal government, performing tests to verify the compliance of products, and sharing information through electronic databases. This information is publicly available at these websites:

FDA site on biomedical devices	www.fda.gov/cdrh/yr2000
GSA site on compliant commercial products	http://y2k.policyworks.gov/
GSA site on telecommunications equipment	http://y2k.fts.gsa.gov/
GSA site on buildings and facilities	http://globe.lmi.org/lmi_pbs/y2kproducts/

Continuity of Business Plans

The next priority that I will highlight is continuity of business planning. No matter how well Federal agencies progress between now and January 1, 2000, there is no question that there will be some problems. This is true both for agencies that complete their work on the problem as well as those that do not. Therefore, as a practical matter, agencies need to begin planning now to assure the continuity of their core business functions.

As a practical solution to this problem, the CIO Council's Year 2000 Committee and the General Accounting Office are developing a draft guide on continuity of business planning. Such planning is to address, in addition to the risk of failure of the agency's internal systems, the implications of the year 2000 problem that are outside of the agency's control, such as the inability of suppliers to provide products or the failure of critical infrastructures. In addition, we will shortly require agencies to provide us with more detailed information on both their continuity of business plans as well as contingency planning for those systems that are expected

to miss the March 1999 deadline for implementation

National and International Preparedness

A final priority of the Council is to promote national and international preparedness. Because of the interconnected nature of our technology dependent world, the Council has realized how important it is that our country as a whole be prepared -- and that the world is ready, too.

The Council implemented a practical solution to the problem of reaching out to so many complex constituencies and groups by building on existing organizational relationships among agencies and outside groups. The Council has identified roughly 30 economic sectors and enlisted agencies who have policy interests in, or connections to, these areas to serve as "coordinators," to increase awareness of the problem and to offer support. The list of sectors includes energy, telecommunications, and financial institutions. These areas are critical because everyone is dependent on them. Thus, the energy sector group is co-chaired by the Department of Energy, which is looking at electric power, and the Federal Energy Regulatory Commission, which is looking at oil and gas. The telecommunications sector group is co-chaired by the Federal Communications Commission and the General Services Administration, and the financial institutions sector group is chaired by the Federal Reserve Board.

In many cases, agencies have a natural constituency. In other cases, agencies have been tasked with reaching out to groups that the Federal government doesn't traditionally do business with. While some agencies have a regulatory role, all agencies have a responsibility to make sure that they groups they are in contact with are ready and to ensure that there are no gaps in coverage.

In the international arena, the Chairman of the Council has met with the United Nations Informatics Working Group on this issue; he has also met with the Chair of the World Bank, who subsequently issued a letter to the leaders of all member nations on this subject. We have met with the year 2000 representatives from a number of nations, including Mexico, South Africa, England, and Canada.

Meanwhile, the State Department is taking the lead overall on raising awareness internationally. For example, Secretary Albright recently sent to all U.S. ambassadors a cable that designates them as U.S. year 2000 coordinators in their host countries and instructs them to determine the year 2000 readiness of those countries' basic infrastructures. The Federal Aviation Administration has met with its international counterparts, while the Federal Communications Commission has been working with the International Telecommunications Union.

While the Federal government is reaching out to a large number of organizations, both domestic and international, it is important to note that it has no authority to directly intervene in most of these areas. Therefore, the most practical approach for the Council to take is to raise

awareness and to facilitate the flow of information help organizations fulfill their responsibilities to make sure their systems work.

Year 2000 Funding

OMB will continue to assist all agencies in ensuring that adequate resources are available to address this critical issue. In the FY 1999 Budget, the President has requested more than $1 billion for Y2K computer conversion. In addition, the Budget anticipated that additional requirements would emerge over the course of the year, and included an allowance for emergencies and other unanticipated needs.

At this time, we believe that the resource levels included in the President's budget will fully address Y2K computer conversion requirements Government-wide. However, as we learn more about how to address this problem, we expect that ensuring Government-wide compliance will require flexibility to respond to unanticipated requirements. To the extent such unanticipated requirements are identified, it will be essential to make that funding available quickly. It will truly be emergency funding.

The emergency mechanism recently approved by the House Appropriations Committee provides such flexibility. We are encouraged to learn that the Senate Appropriations Committee is also expected to approve such a mechanism. As action on the various appropriations bills proceeds, we urge Congress to leave as much as possible of the emergency contingent reserve unallocated so that funds are available to address emerging needs.

It is our understanding that when the House Rules Committee meets on Tuesday to take up the Defense and Treasury/General Government Appropriations bills they will report rules that will strip the emergency funding mechanism from both bills. This regrettable action will not help agencies move forward in addressing this problem.

The value of the emergency mechanism approved by the House Appropriations Committee is the flexibility it provides in the event that we determine that additional resources are required. We have only 557 days until January 1, 2000. We want to solve this problem as soon as possible. By delaying approval of emergency funding and reopening the issue of the use of the emergency spending authority, the House will create controversy and delay. We hope the House will reconsider.

Moving Forward

There is no doubt the year 2000 problem poses a significant challenge to Federal agencies and to our nation as a whole. But I am confident Federal agencies will live up to their end of the bargain, both in fixing their internal year 2000 problems and in increasing awareness beyond the Federal Government.

I thank the committee for its continued interest in the year 2000 problem You are making a valuable contribution to the public dialogue about this matter I look forward to working with you, and I would be happy to answer any questions that you may have.

Mr. HORN. Well, we will do it at the end, but let me just make two remarks. The Speaker is the person that speaks for the House of Representatives, at least a majority in the House, and the Speaker is very determined to have this come, every dollar you want, to have the emergency provisions invoked. So I think that is either misplaced, old news, or whatever. But that will be taken care of. We don't intend to deny you 1 penny, despite 2 or 3 years of procrastination, to be blunt about it. You are going to get every dime you need.

Now, let me just ask one question. You mentioned you would give us those quarterly reports on a timely basis.

Mr. DESEVE. Monthly reports, sir.

Mr. HORN. Monthly reports. What is your view of timely?

Mr. DESEVE. Within 7 working days. We need to get them in, look at them, and there may be some dialog with the agencies if the reports are not responsive, but 7 working days from the time at which they are submitted, both the plans and the reports.

Mr. HORN. Well, I frankly would hope we would get the reports at the same time. I think, as I have told John Koskinen, I said, John, you don't have time for quarterly reports or monthly reports, you need a weekly report if you are going to be serious about this, so I would hope that the reports would come up to us in 24 hours.

All right. Let us go down to the second witness, Dr. Rona Stillman, chief scientist for computers and telecommunications, General Accounting Office.

STATEMENT OF RONA STILLMAN, CHIEF SCIENTIST FOR COMPUTERS AND TELECOMMUNICATIONS, GENERAL ACCOUNTING OFFICE, ACCOMPANIED BY JOEL WILLEMSSEN, DIRECTOR, ACCOUNTING AND INFORMATION MANAGEMENT DIVISION, GENERAL ACCOUNTING OFFICE

Ms. STILLMAN. Mr. Chairman and members of the subcommittee, thank you for inviting me to participate in today's hearing on the year 2000 problem. Because of the urgent nature of the year 2000 problem and the potentially devastating impact it could have on critical government operations, we designated the problems a high risk area for the Federal Government in February 1997. Since that time, we have issued over 40 reports and testimony statements detailing specific findings and recommendations related to year 2000 readiness of a wide range of Federal agencies. We have also issued guidance to help organizations successfully address the issue.

Today I will briefly discuss our major concerns with Government's progress in fixing its systems, highlight the year 2000 risks facing the Government and introduce our guidance on year 2000 testing, which was designed to assist agencies in the most extensive and expensive part of remediation. Overall, the Government's 24 major departments and agencies are making slow progress in fixing their systems.

In May 1997, the Office of Management and Budget reported that about 21 percent of the mission critical systems for these departments and agencies were year 2000 compliant. A year later, in May 1998, these departments and agencies reported that about 40 percent were compliant. Unless progress improves dramatically, a

substantial number of mission critical systems will not be compliant on time.

In addition to slow progress in fixing systems, many agencies were not adequately acting to establish priorities, develop contingency plans, formulate a more complete and accurate picture of year 2000 progress, and ensure that the Government's critical core business processes are adequately tested. First, no governmentwide priorities have been established for fixing systems, based on such criteria as the potential for adverse health and safety effects, adverse financial effects on American citizens, and detrimental effects on national security. Furthermore, while individual agencies have been identifying mission critical systems, this has not always been done based on a determination of the agency's most critical operations.

For example, as noted by the Defense Science Board, defense has no means of distinguishing between the priority of a video conferencing system and the priority of a logistics system, both of which were identified as mission critical. If priorities are not clearly set, the Government will waste time and resources in fixing systems that have little bearing on its most vital operations.

Second, contingency planning across the Government has been inadequate. In their May 1998 quarterly reports to OMB, only four agencies reported that they had drafted contingency plans for their core business processes. Without such plans, when unpredicted failures occur, agencies will not have well-defined responses and may not have enough time to develop and test alternatives. Because Federal agencies depend on data provided by their business partners and services provided by the public infrastructure. For example, voice and data telecommunications, it's imperative that contingency plans be developed for all systems supporting critical core business processes, regardless of whether these systems are owned by the agency.

Third, OMB's assessment of the current status of Federal year 2000 progress is predominantly based on data that is self-reported by the agencies. Without independent reviews, OMB and the President's Council on Year 2000 Conversion have little assurance that they are receiving accurate information. In fact, some data reported to OMB have been inaccurate. The DOD Inspector General found that DOD had no adequate basis for reporting about 320 mission critical systems as compliant in November 1997. In May 1998, the Department of Agriculture reported 15 systems as compliant, even though these were replacement systems that were still under development or were still in planning.

Fourth, end-to-end testing responsibilities have not been defined. To ensure that the mission critical systems can reliably exchange data with other systems and that they are protected from errors that can be introduced by external systems, agencies must perform end-to-end testing of their critical core business processes. Since year 2000 problems affect nearly all digital systems, many systems in the end-to-end chain will have been modified or replaced. As a result, the scope and complexity of testing and its importance is dramatically increased, as is the difficulty of isolating, identifying, and correcting problems. So far, lead agencies have not been designated to take responsibility for end-to-end testing across organi-

zational boundaries and for ensuring the independent verification and validation of such testing.

One of the more alarming problems we have come across is that some agencies are not adequately prepared for testing their systems for year 2000 compliance. For example, in April 1998, we reported that the Department of Defense had not specified a uniform testing strategy for use by all its components. Further, the Army, Navy, and Air Force had not assessed their testing needs or their test facility requirements. In May 1998, we reported the Department of Agriculture's Chief Information Officer had not provided test guidance to the department's component agencies and that 8 of 10 component agencies included in our review had no testing strategies.

To address this problem, we are issuing today another installment in our year 2000 guidance, which addresses the need to plan and conduct year 2000 tests in a structured and disciplined fashion. The guide describes a step-by-step framework for managing and a checklist for assessing all year 2000 testing activities. It incorporates guidance and recommendations of standard bodies and draws on the work of leading information technology organizations. If effectively implemented, our guide should help Federal agencies successfully negotiate the complexities involved in the year 2000 testing.

Mr. Chairman, this concludes my statement. I will be happy, of course, to answer any questions.

[The prepared statement of Ms. Stillman follows:]

Mr Chairman and Members of the Subcommittee

Thank you for inviting me to participate in today's hearing on the Year 2000 problem. As you know, the federal government is extremely vulnerable to Year 2000 problems due to its widespread dependence on computer systems to process financial transactions, deliver vital public services, maintain national security, and carry out its operations. This challenge is made more difficult by the age and poor documentation of some of the government's existing systems and its lackluster track record in modernizing systems to deliver expected improvements and meet promised deadlines. Today, I will briefly discuss the Year 2000 risks facing the government; highlight our major concerns with the government's progress in fixing its systems; and introduce our guidance on Year 2000 testing, which is designed to assist agencies in the most extensive and expensive part of remediation.

RISK OF YEAR 2000 DISRUPTION TO GOVERNMENT SERVICES IS HIGH

Addressing the Year 2000 problem in time will be a tremendous challenge for the federal government. Many of the federal government's computer systems were originally designed and developed 20 to 25 years ago, are poorly documented, and use a wide variety of computer languages, many of which are obsolete. Some applications include

thousands, tens of thousands, or even millions of lines of code, each of which must be examined for date-format problems.

To complicate matters, agencies must also consider the computer systems belonging to federal, state, and local governments; the private sector; foreign countries; and international organizations that interface with their systems. For example, agencies that administer key federal benefits payment programs, such as the Department of Veterans Affairs, exchange data with the Department of Treasury which, in turn, interfaces with various financial institutions to ensure that benefits checks are issued. Department of Defense systems interface with thousands of systems belonging to foreign military sales customers, private contractors, other federal agencies, and international entities such as the North Atlantic Treaty Organization. Taxpayers can pay their taxes through data exchanges between the taxpayer, financial institutions, the Federal Reserve System, and the Department of Treasury's Financial Management Service and the Internal Revenue Service. Because of these and thousands of other interdependencies, government systems are also vulnerable to failure caused by incorrectly formatted data provided by other systems which are noncompliant.

The federal government also depends on the telecommunications infrastructure to deliver a wide range of services. For example, the route of an electronic Medicare payment may traverse several networks–those operated by the Department of Health and Human Services, the Department of the Treasury's computer systems and networks, and the

Federal Reserve's Fedwire electronic funds transfer system Seamless connectivity among a wide range of networks and carriers is essential nationally and internationally and a Year 2000-induced telecommunications failure could cause major disruptions.

In addition, the year 2000 could cause problems for the many facilities used by the federal government that were built or renovated within the last 20 years and contain embedded computer systems to control, monitor, or assist in operations. For example, building security systems, elevators, and air conditioning and heating equipment, could malfunction or cease to operate.

Agencies cannot afford to neglect any of these issues. If they do, the impact of Year 2000 failures could be widespread, costly and potentially disruptive to vital government operations worldwide. For example:

- flights could be grounded or delayed and airline safety could be degraded;
- the military services could find it extremely difficult to efficiently and effectively equip and sustain their forces around the world;
- Internal Revenue Service tax systems could be unable to process returns, thereby jeopardizing revenue collection and delaying refunds;
- the Social Security Administration process to provide benefits to disabled persons could be disrupted; and

- payments to veterans with service-connected disabilities could be erroneous or severely delayed.

KEY YEAR 2000 ISSUES ARE NOT BEING ADEQUATELY ADDRESSED

Because of the urgent nature of the Year 2000 problem and the potentially devastating impact it can have on critical government operations, we designated the problem as a high-risk area for the federal government in February 1997.[1] Since that time, we have issued over 40 reports and testimony statements detailing specific findings and recommendations related to the Year 2000 readiness of a wide range of federal agencies.[2] We have also issued guidance to help organizations successfully address the issue.[3]

Overall, the government's 24 major departments and agencies are making slow progress in fixing their systems. In May 1997, the Office of Management and Budget (OMB) reported that about 21 percent of the mission-critical systems (1,598 of 7,649) for these

---

[1]High-Risk Series: Information Management and Technology (GAO/HR-97-9, February 1997).

[2]A list of publications is included as an attachment to this statement.

[3]Year 2000 Computing Crisis: An Assessment Guide (GAO/AIMD-10.1.14, September 1997), which includes the key tasks needed to complete each phase of a Year 2000 program (awareness, assessment, renovation, validation, and implementation); and Year 2000 Computing Crisis: Business Continuity and Contingency Planning (GAO/AIMD-10.1.19, Exposure Draft, March 1998) which describes the tasks needed to ensure the continuity of agency operations.

departments and agencies were Year 2000 compliant[4] A year later, in May 1998, these departments and agencies reported that 2,914 of the 7,336 mission-critical systems in their current inventories, or about 40 percent, were compliant. Unless progress improves dramatically, a substantial number of mission-critical systems will not be compliant on time.

In addition to slow progress in fixing systems, many agencies were not adequately acting on critical steps to establish priorities, solidify data exchange agreements, and develop contingency plans. Likewise, more attention needs to be devoted to (1) ensuring the government has a complete and accurate picture of Year 2000 progress, (2) setting national priorities, (3) ensuring that the government's critical core business processes are adequately tested, (4) recruiting and retaining information technology personnel with the appropriate skills for Year 2000-related work, and (5) assessing the nation's Year 2000 risks, including those posed by key economic sectors. I would like to highlight some of these vulnerabilities and our recommendations made in April 1998 for addressing them.[5]

---

[4]The Social Security Administration's (SSA) mission-critical systems were not included in these totals because SSA did not report in May 1997 on a system basis. Rather, SSA reported at that time, and again in August 1997, on portions of systems that were compliant. For example, SSA reported on the status of 20,000-plus modules rather than 200-plus systems.

[5]Year 2000 Computing Crisis: Potential for Widespread Disruption Calls for Strong Leadership and Partnerships (GAO/AIMD-98-85, April 30, 1998).

- First, governmentwide priorities in fixing systems have yet to be established. There has not been a concerted effort to set governmentwide priorities based on such criteria as the potential for adverse health and safety effects, adverse financial effects on American citizens, detrimental effects on national security, and adverse economic consequences. Furthermore, while individual agencies have been identifying mission-critical systems, this has not always been done based on a determination of the agency's most critical operations. For example, as noted by the Defense Science Board, Defense has no means of distinguishing between the priority of a video conferencing system and a logistics system, both of which were identified as mission-critical. If priorities are not clearly set, the government may well end up wasting limited time and resources in fixing systems that have little bearing on the most vital government operations.

- Second, contingency planning across the government has been inadequate. In their May 1998 quarterly reports to OMB, only four agencies reported that they had drafted contingency plans for their core business processes. Without such plans, when unpredicted failures occur, agencies will not have well-defined responses and may not have enough time to develop and test alternatives. Federal agencies depend on data provided by their business partners as well as services provided by the public infrastructure (e.g., power, water, transportation, and voice and data telecommunications). One weak link anywhere in the chain of critical dependencies can cause major disruptions to business operations. Given these

interdependencies, it is imperative that contingency plans be developed for all critical core business processes and supporting systems, regardless of whether these systems are owned by the agency.

- Third, OMB's assessment of the current status of federal Year 2000 progress is predominantly based on agency reports that have not been consistently reviewed or verified. Without independent reviews, OMB and the President's Council on Year 2000 Conversion have little assurance that they are receiving accurate information. In fact, we have found cases in which agencies' systems compliance status reported to OMB has been inaccurate. For example, the DOD Inspector General estimated that almost three quarters of DOD's mission-critical systems reported as compliant in November 1997 had not been certified as compliant by DOD components.[6] In May 1998, the Department of Agriculture reported 15 systems as compliant, even though these were replacement systems that were still under development or were planned to be developed.[7] (The department plans to remove these systems from compliant status in its next quarterly report.)

- Fourth, end-to-end testing responsibilities have not yet been defined. To ensure that their mission-critical systems can reliably exchange data with other systems

---

[6]Year 2000 Certification of Mission-Critical DOD Information Technology Systems (DOD Office of the Inspector General, Report No. 98-147, June 5, 1998).

[7]Year 2000 Computing Crisis: USDA Faces Tremendous Challenges in Ensuring That Vital Public Services Are Not Disrupted (GAO/T-AIMD-98-167, May 14, 1998).

and that they are protected from errors that can be introduced by external systems, agencies must perform end-to-end testing for their critical core business processes. The purpose of end-to-end testing is to verify that a defined set of interrelated systems, which collectively support an organizational core business area or function, work as intended in an operational environment. In the case of the year 2000, many systems in the end-to-end chain will have been modified or replaced. As a result, the scope and complexity of testing–and its importance–is dramatically increased, as is the difficulty of isolating, identifying, and correcting problems. Consequently, agencies must work early and continuously with their data exchange partners to plan and execute effective end-to-end tests. So far, lead agencies have not been designated to take responsibility for ensuring that end-to-end testing of processes and supporting systems is performed across boundaries, and that independent verification and validation of such testing is ensured.

In our April 1998 report on governmentwide Year 2000 progress, we made a number of recommendations to the Chairman of the President's Council on Year 2000 Conversion aimed at addressing these problems. These included:

- establishing governmentwide priorities and ensuring that agencies set their own agencywide priorities;
- developing a comprehensive picture of the nation's Year 2000 readiness;

- requiring agencies to develop contingency plans for all critical core business processes;
- requiring agencies to develop an independent verification strategy to involve inspector general or other independent organizations in reviewing Year 2000 progress; and
- designating lead agencies responsible for ensuring end-to-end operational testing of processes and supporting systems is performed.

We are encouraged by actions the Council is taking in response to some of our recommendations. For example, OMB and the CIO Council adopted our draft guide providing information on business continuity and contingency planning issues common to most large enterprises as a model for federal agencies.[8] However, as we recently testified before this Subcommittee, some actions have not been initiated--principally with respect to setting national priorities, independent verification, and end-to-end testing.

GAO GUIDANCE ON YEAR 2000 TESTING

One of the more alarming problems we have come across in our Year 2000 reviews is that some agencies are not adequately prepared for testing their systems for Year 2000 compliance. For example, in April 1998, we reported that the Department of Defense did not have a testing strategy that specifies uniform criteria and processes which its

[8]GAO/AIMD-10.1.19, Exposure Draft, March 1998.

components should use in testing their systems The Army, Navy, and Air Force had not assessed their test needs or test facility requirements.[9] In May 1998, we reported that the Department of Agriculture's Chief Information Officer had not provided test guidance to the department's component agencies, and 8 of 10 component agencies included in our review lacked testing strategies.[10]

The fact that these agencies are not prepared now for effective testing raises serious concern. Complete and thorough Year 2000 testing is essential to provide reasonable assurance that new or modified systems process dates correctly and will not jeopardize an organization's ability to perform core business operations after the millennium. Moreover, since the Year 2000 computing problem is so pervasive, potentially affecting an organization's systems software, applications software, databases, hardware, firmware and embedded processors, telecommunications, and external interfaces, the requisite testing is extensive and expensive. Leading organizations estimate that testing will require at least 50 percent of an entity's total Year 2000 program time.

To address this problem, we are issuing today a new installment of our Year 2000 guidance which addresses the need to plan and conduct Year 2000 tests in a structured

---

[9]Defense Computers: Year 2000 Computer Problems Threaten DOD Operations (GAO/AIMD-98-72, April 30, 1998).

[10]GAO/T-AIMD-98-167, May 14, 1998.

and disciplined fashion [11] The guide describes a step-by-step framework for managing, and a checklist for assessing, all Year 2000 testing activities, including those activities associated with computer systems or system components (such as embedded processors) that are vendor supported. This disciplined approach and the prescribed levels of testing activities are hallmarks of mature software and system development/acquisition and maintenance processes.

The guide describes the five levels of Year 2000 testing activities. The first level establishes the organization infrastructure key processes needed to guide, support, and manage the next four levels of testing activities. For example, it addresses defining and assigning Year 2000 test management authority and responsibility, defining criteria for certifying a system as compliant, identifying and allocating resources, establishing schedules, and securing test facilities. The next four levels provide key processes for effectively designing, conducting, and reporting on tests of incrementally larger system components: software unit/module tests, software integration tests, system acceptance tests, and end-to-end tests. The processes focus on testing of software and system components that the organization is directly responsible for developing, acquiring, or maintaining. Key processes, however, are also defined to address organizational responsibilities relative to testing of vendor-supported and commercial, off-the-shelf

[11] Year 2000 Computing Crisis: A Testing Guide (GAO/AIMD-10.1.21, Exposure Draft, June 1998).

(COTS) products and components (including hardware, systems software, embedded processors, telecommunications and COTS applications).

The test model builds upon and complements the five-phase conversion model described in our Year 2000 readiness guide. The five levels of test activities span all phases of our Year 2000 conversion model, with the preponderance of test activities occurring in the conversion model's renovation and validation phases.

Finally, the guide incorporates guidance and recommendations of standards bodies, such as the National Institute of Standards and Technology and the Institute of Electrical and Electronic Engineers on Year 2000 testing practices and draws on the work of leading information technology organizations including the Software Engineering Institute, Software Quality Engineering, Software Productivity Consortium, and the United Kingdom's Central Computer and Telecommunications Agency.

In conclusion, if effectively implemented, our guide should help federal agencies successfully negotiate the complexities involved with the Year 2000 testing process. However, the success of the government's Year 2000 remediation efforts ultimately hinges on setting governmentwide priorities, ensuring that agencies set priorities and develop contingency plans consistent with these priorities, developing an accurate picture of

remediation progress, designating lead agencies for end-to-end testing efforts, and addressing other critical issues such as recruiting and retaining qualified information technology personnel.

Mr. Chairman, this concludes my statement. Mr. Joel Willemssen, GAO's Issue Area Director for Civil Agencies Information Systems and our focal point for Year 2000 work, has accompanied me today. We will be happy to answer any questions you or Members of the Subcommittee may have.

LIST OF GAO PRODUCTS THAT ADDRESS THE YEAR 2000 PROBLEM

Year 2000 Computing Crisis: Telecommunications Readiness Critical, Yet Overall Status Largely Unknown (GAO/T-AIMD-98-212, June 16, 1998)

GAO Views on Year 2000 Testing Metrics (GAO/AIMD-98-217R, June 16, 1998)

IRS' Year 2000 Efforts: Business Continuity Planning Needed for Potential Year 2000 System Failures (GAO/GGD-98-138, June 15, 1998)

Year 2000 Computing Crisis: Actions Must Be Taken Now To Address Slow Pace of Federal Progress (GAO/T-AIMD-98-205, June 10, 1998)

Defense Computers: Army Needs to Greatly Strengthen Its Year 2000 Program (GAO/AIMD-98-53, May 29, 1998)

Year 2000 Computing Crisis: USDA Faces Tremendous Challenges in Ensuring That Vital Public Services Are Not Disrupted (GAO/T-AIMD-98-167, May 14, 1998)

Securities Pricing: Actions Needed for Conversion to Decimals (GAO/T-GGD-98-121, May 8, 1998)

Year 2000 Computing Crisis: Continuing Risks of Disruption to Social Security, Medicare, and Treasury Programs (GAO/T-AIMD-98-161, May 7, 1998)

IRS' Year 2000 Efforts: Status and Risks (GAO/T-GGD-98-123, May 7, 1998)

Air Traffic Control: FAA Plans to Replace Its Host Computer System Because Future Availability Cannot Be Assured (GAO/AIMD-98-138R, May 1, 1998)

Year 2000 Computing Crisis: Potential For Widespread Disruption Calls For Strong Leadership and Partnerships (GAO/AIMD-98-85, April 30, 1998)

Defense Computers: Year 2000 Computer Problems Threaten DOD Operations (GAO/AIMD-98-72, April 30, 1998)

Department of the Interior: Year 2000 Computing Crisis Presents Risk of Disruption to Key Operations (GAO/T-AIMD-98-149, April 22, 1998)

Year 2000 Computing Crisis: Business Continuity and Contingency Planning (GAO/AIMD-10.1.19, Exposure Draft, March 1998)

Tax Administration. IRS' Fiscal Year 1999 Budget Request and Fiscal Year 1998 Filing Season (GAO/T-GGD/AIMD-98-114, March 31, 1998)

Year 2000 Computing Crisis: Strong Leadership Needed to Avoid Disruption of Essential Services (GAO/T-AIMD-98-117, March 24, 1998)

Year 2000 Computing Crisis: Federal Regulatory Efforts to Ensure Financial Institution Systems Are Year 2000 Compliant (GAO/T-AIMD-98-116, March 24, 1998)

Year 2000 Computing Crisis: Office of Thrift Supervision's Efforts to Ensure Thrift Systems Are Year 2000 Compliant (GAO/T-AIMD-98-102, March 18, 1998)

Year 2000 Computing Crisis: Strong Leadership and Effective Public/Private Cooperation Needed to Avoid Major Disruptions (GAO/T-AIMD-98-101, March 18, 1998)

Post-Hearing Questions on the Federal Deposit Insurance Corporation's Year 2000 (Y2K) Preparedness (AIMD-98-108R, March 18, 1998)

SEC Year 2000 Report: Future Reports Could Provide More Detailed Information (GAO/GGD/AIMD-98-51, March 6, 1998)

Year 2000 Readiness: NRC's Proposed Approach Regarding Nuclear Powerplants (GAO/AIMD-98-90R, March 6, 1998)

Year 2000 Computing Crisis: Federal Deposit Insurance Corporation's Efforts to Ensure Bank Systems Are Year 2000 Compliant (GAO/T-AIMD-98-73, February 10, 1998)

Year 2000 Computing Crisis: FAA Must Act Quickly to Prevent Systems Failures (GAO/T-AIMD-98-63, February 4, 1998)

FAA Computer Systems: Limited Progress on Year 2000 Issue Increases Risk Dramatically (GAO/AIMD-98-45, January 30, 1998)

Defense Computers: Air Force Needs to Strengthen Year 2000 Oversight (GAO/AIMD-98-35, January 16, 1998)

Year 2000 Computing Crisis: Actions Needed to Address Credit Union Systems' Year 2000 Problem (GAO/AIMD-98-48, January 7, 1998)

Veterans Health Administration Facility Systems: Some Progress Made In Ensuring Year 2000 Compliance, But Challenges Remain (GAO/AIMD-98-31R, November 7, 1997)

Year 2000 Computing Crisis: National Credit Union Administration's Efforts to Ensure Credit Union Systems Are Year 2000 Compliant (GAO/T-AIMD-98-20, October 22, 1997)

Social Security Administration: Significant Progress Made in Year 2000 Effort, But Key Risks Remain (GAO/AIMD-98-6, October 22, 1997)

Defense Computers: Technical Support Is Key to Naval Supply Year 2000 Success (GAO/AIMD-98-7R, October 21, 1997)

Defense Computers: LSSC Needs to Confront Significant Year 2000 Issues (GAO/AIMD-97-149, September 26, 1997)

Veterans Affairs Computer Systems: Action Underway Yet Much Work Remains To Resolve Year 2000 Crisis (GAO/T-AIMD-97-174, September 25, 1997)

Year 2000 Computing Crisis: Success Depends Upon Strong Management and Structured Approach, (GAO/T-AIMD-97-173, September 25, 1997)

Year 2000 Computing Crisis: An Assessment Guide (GAO/AIMD-10.1.14, September 1997)

Defense Computers: SSG Needs to Sustain Year 2000 Progress (GAO/AIMD-97-120R, August 19, 1997)

Defense Computers: Improvements to DOD Systems Inventory Needed for Year 2000 Effort (GAO/AIMD-97-112, August 13, 1997)

Defense Computers: Issues Confronting DLA in Addressing Year 2000 Problems (GAO/AIMD-97-106, August 12, 1997)

Defense Computers: DFAS Faces Challenges in Solving the Year 2000 Problem (GAO/AIMD-97-117, August 11, 1997)

Year 2000 Computing Crisis: Time is Running Out for Federal Agencies to Prepare for the New Millennium (GAO/T-AIMD-97-129, July 10, 1997)

Veterans Benefits Computer Systems: Uninterrupted Delivery of Benefits Depends on Timely Correction of Year-2000 Problems (GAO/T-AIMD-97-114, June 26, 1997)

Veterans Benefits Computer Systems: Risks of VBA's Year-2000 Efforts (GAO/AIMD-97-79, May 30, 1997)

Medicare Transaction System: Success Depends Upon Correcting Critical Managerial and Technical Weaknesses (GAO/AIMD-97-78, May 16, 1997)

Medicare Transaction System: Serious Managerial and Technical Weaknesses Threaten Modernization (GAO/T-AIMD-97-91, May 16, 1997)

Year 2000 Computing Crisis: Risk of Serious Disruption to Essential Government Functions Calls for Agency Action Now (GAO/T-AIMD-97-52, February 27, 1997)

Year 2000 Computing Crisis: Strong Leadership Today Needed To Prevent Future Disruption of Government Services (GAO/T-AIMD-97-51, February 24, 1997)

High-Risk Series: Information Management and Technology (GAO/HR-97-9, February 1997)

(511463)

Mr. HORN. Well, we thank you very much, Dr. Stillman. You are always very helpful.

Our next speaker and presenter is Mr. Dennis Grabow, the president of the Millennium Corp.

Mr. Grabow.

STATEMENT OF DENNIS GRABOW, PRESIDENT, MILLENNIUM CORP.

Mr. GRABOW. Good afternoon, Mr. Chairman. Thank you for inviting me to come before you today.

As the financial person on this panel, we bring a sense of realism because we look at the year 2000 from an economic issue, we look at it as a wealth transfer issue. All of our research that we have gone through during these past couple of years indicates how there are so many details involved in year 2000, and they are very important.

However, we need to step back and become a realist and look at the process that we are going through. To reach compliance is a very difficult thing and it's important to understand the technology. The technology is the answer to how we will actually achieve success. I find that the ultimate goal is to be compliant. That is going to create wealth for our country, for our communities, for corporations and for individuals, and, therefore, we believe that the ability to have a compliant strategy is important in terms of understanding this issue. We believe that a new investment model, a new way of looking at this issue is required. Oftentimes we get buried in the many details that get discussed.

As we step back and examine this issue, we came to the conclusion in December 1997 that we were forecasting an economic recession, a global economic recession, and it is not exciting to talk about that. I would like to say that I am an optimist, a supreme optimist, but I am also a realist. As a person dealing with people's finances, we are entrusted with the fiduciary duty of their wealth. So, therefore, it's important to come to this conclusion and look at it in a realistic manner.

We come to the fact that we will have a recession from two key ingredients. One, unfortunately, is the public sector, and I would like to at this moment thank you and your committee for the important work that you have done. It is very critical in the analysis in coming to some of our conclusions. Unfortunately, I think it's time that we have to recognize that the U.S. Federal Government is going to suffer some impairment because all this work cannot be done in time. As you point out in your many reports, we are talking about many of the mission critical systems not being completed, lest we not forget, probably two-thirds of all the other systems that are going on within these various departments add value as well.

In our economic analysis, Government does have value. In today's world, the U.S. Government accounts for approximately 19 percent of GDP. If you drill down into adding the Federal, State, and local public sectors, we are over one-third of our U.S. economy. Unfortunately, when you look at these other public bodies, their work toward remediation is not as successful as we would like to see it.

If you then look broadly across the world and recognize that our Government is the only one that can produce the type of report that you have done so well in preparing, it leads an investor to come to some conclusions about what is taking place with other Federal Governments around the world, and that brings us to our next concern, which leads us into foreign trade. There has not been much analysis.

We issued a white paper recently called ships, chips, and slips, where we detail all the technology activities that are dependent on foreign trade, both mission critical, nonmission critical, and embedded systems. Technology supports the international trade transaction. If you look at an average trade transaction, there is anywhere between 10 and 12 different organizations, from the purchaser to the seller, a couple of banks, a couple of port authorities, maybe five transportation companies, including ships, and I might add, we have studied ships at great length and they do have concerns on the embedded system sides and have to be checked. There are also finance companies, warehousing. Altogether, these 10 or 12 organizations all communicate through the method of various technology platforms. The other part of a foreign trade transaction, which is so critical, is there is 10 to 12 sequential steps. The flow of paper and the flow of goods have to occur in time. They can't be out of order or the process breaks down.

So as investors, and as people that are knowledgeable in understanding the process of remediation and understanding the process of these technologies, we come to the conclusion that foreign trade, unfortunately, is going to decline very rapidly and very quickly as we move into next year. This is going to affect many areas of the Government and the private sector. For example, agriculture will be very important and there will be a significant impact there, as well as many other areas.

The things that concern us, as we look ahead, is basically the lack of understanding. We think it's important and we applaud what was recently said here by the GAO, in terms of coming to a definition and a guideline, we think that that is very important.

I would second your comments that you made just a few moments ago, that the administration must come to weekly reporting. We don't have time. I strongly would recommend, we don't have time to wait for monthly reports. We see this in industry. I cochaired a convention in New York of a bunch of investors and there was a gentleman from Kraft Foods that was there, and they are using weekly reports to monitor their progress and to try to ascertain any slippage. I might add that he said that he was a very knowledgeable manufacturing executive and he knew about the year 2000 in 1980. He tried to work around it, Mr. Chairman, and he couldn't. It's a very difficult issue on the manufacturing floor, and we believe that the ultimate economic impact to our Nation and around the world is going to be felt through the embedded system area.

We talk to many people in almost all industries of our economy and walk away with a very clear picture. And what in our view is misunderstood is the importance of compliance, and what we are suggesting is we need a national debate to begin today, throughout the country, on the area of compliance and its importance. I would

liken it to when President Kennedy challenged the Nation to put a man on the moon. This is equally as important and equally deserves the attention of our country.

That concludes my remarks, Mr. Chairman. I would be happy to answer any questions.

[The prepared statement of Mr. Grabow follows:]

Testimony of Dennis G Grabow
Chief Executive Officer
The Millennium Investment Officer
Before the

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY,
COMMITTEE ON GOVERNMENT REFORM AND OVERSIGHT

June 22, 1998

Mr. Chairman and Members of the Committee:

Through the exceptional work of this Committee, others in the Congress, determined organizations and individuals, the scope and potential impact of Year 2000 is becoming more apparent. This is clearly a tremendous technological challenge of unprecedented scope and we believe that your diligent work on this issue is of tremendous importance to our country and our economy.

At The Millennium Investment Corporation, we focus on the global financial implications of the Year 2000. From a financial perspective, Year 2000 is a worldwide challenge with tremendous economic implications. Technology is a fundamental driver in our ability to achieve efficiencies and increase productivity and compete globally. Worldwide, disruptions in technology will slow production, and the delivery of services and information.

In December 1997 we predicted a worldwide recession based on the impact of Year 2000. Nothing in our continuing work causes us to rethink our views. If anything today we are further behind in the remediation and implementation process than we would have expected at the end of last year when we made our initial forecast. The work in embedded systems is still lagging especially in small and medium sized organizations.

Year 2000 is a so significant because so much of our economy is linked to technology. From electronic financial transactions, to flow controls in a factory, to the heating system in a high-rise office building, technology drives the system. It is a patchwork of technologies that is now roughly 40 years old, and in serious need of attention.

However, rather than being able to upgrade our systems over time, Year 2000 is forcing us to compress the process. This process will be no doubt painful but the long-term affects will be very positive. In solving the Year 2000 problem we will have, collectively, upgraded our technology infrastructure and prepared ourselves for a period of growth -- growth driven by efficiencies in production, the delivery of services, and telecommunications.

If you compare Year 2000 compliance with other initiatives, such as converting our lead-gasoline based systems to an unleaded systems, or converting our wire-based telecommunications infrastructure to a fiber optic based system, you can begin to see how older technologies simply need to be updated to meet current needs. The key difference with Year 2000 is that we do not have the luxury of time to phase in a compliance strategy. It has to happen now. And the result of non-action will be harsh.

We are especially concerned about four Year 2000 factors. First, we do not have the resources to complete the reprogramming, replacements and repairs required in the timeframe available; second, technology failures can have a ripple effect in the economy; third, government: and four, international trade, which impacts such a large sector of the economy, will be adversely affected by Year 2000.

Specifically, in international trade we have a high level of interdependency. International trade is built upon a global network of interdependent relationships and interdependent technology. Inherent in every transaction are three levels of risk: Internal risk is present in all the systems and processes within an organization required in an import/export transaction. External risk should be considered in the systems

and suppliers required throughout the transaction This can involve several companies, government agencies, and all the technology involved in manufacturing, shipping, port authorities, insurance, financial transactions, storage, and inspections. Infrastructure risk is found in transportation systems, power, water, and all other services that allow companies and municipalities to conduct business.

Every import and export transaction involves a number of sequential steps and several companies, including transportation companies, ports, freight forwarders, banks, and warehouses as well as government agencies. All these entities rely on information technology systems and embedded systems, which may or may not be in compliance for the millennium date change. We simply do not believe this system will function properly. Further complicating this transaction is the inability to actually test the systems until January 1, 2000, due to the virtual endless combinations of technologies and enterprises comprising a foreign trade transaction.

As we move to a Year 2000 compliant economy, we believe some countries, companies and individuals will thrive while others will struggle and be left behind. Those that have prepared for Year 2000 will be in a far better position to compete and move forward. Therefore, as an economic factor, we believe that Year 2000 is the single most important wealth transfer event of this century.

The same dynamics were present in the economy in the early 70s when early adopters of technology and computing became dominant players in their market. The key difference is that Year 2000 is not simply an opportunity to get ahead – it is an imperative to ensuring the that our economy is not crippled by shutdowns, slowdowns and system failures that are currently being registered and could continue into the 21st century.

We also recognize that Year 2000 has implications well beyond the financial and the strategic. Technology also is in our lives at the most basic level and we expect to see individuals and families affected by failures in the electronic equipment they depend upon. We are especially concerned about public infrastructure and disruptions in the delivery of essential services.

Compliance is the Goal

The level of disruption and the shift in wealth is based on one simply principle: Year 2000 compliance. Compliance is not an option. Compliance is essential, and compliance must extend to information processing and embedded systems. Currently, we see companies focusing on their mission critical information processing capabilities and largely ignoring the impact of embedded systems.

The great economic benefits obtained from technology are derived from properly working systems. Right now we know these systems can not all function smoothly into the next millennium. For example in the case of the Federal government, by its own self-analysis, it is impossible to achieve compliance over the remaining months. Therefore it is time to begin planning to mitigate the inevitable disruptions.

I realize that this committee is focusing on recommendations and solutions and I believe that risk management is a critical part of the solution. Risk is inherent in any electronic equipment and in every business process that interacts with an electronic system. This is a long-term issue and we see an inadequate understanding of the risk because most people assume everything will be fixed and working properly (over the next 18 months). Our research indicates this is a faulty assumption with significant economic consequences.

Year 2000 a Misnomer

At this point let me clarify why we need action now. The name, Year 2000, is a misnomer. People seem to lock in their minds that on midnight of December 31,1999 we will see the bite of "the bug." No question this will begin the period of significant system failures. However, the reality is system failures have been occurring already and they will increase significantly as this year ends.

In particular on January 1, 1999, our research indicates, the rate of failures in information systems (management reports and financial statements) will begin to be visible to many organizations that have not completed their remediation. Further for technical reasons we anticipate failures also to start showing up

on January 1, 1999 in production facilities as well Those companies utilizing just-in-time inventory methods may begin to experience disruptions from the flow of goods in the economy We have been lulling ourselves into a false sense of deadlines, believing we still have time.

Economic Forecast
Our forecast is predicated upon the lack of resources available and the slow pace to compliance primarily in production equipment. Embedded system remediation is more complicated with longer lead times, compared to fixing information processing systems.

Further, we see that our federal government is behind schedule in meeting its compliance goals. This will begin to erode the ability of services to be delivered and restrict government spending on projects -- which is a key economic driver.

Overall, 1999 will be a difficult year in the economy, as system failures begin to occur both in information processing and in production facilities. This will have the resulting affect unfortunately of gradually increasing the unemployment rate throughout the year.

By our research, state and local governments are also behind schedule and may also see service and performance loses. We also note the increasing intensity of concern regarding Year 2000 by governmental agencies with regulatory responsibility. At some point, these agencies will be forced to take action against companies to protect the public interest and control the scope of problems created by non-compliant systems.

Over the next several months, as system failures intensify, companies will simply pull back, retrench and moderate their internal and external expansion plans to protect their operations. We also predict that some companies who can not or will not reach compliance will choose or may be forced into bankruptcy as a strategy.

Recent mergers and acquisitions may prove to be an albatross to those acquiring companies as they learn they have acquired even more Year 2000 work, thus increasing risk to their capital structures. Our research indicates many transactions currently being completed in the marketplace do not adequately take into account Year 2000 due diligence. Further in disclosures in public documents, based upon our knowledge of Year 2000 remediation issues, companies do not appear to be fully disclosing their risks. This in our view is largely due to their uncertainty of what really is Year 2000.

Further as banks and finance companies move further into the financial implications of this issue we believe credit rationing and ultimately a credit crunch will occur. Just like in the early 1980's these lending institutions will find a safe harbor in purchasing government bonds rather than lending to other institutions.

Therefore, financing of the remediation process will take on a significant determinant of ultimate success to compliance. Again, from a financial perspective, we see this process as a necessary means to create a more fundamentally sound technology infrastructure.

Three factors in our wealth transfer analysis that affect all companies are: public infrastructure, international trade and government. We are particularly concerned about these areas because all are in serious trouble today, in respect to Year 2000 and there is a void in leadership in managing these areas.

As we have learned from recent disruptions in our phone system, when a single satellite failed to operate, it created tremendous disruptions in paging, cellular and other telecommunications. When a company shuts down, from a strike, weather conditions or other reasons, it can send a ripple affect throughout the economy. If we see disruptions in airline travel, in electrical service, parcel delivery, telecommunications or other essential services, our economy will be affected.

Year 2000 Definition
The first step in addressing compliance is to have a consistent definition of the problem. Year 2000 is an issue that involves five areas. You cannot inquire about only one area of compliance and expect to

evaluate an enterprise for total Year 2000 compliance For example, this is not just a mainframe issue The awareness may have started years ago in that area, however, preparation, contingency planning and the resulting economic consequences will be felt from five distinct areas.

Our model for Year 2000 investment analysis encompasses reviewing government, business and production facilities for:

Technology risk factors
1. Information processing – mainframes, client server, personal computers, etc.
2. Embedded systems – microprocessors, programmable logic controllers, etc.

Enterprise dependencies reliant upon information processing and embedded systems
3. Ripple effect – the vender and customer chains
4. Infrastructure – electricity, water, telecommunications, transportation
5. Government – federal, state, and local

Together all these areas have a cumulative impact on the operations of an enterprise whether a corporation or government agency, and have to be examined for Year 2000 consequences.

Managing Expectations
Sometimes this huge project management task can seem intimidating. Everyone I know who is involved in the details of the issue has a very healthy respect for the task. It should not be underestimated, but it should not be feared either.

There will be disruptions. Some will create minor nuisances. Others will be far more serious. My point is that Year 2000 is a national issue, with far reaching economic consequences and we need to address this from a national level.

Like any other challenge we have faced in our country, the American Spirit is ready to rise to the occasion. Throughout our history as a Nation, our citizens have proven they can respond to goals.

What we do need is focused national leadership to lead us one more time to the future we are all seeking together. We cannot hide from the eventual outcome. The American people and others around the world need to be prepared and educated to the possible outcomes. What we don't like are surprises.

Although this Committee, as well as other leaders in the Congress, government agencies and others have been working diligently to bring this issue into focus for the American people, we need to engage everyone in the process.

How difficult the transition will be and the final outcome will be dependent upon the will of our political and business leadership to respond to the Year 2000 challenge.

Plan of Action
The question we are being asked is what are the solutions, what can we do now to prevent or reduce the impact of Year 2000? We have a number of recommendations.

First, we need to adopt and disseminate the real definition of Year 2000 as discussed earlier. To most people, Year 2000 is a computing problem that affects information processing. That is really only about 20% of the picture. To find and repair faulty chips is far more expensive than reprogramming a computer. So we must develop an understanding of Year 2000 that accurately defines the problem.

Our second recommendation is to define a process by which individuals, companies and government agencies can reach compliance, reduce their risk and consider contingency planning. Our definition of this process involves these steps: an inventory of systems, analysis of the condition, developing a compliance strategy that focuses on mission critical systems first, but addresses all systems, testing systems to

determine what needs work, implementing fixes and then retesting equipment. Testing is, by our estimates, about 50 percent of the commitment and most of the situations we track do not provide adequate time or resources for testing.

Our third recommendation is to provide intensive leadership at all levels of our society. We need all of our government and industry leaders to come forward with an accurate profile of what we are facing as a nation and what we are going to do to solve it. Currently we see companies hesitant to come forward for fear of legal action or they do not want to indicate that they project "disruptions" from Year 2000 problems. But the aim of leadership should be cooperation and guidance, not intimidation and regulation.

In January, 1998, 80 business leaders and academics sent a letter to the Prime Ministers of Canada, the United Kingdom and President Clinton expressing their "astute concern" over the lack of action over the "Millennium computer crisis". The letter, signed by members of the British North-American Committee, urges leaders to "deal with the Millennium bug as a top priority in the brief time that remains."

A fourth recommendation is to develop a "national compliance strategy" that places compliance as our Nation's number one goal. The Nation must take on a national debate of the importance and seriousness of achieving compliance. Although we will not get there in time, it will focus attention on compliance and create the necessary framework for risk management and contingency planning.

I feel this effort is consistent with the national initiative in the 1960s to put a man on the moon. At that time, President Kennedy articulated the national imperative to be first in this effort and Year 2000 is equally or even more important. This is an issue that will define our ability to compete in the years ahead, and to continue to lead the industrialized world in an information-age economy.

In other wealth transfer events of the last 25 years, such as globalization, the Internet, and the growth of computing, market forces largely controlled shifts in wealth. Technology has been a tremendous economic force worldwide and the U.S. government has supported and encouraged the use of technology to drive productivity. However, Year 2000 is different and demands a different strategy. Year 2000 is not a productivity issue or simply a technology issue because electronic systems are central to our basic economic structure. We must be more proactive in protecting the technology framework that supports our communities and our economic systems.

My fifth recommendation is that we present Year 2000 as a positive event in our evolution as a technology-driven economy. This is a challenge of tremendous proportion but it is a challenge of will. We know how to solve Year 2000. The question is whether we have the will to do it.

The sixth recommendation would be to review financing for Year 2000 at all levels of government. With the forecast of a recession many of the recent increased revenues coming to government from income taxes and capital gains would be reduced at a time when there would be an increase in demand for government services. This could clearly create a budget shortfall for many public bodies rather than the current surplus condition as found in some cases.

The following are some further thoughts for possibly a later discussion. Certain sectors of the economy like the medical industry, which derives significant revenues from government, may need special assistance, like in the form of block transfers of funds in the event transaction systems are not functioning properly.

Contingency planning throughout the public sector will be an important part of the planning process for Year 2000. One thing is also certain, Year 2000 is a dynamic event, not static and will require constant evaluation as we move toward compliance.

To add a sense of urgency in the government I would recommend weekly reporting of system progress to identify lagging programs quickly and to instill within an organization the overall time constraints. The current quarterly reporting is insufficient for rapid response.

We recognize the scope of this issue and these are just some initial thoughts and time will not permit an all-encompassing discussion.

However, as a first step, if we can galvanize the Nation toward a goal of compliance and send the message across the land and to all our trading partners and friends, of the importance and seriousness of Year 2000, then I think we are on the road to a prosperous new millennium.

In closing let me indicate the important role this Committee has provided by informing us of Year 2000 status within the government. Many of us deal with this information on a daily basis and find it very important in our analysis. On behalf of all those who have seen and used this material, thank you for your diligent and forthright efforts.

Mr. HORN. That's a most helpful statement. I think you are right on target, based on your private experience that you have had and are involved with.

The next presenter is Mr. Dan Steinberg, who is the president of Synthesis: Law and Technology.

Mr. Steinberg.

STATEMENT OF DAN STEINBERG, PRESIDENT, SYNTHESIS: LAW & TECHNOLOGY

Mr. STEINBERG. Good afternoon, Mr. Chairman. I am pleased to appear before this committee to discuss the problem and the top priorities for action/reaction. My top priority today and for the rest of the time remaining is infrastructure. Infrastructure is the key issue, in my mind.

I am focusing in my oral testimony on telecommunications and electricity, but there are parallels in all the other infrastructure sectors. First, the risk. The big risk in all infrastructure is the risk of cascade failure; that is; the risk of one thing bringing down everybody else. This kind of cascade failure is hard to predict, difficult to prevent, and hard to diagnose, even after the fact, as AT&T found out recently in a non-Y2K related major failure that they had. What happens is in the field things don't work the way you expect them to.

To illustrate this, I use the example of Viagra, and no, this is not a Viagra joke, it's deadly serious. People died. Why did they die? The unexpected happened in the field, and I leave it to your imagination what the field is, but there was an unexpected interaction, despite the fact that they did incredibly exhaustive testing on this drug and had full regulatory oversight. The unexpected happens.

How does that relate to what I am talking about today? Here is an example a little closer to home. This is my PCS phone. When I came off the plane on Saturday, I turned it on, I had messages waiting, I said, OK, I have to retrieve my messages. Sorry, this code is not recognized. The carrier here doesn't recognize the codes from my carrier in Canada. It also decided that my phone had caller ID suppressed. I don't suppress caller ID, I want the world to know who I am when I call. Now that could be really critical if there was an emergency call I am trying to make and somebody has caller ID suppression rejection, as I found out.

So what it is is the various telecom players can't get it together to agree on the simplest thing like how to retrieve a message, what is caller ID, how do you suppress it, how do you decide whether it's there or not. Things happen unexpectedly in the field and they don't even interoperate perfectly or 100 percent in a day-to-day operation, and that makes me pretty worried. In case of telecoms, we in North America, and I speak as a Canadian, although not as a representative of the Canadian Government, are connected to the world, and there are many, many, many candidates for failure and we can't even decide who they are today. I can't point any fingers.

The World Bank just did a survey, released, I believe June 11, and half the people basically failed to respond. But I know from a bitter experience that the foreign players are most likely way, way, way behind us. Because, first of all, they have less access to information. Ninety percent of the information on Y2K is published and

disseminated in English, which is great for us but terrible for the rest of the world who doesn't speak English, and this is highly technical information that is not suitable for that automated translation you get in consumer electronics that you sort of wonder about.

They also have less money. This comes as no surprise. We give foreign aid to most of the world. It should be no surprise that those without sufficient funds, who are worried about funding right here in town, they cannot solve their problems quickly enough.

There are cultural differences that in some cases make disclosures difficult. I am not knocking any particular culture, every culture has a hole, but in this case there may be certain barriers to full disclosure that will keep them behind us. God knows it's hard enough to get disclosure in North America.

Finally, every country has a different regulatory environment and in some countries, if they have to make a change to telecom infrastructure because the existing standard doesn't work, it may be against the law. We certainly don't have time to renegotiate telecom agreements. They take years to do. We only have a year and a half left.

Given all this, what can we do to decrease the risk? Well, I frankly don't understand why firms have been reticent to make full disclosure. It is really in their best interest. If a firm knows that something is likely to fail and they fail to disclose it, they are opening themselves up to a big time lawsuit, the kind that makes the papers. Now, if they make a disclosure, sure, they may lose some business, but what is likely to cost more, losing a little business or a few dozen big time lawsuits?

The thing you have to remember about disclosure, for those in the audience who are fortunate enough to not attend law school, is upon disclosure the plaintiff has a duty to mitigate. That means they have to safeguard property against loss; they have to seek treatment if there is a likelihood they are ill. In short, they have to do what it takes to minimize their loss, and if they are minimizing their loss, they can't sue for as much. Now, in some cases, it's impossible to mitigate, but those are rare cases.

Now, the disclosure I would like to see mandated is what are firms doing to investigate their international partners' compliance, and what steps are they taking to insulate themselves from cascade failure, because knowing about something and doing nothing about it is almost as bad as not knowing about it in the first place. But if they have to disclose, they have to investigate, and if they have to investigate, who knows, they may even do something.

I am looking, in general, to narrowly tailored remedies. Those recent broad brush, safe harbor legislations, I am very much against them. They will have the potential to trigger lawsuits early, encourage people to do forum shopping, and most importantly, they will decrease or eliminate the very reason to work on compliance that has finally gotten people to do some work, which is the fear of being sued. The fear of failure was not sufficient back in 1996. It took people worried about being sued to get them started, and I am not recommending any massive new disclosure requirements.

In summary, what I am recommending is, first, a declaration by Congress that Y2K is a global problem, a call to officers of infra-

structure companies to recognize the advantages of disclosure, mandating specific disclosure of the investigation of the compliance of their partners' services, not their coffeemakers, and the steps they are taking to insulate themselves from cascade failure. If you are going to have that disclosure, you need some sort of watchdog agency to track these disclosures and issue a report card on a regular basis. That is the stick. The carrot might be some form of limitational liability here, not outside of the country, for losses due to cascade failure for firms that disclose the risk in advance, with evidence; and, finally, some sort of mechanism to protect infrastructure here from lawsuits, if they have to cutoff a foreign partner in contravention of any existing agreement.

I thank you for your interest in the year 2000 problem, and I would be happy to answer any questions you may have at this time.

[The prepared statement of Mr. Steinberg follows:]

STATEMENT OF DAN STEINBERG

PRESIDENT

SYNTHESIS: LAW & TECHNOLOGY

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION AND TECHNOLOGY OF THE COMMITTEE ON GOVERNMENT REFORM AND OVERSIGHT

UNITED STATES HOUSE OF REPRESENTATIVES

June 22, 1998

Good afternoon, Mr. Chairman. I am pleased to appear before the committee to discuss the year 2000 problem and the top priorities for action. My focus today is on electricity and international telecommunications. But the process of finding that focus is almost as important. I have been studying the Year 2000 problem for over 3 years, and actively helping the Canadian Federal government and private sector clients with their own quest for compliance. In all cases, the exercise of risk management has led to the conclusion that there is much that is beyond the control of any individual organization. In general, I see three areas of concern:

- Government progress
- Infrastructure
- International

The committee is already seized with the issue of Government progress, so I see no need to discuss it further. Of the remaining two, the biggest remaining priority should clearly be infrastructure. As the CIO of a local bank recently remarked (off the record, of course) 'it doesn't do a lot of good to be compliant and test our partners' systems if neither of us has electricity'. Infrastructure is something we tend to depend on without giving much thought. More important, much of the current infrastructure crosses state and National boundaries. Crossing borders makes intervention more challenging, but still feasible. Everyone has their own priorities, but most agree that critical infrastructure includes:

- Banking and financial markets
- Electricity
- Water
- Fuel
- Telecommunications
- Transport

Every single one of these has an international component. I will focus on electricity and international telecommunications in my examples, although there are parallels in other sectors. I have included a list of key questions regarding other infrastructure components as an appendix to this testimony. But again, my focus and my recommendations are on electricity and international telecommunications.

Let me begin with telecommunciations. It is the international component in many cases that makes this challenging. Why is the international aspect a problem? First the basics. Everything you have already heard about Y2K in the US is true for the rest of the world. What you have probably heard includes:

- 82% of Project Managers decided afterwards that their preliminary budget was too low (Cap Gemini survey)
- projects started late
- it took a while to get senior management involved.

It's a serious enough problem here in North America to require regulatory intervention, government oversight at various levels and a massive awareness campaign. In an international context, the problem is:

- the rest of the world has less information that we do. A large percentage of the work written about Y2K is in English, and those that don't speak English very well are at a distinct disadvantage. They don't have ready access to the volumes of awareness, technical and legal information available to North American firms. And the limited amount that may get translated might not even be applicable. For example, there is a dearth of civil law information on Y2K liability. Yet much of the world operates under civil law. English-speaking common law jurisdictions had the benefit of discussing legal issues since at least early 1996. It is difficult to get lawyers to agree on anything, but in the intervening years we have at least managed to gain consensus on the major issues. This process is only just beginning in many civil law jurisdictions. And they have just as much trouble reading each others' languages each other as they have reading English.
- Other countries have very different regulatory environments, so they may be slower to require disclosures. They may be required by law to follow certain standards that North American companies have learned to avoid in the interest of Y2K compliance. In some cases, regulatory waivers may be required in order for them to achieve compliance and interoperability with North America.
- In certain cultures, admitting to a mistake is a serious loss of face. This may have caused them to delay longer than we in North America did. We in North America have (for the most part) have finally moved on from trying to assign blame into the challenge of getting things fixed in time. This transition may be delayed in other countries for the above-mentioned cultural reasons.
- Other countries just don't have the same level of financial resources. Any country receiving foreign aid should be suspect as they have already demonstrated that they are lacking in resources.

As much as it might be tempting to walk away from these countries, we have to interact with them. North American firms buy/sell products/services globally. Infrastructure components like banking, telecommunications, etc. are interconnected in shared infrastructure. This view is shared by the current administration. In his testimony before Congress April 1, 1998, John Koskinen said:

> "Finally, the Council will have a world-wide focus. We live in a global economy that is increasingly dependent upon the electronic exchange of financial and other data. Unfortunately, it is not clear that all other nations are devoting the appropriate level of attention to the year 2000."
>
> "While this is the one area in which the Council may have the greatest difficulty in exercising influence, we need to do everything that we can to raise awareness in other countries. Therefore, the Council will work with Federal agencies to leverage the influence of international organizations like the United Nations, the World..."[1]

With respect, I think that there is more than can be done and should be done on an international level. There is a risk in almost all infrastructure of cascade failure. That is the failure of a component causing others to fail as well. Often, cascade failures are brought about by the simple process of a component broadcasting too many error messages. Because of this, we have to attack the problem on two fronts:

- Decrease dependencies on foreign telecommunications infrastructure
- Increase their level of activity

Telecommunications

A key target for this action is telecommunications infrastructure. Telecommunications failure could have catastrophic impact on business and public security. Unfortunately, even today there is some disagreement as to the extent of the telecommunications problem.

> "Fortunately, telecommunications networks are designed to be fault-tolerant and there is no reason to believe that one or two Y2K-related failures could lead to a chain reaction that could disable large parts of the nation's telecommunications networks," Powell said in his testimony for the House Ways and Means Committee's oversight subcommittee.
>
> The FCC, however, couldn't provide the General Accounting Office, Congress' watchdog agency, with data on the progress being made by major long-distance carriers to fix their Year 2000 problems, according to GAO official Joel C. Willemssen.[2]

---

[1] http://www.y2k.gov/council/tt040198.htm

[2] http://www.chicago.tribune.com/version1/article/0,1575,SAV-9806170080,00.html

To add perspective to this uncertainty, remember the recent AT&T outage. The whole network was brought down by what amounts to the broadcast of errors encountered during the testing of a device. A large number of error messages being broadcast over a network can flood that network and effectively shut it down. This is called a cascade failure. Considering this domestic example, how likely is it that international telecommunications carriers will bring down our domestic network? How should we protect ourselves?

We live in an exceedingly complex world, where unexpected interactions are a fact of life. Consider Viagra. This drug underwent extensive testing before release. Yet several people died. These people were cardiac patients. Most of them were used nitroglycerin as well as Viagra. Viagra is a vasodilator. It 'loosens' the blood vessels (primarily in a certain part of the anatomy), facilitating blood flow. 'Nitro' is also a vasodilator. One of the first things they check for drug interactions is synergy between common products (like using two drugs that have a vasodilator effect). So why did people die? Didn't the company test this? Didn't the regulator verify the appropriateness of the drug testing before granting approval? Of course they did. In the lab. What they probably failed to account for (and who can blame them) is what happens 'in the field' to people of that particular age group. You can bet that the company didn't want people to die. You can bet that they spent many hours working on product safety and thinking about the possible problems. Yet people died just the same. And you can bet that someone will get sued as a result.

The same kind of unexpected results can happen in telecommunications 'in the field'. So it is reasonable to expect that even with extensive testing, there may be some failures in local infrastructure. As a resident of the Northeast, I can personally testify to the inconvenience brought about by this winter's weeklong freezing rain in January. No one could have prevented the major hydro pylons from falling after a week's worth of ice. But what could have been prevented were the thousands of local failures and consequent cascade failures because the trees near the power lines were not cleared often enough. It looked like a good idea at the time: clear away from the local lines every two years instead of one. Save a pile of money. But again, they failed to consider what could happen in an extreme case (more than two days of freezing rain at a time). As the incidents piled up in the command centers, two things happened. They ran out of fresh troops to fix the lines and the managers started seeing double in the command centers. In both instances personnel started making mistakes from fatigue. Will they get sued? Probably. If I wanted to, I could be first in line. But I would rather they took steps to avoid a repeat performance. The biggest thing they could do for me (short of putting all wires underground) would be to ensure that their own standards for the right-of-way are enforced on a yearly basis. Think of this as a simple innoculation against some of the effects of freezing rain. It's not much to ask in retrospect, but I would probably have more luck with a lawsuit. I may end up having to file just to force the utilities to do something. Bottom line: no one can say with absolute certainty today that there will be no disruption. It's just too much to ask.

Because of this, for Y2K, we actually have time to do analogous "innoculations' up-front This applies both locally and internationally. It is therefore imperative that the level of remediation and testing of foreign telecommunciations infrastructure be as thorough as possible within the current time constraints. If they don't make sufficient progress, we have to do something:

- Embarrass them with disclosures, or
- Exercise regulatory authority or some other means to cut them off. It is possible under existing law to direct regulatory authorities to cut foreign dependencies to protect American interests.

Key questions (I have to admit that I don't have answers):
Given the risk of cascade failure, it makes business sense to plan for such a contingency. At what point does it become the obligation of a telecommunications carrier to cut off a foreign country to prevent cascade failure? Can it be done pre-emptively? Do the carriers know themselves? Most importantly, do they have the right to take unilateral action under their existing agreements?

Electricity
From recent Senate testimony:

> Only two out of 10 of the major utilities contacted by the US Senate's special committee on the Year 2000 issue said that they had even completed an assessment of what had to be done. More disturbing, none have formed any contingency plans to cope with computer failures.[3]

It is evident that the local regulators have been unable to get the public utilities to take appropriate action. Electricity is in most jurisdictions a regulated monopoly. That means that citizens cannot go to a competitor if they suspect their supplier will have a Y2K-related failure. But the users of electricity will certainly be upset if such a failure occurs and there will undoubtably be lawsuits. It is clear that here is an excellent opportunity for disclosure as a means to diminish the legal bloodbath and perhaps decrease the possibility of injury or death. Another way to avoid lawsuits would be to provide safe-harbour legislation, but that would serve to remove the reason for remediation.

Again, there is the possibility of cascade failure. I spent a few nights in the dark because of failure somewhere else on the grid gave my local transformer farm a serious case of indigestion. I learned a lot more about the fragility of the grid than I really wanted to. This leads me to suggest that utilities should take steps as well to innoculate themselves from cascade failure.

At what point does it become the obligation of a public utility to cut off another utility in order to prevent cascade failure? Can it be done pre-emptively? Do the utilities know themselves? Most importantly, do they have the right to take unilateral action under their agreements?

---

[3] http://webserv.vnunet.com/www_user/plsql/pkg_vnu_news.right_frame?p_story=56468

Summary of Recommendations.

THINK GLOBALLY, ACT LOCALLY

The timeframe for action is short. For this reason alone, I cannot recommend an omnibus bill that will be referred to too many committees and be delayed. Rather, I propose the introduction of limited changes. These recommendations serve to diminish the risk of infrastructure failure and at the same time diminish some of the risk of litigation. Litigation is a Sword of Damocles hanging over all businesses (and many governments). There have been many estimates as to the litigation amounts. Some have said trillions, but who really knows? We can't reliably predict the quantum of the damages until we know what will fail and how well people are prepared for failure.

The key to this is disclosure. In general, it is in an industry's best interest to disclose potential loss to the right people. This is a good way to avoid punitive damages (unless the risk was disclosed foolishly as in warning that a dam would fail without any evidence of cracks or leaks). On an individual basis, firms normally weigh the risk of loss due to disclosure (lost sales, decreased share price, etc.) against the risk of damages subsequent to an actual event. To get around this balancing act, it is easier to get disclosure from industry associations.

What is key is that once a risk is disclosed, there is a duty to mitigate where a potential plaintiff has been put on notice. Plaintiffs (in general) must take reasonable precautions to:

- preserve and safeguard property
- seek treatment in the event of injury
- etc.

So the declaration of a forseeable risk should preclude recovery of the big ticket additional damages. In the case of a monopoly utility, there is not even an immediate business loss to be weighed. But unless the disclosure was deemed reckless, there should be no liability to a power company if a property transaction failed to close because the buyer didn't want to locate in a neighbourhood where there was going to be a power failure.

In other industries, disclosure does raise the possibility of loss of business, and companies have to weigh this possibility against the size of the eventual lawsuit(s). But even in non-regulated environments, I believe that the benefits will always outweigh the upfront costs of disclosure. It has been said that disclosure will bring on lawsuits. My contention is that the lawsuits would occur anyway if there is a failure. Disclosure may affect the timing, and it certainly should reduce the amount of damages, but it should not cause any new cause of action to be created.

My recommendations follow the theme of measures to encourage disclosure in key infrastructure industries. Again, my position is that broad brush measures are inappropriate for this crisis. There is not sufficient time to fine-tune such measures and there is a serious danger of overkill. Rather, I propose the following narrowly-tailored remedies. These remedies target infrastructure players in an attempt to get them to insulate us from both local problems and foreign failures over which they have limited control.

In the short-term, I propose:

1. a declaration by Congress that Y2K is a national and global problem of the utmost urgency
2. a call to officers of infrastructure companies to recognize the advantage of disclosure in preventing certain lawsuits (irrespective of opinions to the contrary by legal counsel). To be effective, someone should go and talk to these officers and explain the ramifications of disclosure.
3. mandating specific disclosure on the steps each public utility (and possibly other infrastructure player) is taking to prevent a cascade failure This puts the focus on what's important without imposing an overly onerous reporting burden. It's simple and doesn't involve setting up a massive organization to track progress either. If utilities have to report on it, they have to think about it. If they have to think about it, maybe they will actually do something about it rather than face lawsuits from unhappy customers.
4. Establishing a watchdog agency to track progress of critical infrastructure industries in both remediation and disclosure
5. A limitation of liability for infrastructure companies **solely** for domestic fallout from international failures. This may require the proviso that the likelihood of such failures must be declared in advance AND backed up with evidence. This relief could conceivably be extended to other industries if it proves effective.
6. Provision of a mechanism (i.e. protection from lawsuits) whereby the US could force/permit infrastructure players to unilaterally cut off foreign partners and/or entire countries if it appeared that they could impact services. This is similar to the use of the right to adequate assurance of performance under UCC 2-609 and the UN convention on the international sale of goods (articles 71 & 72), but would specifically targets services.

While not the focus of my presentation, there are minor measures that could be undertaken to facilitate government Y2K progress as well. These are items to consider in a few months' time (or earlier if things start looking bad):

- suspension or elimination of 3rd party treble damages in Y2K contracts governed by FAR & DFAR
- a specific attorney/client priviledge for all government. attorneys working on Y2K if government. priviledge gets deemed inapplicable by the courts
- require a full Y2K legal audit for all public companies, the idea being that once they have the information, it becomes obvious that it is in their best interest to disclose because this information will be discoverable in an eventual lawsuit. This is a last-resort to get people talking, and would need accompanying guidelines/methodology/etc. and someone (another agency) to watch over the process
- specific waivers from anti-trust action on industry cooperation on Y2K efforts. The current statement from DOJ is a non-statement, but that's not what has prevented people from talking up to now. They just didn't have anything useful to share (but they will, and they all have in-house counsel opinions telling that they dare not share)
- specific penalties for failure to perform in a particular industry sector. For example, $100/day per customer for power failures of more than x minutes in a day. Or $100/day/customer for lack of dialtone or international dialtone (as applicable).
- Financial aid to developing countries specifically for Y2K remediation of international infrastructure components.

Finally, I have come up with a list of points I have seen raised elsewhere that I feel would be inappropriate. Things to avoid (if at all possible) include:

- generic safe harbour legislation - any safe harbour legislation would immediately trigger every lawsuit that had not yet been filed and cause plaintiffs to go forum shopping.
- acceptance of the validity of state safe-harbour legislation in inter-governmental agreements. There is no reason to encourage this behaviour and when citizens realize what has happened, the governments that enacted such legislation will be extremely unpopular.
- mandating specific dates for compliance or forcing industries to correct one class of problems over another. This is a good way to get blamed for any messes without really knowing if you are doing good in the first place. Let companies do their internal triage using their own best judgement. You might want to look at penalties for failure to perform, however (as discussed above).
- New bankruptcy protection. There will probably be many firms that try to escape liability via bankruptcy protection. The existing legislation, if adequately enforced, is sufficient to prevent fraud.

I thank the committee for its interest in the year 2000 problem. You can make a valuable contribution to the effort. I look forward to working with you to increase understanding on these issues, and I would be happy to answer any questions that you may have.

APPENDIX A

OTHER INFRASTRUCTURE ISSUES TO CONSIDER

It is clear that governments are seized with the issue Y2K on an international scale But what of the thousands of firms that do business globally (or at least internationally)? There has been much discussion in the literature of the 'food chain' issues and how they affect an organization. The food chain becomes an order of magnitude more complicated when you factor in the international aspect. This paper cannot unfortunately provide answers. In many cases, the questions have not been asked. In other cases, the answer changes so radically from country to country that no generalized statement can be made.

To get the ball rolling, I have assembled a brief list of questions that I believe need to be answered in order to minimize disruption to firms operating abroad. The questions are primarily focused on infrastructure issues. Everyone has their own definition of critical infrastructure, but most agree that it includes:

- Transportation
- Banking and financial markets
- Electricity
- Water
- Fuel
- Telecommunications

Transportation

What if a ship cannot leave harbour because the port is under quarantine? If a countries' medical infrastructure collapses due to Y2K problems in the hospitals, quarantine may be necessary.

What if a ship cannot leave harbour because the harbour infrastructure has broken down? There are many things that can go wrong, including:

- Failure of automated refueling systems
- No working payment system
- Cargo cannot be loaded
- Failure of environmental control systems
- Failure of local infrastructure like electricity, fuel delivery etc.

In both of the above examples, there will surely be insurance claims made. **But who should pay?**

How about airport closures and/or no-fly zones? It is evident that the regulatory authorities will take the steps that are necessary to avoid unnecessary risk to passengers. **But what happens to those caught outside the US?** Unless there is certainty of failure of air transport, it is doubtful that foreign employees will be 'called home'. **Who will pay for their losses? And how will they get home?**

Banking and financial markets

Think of all the steps involved in an international Letter of Credit (LC) It only takes one failure to stop the process If a foreign factory does not receive the LC, they don't produce. If they don't produce, some North American company will be sitting idle waiting for goods. Many firms have sent out questionnaires to their trading partners asking about Y2K compliance. **But how many firms asked the same question of every bank in their LC chain?** And of course the old favorite **"How reliable are the responses?"**

Electricity

As stated in the main testimony, there is some disagreement as to the extent of the problems facing the various public utilities in North America. It is difficult to believe that anyone can say with assurance that they will not have a problem before an assessment has been completed. Has any information on higher degree of Y2K assessment work being done in foreign countries? Not that I have seen. So it is easy to conclude that there is the potential for failure of the grid in foreign countries. The question is: **"which one(s)?"**

Water

Everything that has been said about electricity can be extended to water. In addition, there is a risk not only of delivery failure but quality control problems. This problem is exacerbated in regions where the source water is significantly more 'dirty' than the source for most North American treatment plants. **Can firms operate in foreign countries in the absence of drinking water? Is it even worth trying?**

Fuel

Fuel delivery is dependent (in part) on the transportation infrastructure, particularly large supertankers. There has been much discussion of late on the potential for problems with embedded chips on supertankers. **Can sufficient fuel delivery be guaranteed in foreign countries where firms are operating? If not, can the firms continue to operate?**

Telecommunications

A key target for investigation is telecommunications infrastructure. Unfortunately, as stated in my main testimony, even today there is some disagreement as to the extent of the telecommunications problem. Again, I point to the recent AT&T outage. The whole network was brought down by what amounts to the broadcast of errors encountered during the testing of a device. A large number of error messages being broadcast over a network can flood that network and effectively shut it down. This is called a cascade failure. Considering this domestic example, **how likely is it that international telecommunications carriers will bring down our domestic network? How should we protect ourselves?**

Key questions (I have to admit that I don't have answers).
Given the risk of cascade failure, it makes business sense to plan for such a contingency. **At what point does it become the obligation of a telecommunications carrier to cut off a foreign country to prevent cascade failure? Can it be done pre-emptively? Do the carriers know themselves? Most importantly, do they have the right to take unilateral action under their agreements? Do their customers have the right to make such demands?**

General Business Environment
Finally, a few questions in the context of the general business environment. **Can North American firms do business in a country whose health care system is in fail mode? Is such a failure considered forseeable under US tort law? Is it forseeable under the foreign countries' tort law (or civil law equivalent)? Is such a failure forseeable under the terms of current insurance policies?** And most importantly: **"have local counsel been retained to represent our interests abroad?"**

The foregoing are questions that I believe each firm must consider for each country they do business in. Just what everyone wanted: more work.

Mr. HORN. Those are most helpful, practical suggestions, and we thank you for them.

Next is Mr. Alan Simpson, the president of ComLinks.Com.

STATEMENT OF ALAN SIMPSON, PRESIDENT, COMLINKS.COM

Mr. SIMPSON. Mr. Chairman and distinguished members of the subcommittee, the ability to communicate is the essential cement that holds together the building blocks of our modern society. Over the past century, we have crafted a complex, global, electronic communications network, which seamlessly allows us to send our messages anywhere on the surface of the Earth and even to the depths of the oceans and into deep space.

Today I need to address both the technology, consequences of failure and the need for a global media message explaining year 2000. This message needs to reassure the public, explain the impact of the millennium bug, and the actions that need to be taken to minimize its effects.

Every day trillions of dollars of global wealth are transmitted electronically around the world from New York. This wealth is retransmitted again and again in the course of a normal business day. This is done electronically by computers, using date dependent software over date dependent networks.

On initial examination, telecommunications networks seem not to be affected by dates. They appear to consist of copper wire, fiber cable, and satellite links, all connected by switches. Few realize the massive, computerized infrastructure that supports this circuitry. This support infrastructure is often ignored, and is of little consequence if the computer that connects the call is compliant, if the billing computer has automatically disconnected the callers through nonpayment to that account for the past 100 years. This complex network carries much more than financial transactions. It carries the control signals for power stations, switch and commands for electricity grids, gas and oil pipelines, and the information to manage critical infrastructure services, such as water, sewage, and environmental systems.

Here is the first problem. This highly sophisticated command and control network depends on the telecommunications network. The telecommunications network depends on clean electric power, electric power generation, and distribution depends on telecommunications. It's a catch-22.

Both the telecommunications network and the power generation distribution grid can operate at less than 100 percent, without damage to the critical infrastructure. There exists a point where the losses in the generation capacity and distribution capacity are multiplied by gaps in the telecommunications network. This can create a dangerous, critical mass.

Looking at the global perspective for a second, we are not an island insulated from the telecommunications problems of the rest of the world. We trade, we communicate, and we point nuclear missiles at each other. The potential for catastrophic miscommunication in 2000 is immense. One prudent safety valve will be to have the global nuclear shutdown from a mutually agreed period over midnight and into 2000. The question is, how will a launch system react if it believes it has lost communications

with its command and control masters for 100 years? That should be asked of all the world leaders. These world leaders should also be asking if the web of diplomatic outposts, the Embassies and the consulates will be able to keep them informed, as well as effectively deliver their cables and messages to their hosts. The last thing the President needs to find out from CNN is that one of his Embassies has been occupied.

It is not only the United States that needs to ensure unambiguous and clear communication channels. In this age of nationalistic and local tensions, we must all ensure the regional trigger fingers are kept away from weapons, especially nuclear weapons. In areas of high tension, the last thing we need is no communication between diplomats. There needs to be a communication plan to prioritize the use of scarce circuits in the event of failure. Little Freddy calling his aunt to chat needs to be given less priority than the major bank transferring funds or an essential business transaction. Until this problem is resolved, which it will be, there may have to be a rationing of circuits.

Critical supplies. In the 1980's, we were sold on the idea that just in time was the answer to maximize profits. This concept will be put to the test, especially with critical materials and subassemblies from overseas. Major corporations should examine their communication links to their overseas offices, and as a worst-case scenario, ensure that there are buffer stocks of critical materials, supplies and subassemblies. Additional stocks in business need to be planned in consultation with the banks, for an increase in stock levels will trigger a credit warning in the lending departments of the bank. Let them know this is prudent contingency planning, not a downturn in business.

Effective communication means getting the message through, regardless of transmission medium. There are alternative means of maintaining business communications. These must be explored. Sitting pretty, hoping the telecoms will get their acts together in time is not prudent business management. If there is no dial tone, think plan B.

On to the message now. There are those who compare the disruption from the year 2000 millennium bug to be akin to World War II, especially the denial, lack of preparation and global consequences. Winston Churchill is often quoted in many of his speeches. Many forget that President Roosevelt skillfully prepared the United States for war, held by Hollywood and those in the media with foresight. Industry was prepared and the White House showed positive leadership, preparing for the crisis.

We hear the sky is falling. No, the sky is not falling, it's just the computers won't work. This is the crux of the awareness problem. If the sky was falling, the river flooding or the blizzard blowing, then we could relate to these events and, using historical precedents, realize we were facing imminent danger and act accordingly. This generation has never known shortages. They have never known a crush in the economy. They cannot perceive that the United States can possibly allow such a situation to occur. They are currently in complete denial of their technology or that elected leaders can allow such a scenario. A large segment of the popu-

lation is waiting for Bill Gates and Microsoft to release MS 2000, the millennium virus fixer. There is no millennium virus fixer.

The predominant group affected by year 2000 are the baby boomers. They are the ones who will see their investments, real estate, retirement, and way of life decimated when the worst case scenario occurs. The baby boomers are well known to react like a shoal or herd. One turns, they all turn. One panics, they will all panic. This is the worst-case scenario for the banks. If this herd is spooked with only 1.5 percent cash reserves, panic withdrawals will crush the system and create a self-fulfilling prophecy.

It is the duty and responsibility, therefore, of all governments to prepare the populations for a time of crisis. In the new global information age, we would have assumed that the leader of the United States would have led the global awareness and rectification campaign. We assumed wrong.

We need world class leadership now to give the people of the global information society true and positive leadership. We must not create a general environment of pessimism. We must create from strong leadership an environment that the problems can and will be fixed. It is in this type of environment that this country was able to mobilize its enormous resources and prepare for World War II.

In conclusion, Mr. Chairman, we have a serious communication problem, both with the technology and the message. The good news is that both the technology and the message can be prepared to serve the Nation and the world during the year 2000 transition. We can find alternative routings for data. We can, if needed, jerry-rig circuits to continue operations and we certainly can craft an effective media campaign to prepare, educate, and inform both the American public and the people of the world.

Keep in mind, if the worst-case scenario occurs on a global scale, the United States will be blamed for this catastrophe. The world will point to the computers, software, and technology developed and supplied by the United States for everything that goes wrong with their economies and infrastructure in 2000. We need communication planning now. Failure is not an option.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Simpson follows:]

Alan Simpson
President, ComLinks.Com

**Testimony
before the**

**Subcommittee on Government Management, Information and Technology
of the
Committee on Government Reform and Oversight**

June 22, 1998

Communications & Year 2000

Mr. Chairman and distinguished members of the Subcommittee.

The ability to communicate is the essential cement that holds together the building blocks of our modern society. Over the past century we have crafted a complex global electronic communication network, which seamlessly allows us to send our messages to anywhere on the surface of the Earth, and even to the depths of the oceans, and out into deep space.

Today I need to address both the technology, consequences of failure, and the need for a global media message explaining Year 2000. This message needs to reassure the public, explain the impact of the "Millennium Bug", and action that needs to be taken, to minimize it's effects.

The Technology

The Problem

Every day trillions of dollars of global wealth are transmitted electronically around the world, from that spot on the Earth's surface known as New York. This wealth is retransmitted again, and again, in the course of a normal business day. This is done electronically by computers, using date-dependent software, over date-dependent networks.

On initial examination, telecommunications networks seem not to be affected by dates. They appear to consist of copper wire, fiber cable and satellite links, connected by switches. Few realize the massive computerized infrastructure that supports this circuitry.

This support infrastructure is often ignored. It is of little consequence if the computer that connects the call is compliant, if the billing computer has automatically disconnected the callers line, through non-payment of their account for the past one hundred years.

But this complex network carries much more than financial transactions. It carries the control signals for power stations, switching commands for electricity grids, gas and oil pipelines, and the information to manage critical infrastructure services such as water, sewerage and environmental systems.

"Catch 22"

Here is the first problem This highly sophisticated command and control network depends on the telecommunications network The telecommunications network depends on clean electric power. The electric power generation and distribution system depends on telecommunications.

Both the telecommunications network, and the power generation and distribution grid, can operate at less than 100%, without damage to the critical infrastructure. There exists a point where the losses in the generation capability, and distribution capability, multiplied by gaps in the telecommunications network can create a dangerous critical mass. Under normal circumstances this condition can be rapidly corrected, using alternative circuits, and signal paths. All indications point to starting 2000 with a reduced level of options.

"Three Strikes and You're Out"

For the telecommunications network the Year 2000 problem will be the third strike, between now and 2000.

First there will be the peak of the micro-meteorite shower, this event could seriously effect space assets, such as telecommunications satellites. There is the possibility that there could be no effect. Every piece of dust, or debris could miss the hundreds of orbiting satellites, or impact with little effect.

The worst case scenario is that a number of satellites, with their data and voice circuits, could be destroyed, or crippled. We need to ensure the vulnerability lessons, learned from Galaxy IV, have not been forgotten.

The next event is "Solar Max 23", where the Sun reminds us that it controls our life on Earth. This burst of energy could have tragic, or little effect on the satellites, spared by the micro-meteorite onslaught. This event could, like earlier Solar Max's cause disruption in power grids. Again, we must wait and see, but in the meantime create a number of "what if" scenarios for our operations.

These "What if" scenarios must be included in any contingency planning for Year 2000. It is essential that a level of safety be maintained in number of available circuits, and space assets, and we do not blindly assume 100% of all satellite circuits will be at our disposal on 1/1/2000.

The Global Perspective

We are not an island, insulated from the telecommunication problems of the rest of the world. We trade, communicate and point nuclear missiles at each other.

The potential for catastrophic mis-communication is immense.

The concerns of New York banks, and their credit transactions, pale in comparison with the scenario of global thermo-nuclear holocaust caused by a computer malfunction.

One prudent "safety valve" would be to have a global nuclear shutdown for a mutually agreed period over midnight, and into 2000. The question, "How will a launch system react, if it believes it lost communication with it's command and control masters, for 100 years," should be asked of the world leaders.

These world leaders should be also be asking if the web of diplomatic outposts, Embassies, and Consulates, will be able to keep them informed, as well as effectively deliver their cables, and communications, to their hosts.

In the case of the United States of America, I am concerned that The Department of State has such a pathetic rating on the scorecard, prepared by this committee. It is essential that they have comprehensive plans, to maintain secure communications, especially from the "Hot Spots" of the

Trains & Boats & Planes

There is no more dangerous an area for mis-communication than in the area of transportation, especially in aviation. The demands of the travelling public have been met by cramming an extraordinary number of planes into a small congested area.

This global air traffic control network is a masterpiece of technology, sophisticated, yet aging, electronics, and dedicated well-trained personnel. Unfortunately it has to deal with irate, economy-minded, and impatient passengers, who demand convenient flights in all weathers.

The airlines own the planes. The airports control them on the ground, and the air traffic organizations of governments, control them in the air. They are supplied with fuel by third parties, and are serviced by a whole army of computer managed entities, from fire crews to maintenance personnel.

Behind this complex operational network is another one for administration, encompassing travel agencies, reservation systems, scheduling, personnel, finance, and finally the insurers. If these insurers do not feel confident then the planes are grounded! Any aspect of this complex puzzle can bring the world's aviation industry to a crawl, even a halt.

The FAA responses to this committee has raised doubts about the ability of the Air Traffic Control Network, to manage the current level of traffic, during and immediately after the millennium changeover. The safety of the travelling public needs to be honestly reported, free of speculation, yet subject to massive penalties for hiding the truth.

Fortunately the aviation industry has awoken to the problems, and is taking steps to ensure it will have all the facts available, to make safe decisions for this busy travel period. Nevertheless the aviation industry will be under the microscope.

The railroads on the other hand have somewhat missed the public scrutiny. Few realize how dependent modern railroad systems are, on computer networks. Over the past few months we have seen confusion in communications, especially in scheduling rolling stock.

The scheduling of rolling stock, and the control of points and switches, must be addressed by the oversight committees. The scenario of the Soviet Union, in earlier decades, with crops rotting in the fields, and famine in the major cities, must not be allowed to become the United States in 2000, with crops rotting in California and Florida, with no rolling stock, or rail lines available to bring the produce to New York, Chicago, or the other major centers of population. There is no excuse, given the time scale, for breakdown of critical lines on communication, and supply.

The shipping industry poses a different problem. Supertankers are computer controlled, their operation too complex for humans. Fortunately their numbers are small, and they do act somewhat in isolation. The shipping companies are aware of the dangers of valves malfunctioning, or worse still, a massive tanker failing to slow down, and ploughing into some port facility, at full speed. The danger of valve malfunction whilst connected to a refinery is another matter. The enormity of the embedded system problem is just being realized.

Embedded systems, like Year 2000, pose a threat beyond comprehension, which leads to the second communication issue, the message. Few can comprehend Y2K.

The Year 2000 Message

There are those who compare the disruption from the Year 2000 "Millennium Bug" to be akin to World War II, especially the denial, lack of preparation, and global consequences. Winston Churchill is often quoted, and many see parallels in many of his speeches.

world, taking into account that the local telecommunications infrastructure may be fragmented, that space assets may not be available, and that the old standby of HF may be seriously impacted by solar activity.

The last thing the President needs to find out from CNN, is that one of his Embassies has been occupied.

But it is not only the United States that needs to ensure unambiguous and clear communication channels are available. In this age of nationalistic, and local tensions, we must all ensure the regional trigger-fingers are kept away from weapons, especially nuclear weapons. In areas of high tension the last thing we need is no communications between diplomats.

There needs to be a telecommunications plan, to prioritize use of scarce circuits, in the event of failure. Little Freddie calling his aunt to chat, needs to be given less priority than a major bank transferring funds, or an essential business transaction. Until this problem is resolved, which it will be, there may have to be rationing of circuits.

In the case of the worst case scenario being realized, which we hope will never happen, then we need to find alternative transmission paths for critical communications. This could be achieved, in major urban and business centers, by utilizing wireless technologies, and even running cables around Manhattan streets. The potential of using Cable TV lines for interconnecting businesses needs to be addressed by all Communications, or IT Managers.

Above all, Corporate Officers need to be aware that the Year 2000 problem is one of business survival, and it's consequences have been known for the past 30 years. Not being prepared to maintain essential services is not an option. Careful planning, and alternative communication strategies, can neutralize many of the effects of Y2K. Ownership of this responsibility lies with the officers of each individual company.

Critical Supplies

In the 1980's we were sold on the idea of "Just in Time", as the answer to maximize profits. This concept will be put to the test, non more searching that with critical materials, and sub-assemblies from overseas.

Major corporations should examine their communication links with their overseas offices, and as a worst case scenario, ensure there are buffer stocks of critical materials, supplies and sub-assemblies. This needs to be achieved in consultation with the banks, for an increase in stock levels will trigger a credit warning in the lending department of the bank. Let them know this is prudent contingency planning, not a downturn in business.

Every company, that is trading on a global scale, should be undertaking contingency planning, especially for transmission of critical data. The old concept of messengers, or couriers, needs to be in place as a last resort. If data lines are not available, or unreliable, then make provisions to carry removable magnetic, or optical media, by courier. The focus at this late stage is to keep the business alive, and running over the millennium changeover. Instead of a runner with an Olympic Torch, have a runner with a floppy disk.

Effective communication means getting the message through, regardless of transmission medium! There are alternative means of maintaining business communications, these must be explored. Sitting pretty, hoping the Telcos will get their acts together in time, is not prudent business management. It is becoming obvious that many Telcos, especially in third world countries, have only just become aware of the issues, and the problems. Suing the carriers after the event, is not a practical recipe for business survival.

If there is no dial tone....Think "Plan B"

Many forget that President Roosevelt skillfully prepared the US for war, helped by Hollywood and those in the media with foresight. Industry was prepared, and the White House showed positive leadership, preparing for the crisis.

Today, eighteen months away from potentially the worst global crisis since World War II, leadership is totally lacking. This is surprising considering this administration will have to face the electorate in 2000, months after the crisis has struck.

"The Sky is Falling"

No, the sky is not falling, it's just that the computers won't work!

That is the crux of the awareness problem. If the sky was falling, the river flooding, or the blizzard blowing, then we could relate to the events, and using historical precedents, realize we were facing imminent danger, and act accordingly.

Telling the public that the computers can't do arithmetic, and they face imminent danger, is such an abstract concept that most do not take it seriously.

This generation have never known shortages. They have never known a crashing economy. They can not perceive that the United States can possibly allow such a situation to occur. They are currently in complete denial, that their technology, nor their elected leaders, can allow such a scenario to occur. A large segment of the population is waiting for Bill Gates and Microsoft to release MS 2000, the "Millennium Virus Fixer", at $49.95, from your local computer store.

There is no "Millennium Virus Fixer".

"Don't Spook the Herd!"

The predominant group affected by Year 2000 are the "Baby Boomers". They are the ones who will see their investments, real estate, retirement and way of life decimated if the worst case scenario occurs.

The "Baby Boomers" are well known to react like a "shoal", or "herd". One turns, they all turn, one panics, they all panic, one buys yuppie four-wheel drive, off road vehicles, Manhattan is full of off-road vehicles.

The task for the media managers, and PR practitioners, is to prepare the "herd" for a rough patch, without them stampeding and crushing the drovers underfoot. A stampeding herd crashes through, and destroys everything in its path, including many of its own.

Major Banks are especially at risk from this "herd" mentality of the "Baby Boomers". With only around 1.5% cash reserves in US banks, any panic withdrawals could crash the system, and create a self-fulfilling prophesy.

There are those on the fringe of Y2K, who would welcome such a crash. This could statistically occur from one pessimistic feature on the evening TV news. If ratings were seen to soar, the ratings-led, entertainment-biased news executives would run this story to it's bitter end.

It is essential that major banks, and corporations, inform and prepare, their customers, investors, and suppliers for the possible impact of Y2K, and their progress towards a safe, and comfortable transition. Currently the lawyers are blocking most sources of information, demanding silence at all costs! But like an earthquake fault, the longer it waits, the more energy it builds up, and the greater the destructive power, when it finally breaks and moves.

It is the duty, and responsibility of a government, any government, to prepare the population for a time of crisis. In the new global information age, we would have assumed that the leader of the

United States, would have led the global awareness, and rectification campaign We assumed wrong.

We need a world-class leader to emerge, and give the people of the global information society, true and positive leadership.

"It's Too Late!"

The doomsayers preach that it is too late, that all is already lost. No it is not too late!

"Get on with the job, and fix what you can" should be the message. Start with the mission-critical, or core-business systems, and work outwards. The non-essential systems can be fixed later.

We must not create a general environment of pessimism. We must create, from strong leadership, an environment that the problems can, and will be fixed. In this type of environment this country was able to mobilize it's enormous resources and prepare for World War II.

The key of course is strong, positive, and believable leadership.

Media Plan

Many reading this testimony may take offense at referring to the public in behavioral terms as a "shoal" or "herd". That describes how they react. The "herd" is more accurate for Y2K, because when the true picture is known, the public will get very angry, and possibly violent.

We are accused of only giving the public bad news, doomsday scenarios, and unsubstantiated figures. Unfortunately those are the only figures the corporate lawyers will release.

Every company, government department, state entity, county, or city, should be initiating a media plan to inform, and reassure the public. The President should already be taking the initiative in this, and using the extensive media apparatus available to the White House, to address the nation, and the world.

Silence is counter-productive, and dangerous.

In conclusion, Mr. Chairman, we have a serious communications problem, both with the technology, and the message.

The good news is that both the technology, and the message, can be prepared to serve the nation, and the world during the Year 2000 transition. We can find alternative routings for data. We can, if needed "jerry-rig" circuits to continue operations, and we certainly can craft an effective media campaign to prepare, educate and inform both the American Public, and the people of the world.

Keep in mind, if the worst case scenario occurs, on a global scale, the United States will be blamed for this catastrophe. The world will point to the computers, software and technology, developed and supplied by the United States, for everything that goes wrong with their economies, and infrastructure in 2000.

We need communication planning now. Failure is not an option!

Mr. HORN. Thank you very much. You have put it in very simple English that anybody should be able to understand, and we thank you for that presentation.

Our next speaker is Mr. Bruce Webster, the chief technical officer, Object Systems Group, director of the Washington, DC Year 2000 Group. You might explain what that is.

STATEMENT OF BRUCE F. WEBSTER, CHIEF TECHNICAL OFFICER, OBJECT SYSTEMS GROUP, AND DIRECTOR OF THE WASHINGTON, DC YEAR 2000 GROUP

Mr. WEBSTER. The Washington, DC Year 2000 Group, with over 1,300 members, represents people working in all areas of the Y2K problem here in the Washington, DC area and elsewhere. I am honored to appear before you, Mr. Chairman, and this committee today, both representing myself and that group as a whole.

Humanity has been developing information technology for half a century. That experience has taught us this unpleasant truth. Virtually every information technology project above a certain size or complexity is significantly late and over budget or fails altogether. Those that don't fail are often riddled with defects and difficult to enhance. The causes stem not from technology but from human frailties. Indeed, when asked why so many IT projects go wrong, in spite of all we know, one could simply cite the seven deadly sins: Avarice, sloth, envy, gluttony, wrath, lust, and pride. It's as good an answer as any and more accurate than most.

In the midst of all this, we face the chasm on the road ahead, known as the year 2000 crisis, which has its roots in all the sins related. Anxiety has begun to set in through the public and private sectors as the true scope and difficulty of the Y2K problem, with its foundation in all the regrettable IT business practices of the half century become apparent. For the first time in those 50 years, these organizations face a problem that is inexorable, with a deadline that is immovable. The difficulties cannot be finessed, buried, rescoped, bought off, reorganized away or dragged out until they are finally fixed. There is too much complexity to handle, too much damage to undo, too little time to allocate, and too few people to deploy. What, then, can and should we do? I believe our best course lies in four principles: Recognize, resolve, repair, refrain.

Recognize. We need a broad public acknowledgment of the nature, scope, and difficulty of the year 2000 problem, starting with President Clinton and followed by other leaders in the administration, in Congress, in the military industry, and elsewhere. A good friend of mine admitted that years ago he went through a substance abuse program and says he has been quite amused and fascinated at all the classic and well-documented forms of denial and self-deception he has observed in people at all levels dealing with the year 2000 problem. Industry and society must realize that the Federal Government isn't going to solve their problems; indeed, the Government will be hard pressed to solve its own. And that no other organization, vendor or individual, least of all, Bill Gates, will come riding up with a miracle solution.

Resolve. We need to resolve that whatever the nature and level of Y2K consequences, we will pull together as communities, as industries, as a society, and as a Nation. With that cohesion, even

major Y2K events can be weathered. Without it, even minor Y2K events could be disastrous.

Repair. We need to do the work. It will be long, difficult, expensive, and tedious, and will probably last well into the next decade, but what we can repair and replace, we should, and as quickly as possible, using the necessary priorities.

Refrain. We must refrain from our long established and self defeating patterns in information, technology, business, law, and government. The most critical restraint, as far as humanly possible, and perhaps a bit beyond that, we must voluntarily refrain from Y2K litigation.

One of the best run year 2000 repair projects in America, and therefore in the world, is right here in Washington, DC at Fannie Mae. The head of that effort, Carol Teasley, distributed to her staff some months back a clipping from an article in Parade Magazine, written by Thomas Ricks based on his book, "Making the Corp." The clipping details what Ricks felt the fundamental lessons were at the U.S. Marine Corps boot camp at Parris Island. Carol told her staff that these were the operating principles for the duration. Tell the truth; do your best, no matter how trivial the task; choose the difficult right over the easy wrong; look out for the group before you look out for yourself; don't whine or make excuses; judge others by their actions, not their race, or, I might add, their position, political party, or profession.

I would suggest that a top to bottom application of these principles in Government, the military, industry, and society at large is our best hope for determining the true scope of the problem, repairing as much as we can and minimizing the impacts that do occur. I would also submit that virtually any major year 2000 repair effort or contingency plan not following these principles will fail.

Exactly 58 years ago last Thursday, Winston Churchill gave what is perhaps his most famous address. He sought to rally the British Nation in the wake of Dunkirk and the fall of France, asking them to brace themselves for the task ahead. What, we have to ask, will those of the mid-21st century say of us? Will they say that January 1, 2000 was, to paraphrase our own World War II leader, President Roosevelt, a virtual day of infamy, a sad and tragic symbol of short-sightedness, incompetence, denial, blame, and political maneuvering, or will they look back at midnight of December 31 of next year and say of our generation, as Churchill felt the future would say of his, this was their finest hour? The choice, I submit, is still ours, but won't be for much longer.

I would be happy to answer any questions the committee might have.

[The prepared statement of Mr. Webster follows:]

STATEMENT OF BRUCE F. WEBSTER
CHIEF TECHNICAL OFFICER, OBJECT SYSTEMS GROUP
CHAIR, WASHINGTON D.C. YEAR 2000 GROUP

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

U.S. HOUSE OF REPRESENTATIVES

JUNE 22, 1998

TESTIMONY

Mr. Chairman and distinguished members of the Subcommittee, I am honored to appear before you today. I do so representing not just myself but also the 1300 members of the Washington D.C. Year 2000 Group, most of whom work on or deal with this problem full time in the government, the military, corporations, educational institutions, and other organizations.

I didn't come to Washington to do Year 2000 work—it's not what my company does—but like many others, I was drafted into it. Once involved, I became profoundly concerned, both because of the scope of the problem and my own professional experience with information technology projects large and small. A quote from Shakespeare has repeatedly come to mind during the past 18 months while observing those who arbitrarily set schedules and deadlines, or who make blithe statements about how simple the problem is and how readily they will solve it. It's from *Henry IV*, Act III, Scene I. In it, the character Glendower boasts of his supposed command over the leading technologies of his day, declaring, "I can call spirits from the vasty deep." Another character, Hotspur, with a firmer grip on reality, replies, "Why, so can I, or so can any man; but will they come when you do call for them?"

Humanity has been developing information technology for half a century. That experience has taught us this unpleasant truth: virtually every information technology project above a certain size or complexity is significantly late and over budget or fails altogether; those that don't fail are often riddled with defects and difficult to enhance. Fred Brooks explored many of the root causes over twenty years ago in **The Mythical Man-Month**, a classic book that could be regarded as the Bible of information technology because it is universally known, often quoted, occasionally read, and rarely heeded. Most publications and books on IT since then have debated, discussed, and deplored these same problems. And they are with us still. Their causes stem not from technology but from human frailties. Indeed, when asked why so many IT projects go wrong in spite of all we know, one could simply cite the seven deadly sins: avarice, sloth, envy, gluttony, wrath, lust, and pride. It is as good an answer as any and more accurate than most.

In the midst of these human challenges, we place ever-growing demands on information technology. Like ratcheted gears on a torture rack, the tension only increases; there is no relief; things never simplify. Part of that is beyond our control, a natural consequence of the complex systems—social, economic, informational, technological, logistical, and even political—that we have nourished and which now enmesh us. Those complex relationships have made our miracle economy possible, giving us low inflation, low unemployment, low interest rates, and steady growth. But they also create the situation where a currency crisis in a small Southeast Asian country roils financial markets around the world and impacts the monetary policy of the richest nation on earth, or where a single strike at a single supplier can cause the world's largest company to shut down most of its North American manufacturing operations, furloughing tens of thousands of workers.

The other part of the problem comes from our fundamental ability to conceive and demand systems more complex than we can safely build, and our unwillingness to acknowledge and deal with those limitations. While only optimists successfully build complex systems, many complex failures come from those who are both optimistic and ignorant, or perhaps just arrogant. In the field of information technology, we have begun and abandoned the tower of Babel repeatedly in the past half century, ranging from innumerable small project failures to the incomprehensible 11-year, $4-billion IT modernization fiasco at the IRS. New foundations start each day.

In the midst of all this, we face the chasm on the road ahead known as the Year 2000 crisis, which has its roots in all the sins related. True familiarity in this case breeds deep concern; it is ignorance of the problem's actual scope and ramifications that yields popular contempt. Indeed, the Y2K controversy differs from most popular scientific disputes—such as global warming—in that there are few ideological overtures, the reality of the problem is trivial to prove, the consequences are sure and soon, and it is the most technical, informed, and involved practitioners who are most worried. Two surveys were done of the membership of the Washington D.C. Year 2000 Group, one in March and a repeat survey in May, to ask their projections of the Year 2000 impact in the United States. Both surveys yielded the same results. Two-thirds of the members responding felt there will be at best an economic slowdown; one-third felt there will be at least a strong recession and regional infrastructure failures; a tenth foresaw a second Great Depression or worse. Even when the votes from those who might stand to profit from such concerns—vendors, consultants, and lawyers—were factored out, the results remained largely the same.

Likewise, anxiety has begun to set in through the public and private sectors as the true scope and difficulty of the Y2K problem—with its foundation in all the regrettable IT and business practices of the past half-century—become apparent. For the first time in those 50 years, these organizations face a problem that is inexorable with a deadline that is unmovable. The difficulties can't be finessed, buried, re-scoped, bought off, reorganized away, or dragged out until they're finally fixed. There is too much complexity to handle, too much damage to undo, too little time to allocate, and too few people to deploy.

What, then, can and should we do? I believe the best course lies in four principles: recognize; resolve; repair; and refrain.

Recognize. We need a broad, public acknowledgement of the nature, scope, difficulty, and potential impact of the Year 2000 problem, starting with President Clinton and followed by other leaders in the Administration, in Congress, in the military, in industry, and elsewhere. (A

good friend of mine told me that many years ago he went through a substance abuse program; because of that experience, he is fascinated by all the classic and well-documented forms of denial and self-deception he's observed among people at various levels confronting the Year 2000 problem.) Each organization needs to discover and be honest with itself about the status of Y2K challenges inside and outside. Industry and society must realize that the Federal government isn't going to solve their problems—indeed, the government will be hard-pressed to solve its own—and that no other organization, vendor, or individual, least of all Bill Gates, will come riding up with a miracle solution.

Resolve. We need to resolve that whatever the nature and level of Y2K consequences, we will pull together as communities, as industries, as a society, and as a nation. With that cohesion, even major Y2K events can be weathered; without it, even minor Y2K events could be disastrous.

Repair. We need to do the work. It will be long, difficult, expensive, and tedious, and it will probably last well into the next decade. We can't get it all done in time; simple mathematical exercises demonstrate that for the embedded systems alone, we can only hope to get a small percentage tested, repaired, and replaced by the end of next year. This means will we also have to repair whatever economic, infrastructure, and even ecological damage is caused when Y2K problems hit. But what we can repair or replace, we should, and as quickly as possible.

Refrain. We must refrain from our long-established and self-defeating patterns in information technology, business, law, and government. Without that, we have little hope of making things better; as another friend is fond of saying, if you keep doing what you've always done, you'll keep getting what you've always gotten. The most critical restraint: as far as humanly possible, and perhaps a bit beyond that, we must voluntarily refrain from Y2K litigation

One of the best-run Year 2000 repair projects in America—and therefore in the world—is right here in Washington at Fannie Mae. The head of that effort, Carol Teasley, distributed to her staff some months back a clipping from an article in *Parade Magazine* (November 9, 1997) written by Thomas E. Ricks based on his book, **Making the Corps**. The clipping details what Ricks felt the fundamental lessons were at the USMC boot camp at Parris Island. Carol told her staff that these were their operating principles for the duration:

- Tell the truth.
- Do your best, no matter how trivial the task.
- Choose the difficult right over the easy wrong.
- Look out for the group before you look out for yourself.
- Don't whine or make excuses.
- Judge others by their actions not their race (or, I might add, by their position, political party, or profession).

I would suggest that a top-to-bottom application of these principles—in government, the military, industry, and society at large—is our best hope for determining the true scope of the problem, repairing as much as we can, and minimizing the impacts that do occur. I would also suggest that virtually any major Year 2000 repair or contingency effort not following these principles will fail.

Exactly fifty-eight years ago last Thursday, Winston Churchill gave what is perhaps his most famous address. He sought to rally the British nation in the wake of Dunkirk and the fall of France, asking them to brace themselves for the task ahead. What, then, will those of the mid-21st century say of us? Will they say that January 1st, 2000, was—to paraphrase our own great WWII leader, Franklin Delano Roosevelt—a virtual day of infamy, a sad and tragic symbol of short-sightedness, incompetence, denial, blame, and political maneuvering? Or will they look back at midnight of December 31st of next year and say of our generation, as Churchill felt the future would say of his, "This was their finest hour." The choice, I submit, is still ours—but won't be for much longer.

I would be happy to answer any questions that you or the Subcommittee members might have.

Bruce F. Webster (www.bfwa.com/bwebster; bwebster@bfwa.com) is Chief Technical Officer of Object Systems Group (www.osgcorp.com), an international consulting firm working to help Fortune 500 companies successfully develop and deploy information technology. He is based out of Washington, DC, where he does high-level consulting on Year 2000 issues, software development management and organization, information technology infrastructure, object-oriented development, reuse, and quality assurance. He has helped engineer a dozen commercial software products and has published three books and over 160 articles. He also serves as Chair of the Washington D.C. Year 2000 Group (www.wdcy2k.org), the largest and most active Y2K organization in the world.

Mr. HORN. Well, that's an excellent statement. We have one more presenter, Mr. Tom McCabe, Chairman of McCabe & Associates.

Mr. McCabe.

STATEMENT OF TOM McCABE, SR., CHAIRMAN, McCABE & ASSOCIATES

Mr. MCCABE. Thank you, Mr. Chairman. Mr. Chairman and members of the committee, my name is Tom McCabe. I have been invited to assess the year 2000 conversion efforts and recommend a responsive strategy, and I am very happy to do such. First, I want to commend you, Mr. Chairman, and the committee for focusing attention on this huge problem and noting its urgency in the crisis it beholds.

My background is as a mathematician and a scientist and I have been involved in developing techniques and methods to test computer software, and I want to say in front of this committee that I am very deeply concerned about the status of the year 2000 conversion and the real possibility of massive failures at that magic date.

I have been involved in testing mission critical systems for the military and commercial sectors for long before the year 2000. The question in that arena has always been will the system work. And the answer has always been the same, and that is that one has to test very rigorously to be certain. When testing is done correctly, it provides objective information with a greater sense of security that the system being remediated would actually work.

The question about where we stand today on the year 2000 can therefore only be answered by looking at the kind of testing that is being performed today on these systems. Structured testing is based on an objective and quantifiable set of metrics. Integrators and weapon system developers have for years used such discipline testing as the best practice. The GAO's report and testing guideline also endorses such disciplined testing as the best practice. At least 10 companies offer year 2000 test discipline coverage tools, and 50 large integrators provide solutions doing the same. Progress reports indicating compliance must incorporate testing metrics about dates to validate what was and was not done and tested. Reports without such coverage metrics concerning dates are merely random, subjective assessments, which may create a false sense of security.

Mr. Chairman, since there is currently no requirement for an objective measurement of date testing or reporting, the answer to the question about where we stand on remediation today is that nobody knows. That is quite unacceptable and, I might add, very, very dangerous.

The Government's Inspectors General, for example, have discovered that several systems, reported as being compliant, failed when they attempted to test them in a year 2000 environment. These systems failed because of the absence of such date-related metrics in disciplined testing. Such failures have also occurred in the commercial sector as well.

A major insurance company recently ran exhaustive tests on a system that had 25,000 logic paths, of which only 200 contained dates. The testing coverage indicated that the original testing

reached only 10 of the 200 dates passed. Mr. Chairman, testing metrics showed that the program was in fact about 5 percent tested, and that, I might add, is a very frequent occurrence.

What then is my recommendation for action?

First, that we require rigorous testing for mission critical software which will incorporate date-related test metrics and coverage. Second, that it is required that we have compliance reporting based on these date metrics.

If you refer to those suggested by the GAO, Mr. Chairman, it's only when you have reliable information based on sound testing procedures in metrics that you can begin to manage the remaining remediation. Two Harvard professors in their book, "The Balanced Scorecard," say it best when they state, "If you can't measure it, you can't manage it."

With only 557 days remaining, we have neither the time nor the resources to test everything. If we attempt to test all the systems, most of this effort will be wasted and ineffective.

Therefore, I urge the committee to demand targeted testing aimed exclusively at the date code in every mission critical system. This testing will not only reduce the risk of failure but will also identify the high-risk areas for contingency planning.

The cost of year 2000 testing is substantial, between 50 and 70 percent of the total conversion effort. Mr. Chairman, targeted, structured testing requires fewer resources and saves time. Industry experience including Nabisco, Prudential, Citibank, Merrill Lynch, and Paine Webber has typically shown that only 25 percent of the logic is date-related. Therefore, a testing plan that focuses specifically on those dates will save 75 percent of the resources.

The results are faster testing, more focused testing, reduced effort, less expense, and a better coverage of the specific dates that are causing the problem. The savings impact is confirmed in a letter from GAO to Congressmen Kolbe and Hoyer which states: However, disciplined test management, including the collection and reporting of metrics, is not an expansion of these activities, but rather is part of an effective testing process.

In conclusion, targeted testing based on metrics aimed at the date code requires less time and effort and will save the Government resources. In the coming days and weeks leading to January 1, 2000, this committee's continued involvement through a rigorous reporting system of this date coverage will be every bit as important as any recommendation I can make.

I thank you for your time. I will be happy to take any questions.

Mr. HORN. We thank you very much.

[The prepared statement of Mr. McCabe follows:]

Mr. Chairman and Members of the Committee, I am Tom McCabe. I was invited here today to assess the status of the Year 2000 conversion effort and to recommend the most important priorities for the remaining time available. I am happy to do so. First, however, I wish to commend you, Mr. Chairman, and the Members of the Committee for focusing on Year 2000 conversion and for recognizing the urgency of this crisis.

I am a mathematician and scientist specializing in testing metrics and validation techniques for computer software. I was involved in testing mission critical systems for the military, aerospace and telecommunications sectors long before Year 2000 became an issue.

The ultimate question is always the same -- will it work? Never have those words had greater meaning than they do today. When done correctly, testing provides objective information and a greater sense of security that what has been developed or repaired will actually work. Risk of failure can only be understood when such testing is done. Therefore, an accurate answer to the question, "Where are we today on Year 2000 conversion?" -- can only be answered by looking at the type of testing and reporting that is actually being done. When making that assessment we must also understand that Year 2000 presents a specific problem -- a date-related problem -- and consequently, a specific type of testing needs to be done.

Structured testing is testing based on objective and quantifiable metrics Numerous systems integrators and weapon systems developers have used such disciplined testing as best practices for more than a decade. The use of such testing procedures and metrics is also inherent in the GAO best practice testing guideline for Year 2000 as outlined by my colleague on this panel. For Year 2000 testing, there are at least ten companies that offer test coverage tools and at least 50 large integrators that routinely provide disciplined, metrics-based testing services.

Progress reports indicating system compliance must incorporate testing metrics to validate what was and was not fixed and tested. If progress reports do not include such test coverage metrics, then you are not getting factual and objective information. Rather, you are getting random and subjective assessments that may create a false sense of security. Mr. Chairman, since neither test coverage metrics nor the duty to report the extent of test coverage are currently required government-wide, it is impossible to ascertain the status of the government's remediation and conversion efforts. Since there is no standard of measurement for testing or reporting, the answer to the question, "What is the status of the remediation effort today?" is -- NO ONE KNOWS. I find that unacceptable and dangerous.

The inspectors general of many of the major government agencies, including the Departments of Agriculture, Education and Defense, have discovered that systems reported as compliant failed when the IG attempted to test them in a post 1999 environment. These systems failed because of the absence of disciplined testing. The testing was not structured, and coverage metrics were not collected or reported to indicate that all of the date-related decisions were tested.

Let me give you an example from the commercial sector. A major insurance company recently ran what it considered to be exhaustive tests on a program with 25,000 logic paths, of which only 200 contained dates. Typically, only a small percentage of the logic contains dates. The test coverage metrics analysis indicated that the original testing reached only 10 of the 200 test paths with dates. In other words, testing metrics showed that the program was only about 5% tested. This is a typical result of unstructured, untargeted, undisciplined testing, whether in industry or government. As I said before, testing without coverage metrics results in a false sense of security, high risk and unexpected failures.

I was also asked to set a priority for the actions that should be taken in the remaining days. My answer is simple and clear: Require rigorous testing of mission critical software which incorporates date-related test coverage

metrics In addition, require compliance reporting based on this testing standard and these metrics, and I would refer you to those suggested by GAO. Only when you have reliable information based on sound testing procedures and metrics can you begin to manage the remaining remediation and devise contingency plans. Two Harvard professors in their book, "The Balanced Scorecard," said it best, "if you can't measure it, you can't manage it."

The problems of today are the result of the delays and lack of focus that have characterized this effort to date. If government had started early, complete testing of every governmental system would now be well underway. We missed early. With only 557 days remaining, we have neither the time nor the resources to test everything. If we attempt to test everything, most of this effort will be wasted and ineffective.

Specifically, given the time remaining, I urge the committee to demand targeted testing aimed exclusively at the date code. In the next year, we need to test all date-related computer code in every mission critical system. This testing will not only reduce the risk of failure but will also identify high risk areas for contingency planning. We should also test any other code that was changed in the Year 2000 conversion process.

It is widely recognized that the cost of Year 2000 testing is substantial, estimated to require between 50 and 70 percent of Year 2000 conversion time and resources. Mr. Chairman, targeted, structured testing requires fewer resources and saves time. It is the equivalent of a rifle shot versus a shotgun approach. Industry experience at Fortune 500 companies including Nabisco, Prudential, Citibank, Merrill Lynch and Paine Webber has typically shown that only 25% of the logic is date-related. Therefore, a testing plan that focuses exclusively on the dates requires 75% fewer tests. The results are faster testing, reduced effort, less expense and better coverage of date logic. This savings is confirmed in a letter from GAO to Congressmen Kolbe and Hoyer which states:

> "However, disciplined test management, including the collection and reporting of metrics, is not an expansion of these test activities. Rather, it is part of an effective testing process. If an agency is already collecting coverage metrics and using them to manage its testing efforts, it may not take any significant additional effort to also report these to OMB in summary form."

In conclusion, targeted testing based on metrics aimed at the date code requires less time and effort and will save government resources. In the coming days and weeks leading to January 1, 2000, this Committee's continued involvement through a rigorous reporting system will be every bit as important as any other recommendation that I could make. Thank you for the opportunity to appear before you, and I am happy to answer any of your questions.

Mr. HORN. The questioning will begin on my behalf by the gentleman from Virginia, Mr. Davis. 10 minutes.

Mr. DAVIS. Thank you, Mr. Chairman.

Let me start with my good friend, Ed DeSeve, who—we worked on so many issues. And I guess, Ed, you do duty today to come up here on behalf of the administration.

I followed this for over a year and a half on this committee now and was very happy to see Mr. Koskinen appointed and take the role. I think it was late. I think that we've been late throughout this process.

As we get later into this in terms of hiring people, the costs keep going up because there's only a finite number of people that are trained to do this, and a bidding process between the private sector and public sector keeps raising the cost up. I think Congress has shown a willingness at every step to come forward with the funding levels, if we knew what they were, but the costs keep going up every time the administration comes back here.

I've got a few questions for you. First of all, you mentioned in your testimony that you're trying to coordinate with the State and local governments. That's absolutely critical. We can solve this at the Federal level. But the State and local governments are so much more intertwining and sharing of data that get down to the people we're all trying to help.

We just had Chief Ramsey from the District of Columbia Police Department here last week telling us we didn't have a Y2K problem. I reminded him that he was under oath, and he should just check with his people. He came back and he said, "Well, maybe we do have a problem." We just got a report back last week, and it shows that it was awful.

I think you're going to find it varied among different cities and counties and States across the country. But we know the Federal Government is behind on this and not where any of us would like it to be. And my strong suspicion is that State and local governments are even further behind. And we have appropriate time to come in and test some of this. In other words, we're talking to each other. I think we are heading toward some very potentially serious consequences.

How comfortable are you with the level of progress being made by State and local governments at this point?

Mr. DESEVE. Let me answer that two ways. The first way is looking at their abilities—State and local governments' ability to interface with us in programs that the Federal Government operates, whether they be HUD programs, HHS programs, or statistical programs.

We've worked with the National Association of State Information Resource Officials to inventory all of those interfaces, and we've posted it on a series of websites, how those interfaces work.

We're in the process right now of literally testing them to see if we can exchange data and exchange money, quite importantly, for the States across those interfaces. We will shortly have that finished and we, together with NASI, will publish that information on each interface across the web.

We are fairly sanguine in that area where we can identify the interfaces, and we've got about a year to fix those interfaces, and it is in our interest and their interest that they get fixed.

We're less sanguine in the specific State and local and county enterprises that we know about. We just don't have a good look at what's going on there. There we are working with, first, the National Association of Governors, and then with, I don't know if it's the big 5 or big 6, to try to give them as much information as we have and get from them as much information as we can.

So we have a pretty good look on interfaces. We have a less good look in some of the other areas.

Mr. DAVIS. Well, you know, we might—I was just saying we might want to do a hearing for the State and local hearings for this committee, but the only people that can really coordinate that is the executive branch. I am concerned because the information we get back, even at the Federal level, tends to be filtered when it comes to the top, to the people who are supposed to report back. And we just hear too many stories that this information we're getting back is feel good and filtered, and some of the people who are giving the reports aren't going to be around for judgment day when it turns around.

I suspect we're getting the same from State and local governments. Of course, if we don't have time to test this through and correct the testing, it can just go all haywire. So I met with Mr. Koskinen on this. He has, I think, got in it very late. If he is given the resources, I think we can make a decent effort on this. But the State and local governments, combined with what we're doing internationally on the embedded chips issue, at this point I still don't think we have a handle on it.

Our own systems we've made some progress on that and are working toward that, but it's all of the other things that go with it that make me—I think you're concerned about it, but we're really nervous about it.

And—the buck doesn't stop here. I think we've been talking about this in this committee in the last Congress, holding report cards and everything else. It really stops with the administration, and I think that's where it's going to rise or fall at this point.

As time runs out, we want to ensure that we give you the right resources, but we can't give you the right resources if we don't know what they are. Every time the estimates keep coming up in terms of what it costs. They keep going up every time.

We talked about the timely sharing of Y2K reports to OMB. What does that mean? Does that mean that when you get the copies, we get the copies? Or does it mean that when you get the copies you have a month to massage them and then send them up here?

Mr. DESEVE. No, the only thing we try to do is provide decent quality control so the information you get is in good form. I need to get it to the chairman—7 working days, I thought it was appropriate. He asked for 24 hours. I will try to figure out with staff of the committee a way that is most effective. It certainly doesn't mean 30 days.

But sometimes we get information that's either nonresponsive or in the wrong columns, and you would be better off getting good

data than having—what do they call it—garbage in, garbage out, too early.

But I would be happy to work with staff to try to set up the protocol for the monthly reporting.

Mr. DAVIS. I think the chairman would be willing to agree, we would be willing to work with you every step of the way, get the data when you get it. And if it's not adequate, work with you. We would like to make this a partnership to make this succeed. I fear what will happen when things go haywire January 1, 2000. There will be a lot of finger pointing.

Mr. DESEVE. We started working with you 2½ years ago, and the first quarterly report was actually back in 1996, and the agency data is provided to you in essentially the same time as it's provided to us. And we applaud that and want to continue working in that spirit.

Mr. DAVIS. But, again, a lot of the people that were signing the reports there and some of these agencies—FAA one—notably one—has switched the coordinators two and three times in some cases over that period of time. And so John Koskinen is the guy we're looking for to coordinate all that as we move through.

Let me just ask, we're coordinating with a number of countries with the year 2000 response classifications, and I noted that a number of countries at this point aren't responding at all in terms of what we know. And now you've labeled the Ambassadors to be the Y2K points of contacts when, based on the current data, the State Department itself isn't even going to be compliant. How does this—isn't there a better way to do this?

Mr. DESEVE. I think what we want to think about is two different things going on simultaneously. I believe Treasury will testify tomorrow in one of the Banking Committees about their work in the G–8 and their functional work with bank regulators throughout the world. So we approach this not just through the Ambassadors but also in the function outreach committees. So that the Commerce Department, working in its area, the work that the Federal Communications Commission is doing, the work that FAA is doing, all with their international counterparts is supplemented by the work of the country heads.

The purpose of the country heads, the Ambassadors, looking at the data in their areas is try to get the best assessment of the highest ranking American official in that country of what's really happening on the ground. It isn't the only thing going on. Because if we're in country A, FAA, FCC, OCC, Treasury and so on will all be working together. We've asked the Ambassadors in addition to give us the benefit of their in-country expertise.

Mr. DAVIS. OK. Let me turn the questioning to Mr. Steinberg.

Most corporate lawyers right now are telling their companies to shut up basically, to be quiet. And yet you're suggesting that we're better off with disclosure.

Mr. STEINBERG. Definitely.

Mr. DAVIS. Why are they wrong?

Mr. STEINBERG. Basically, disclosure serves to limit your liability. You tell someone there's a problem, they can't sue you claiming that they didn't know about it.

If you tell them that the brakes are bad on a car, they have a very hard time of complaining that they drove that car right off a cliff because the brakes failed if you already warned them. Sometimes they have to, if they need to use that car for an emergency.

Mr. DAVIS. Walk me through the legal ramifications. I know there have been class action suits in Michigan and California. I'm already getting mail-outs from law firms that are starting a Y2K practice. I assume that's——

Mr. STEINBERG. It's a growth industry.

Mr. DAVIS. Exactly. They're looking for litigation. We're certainly not going to consider anything of a safe harbor nature in this Congress and, you know——

Mr. STEINBERG. That would be a grave mistake.

Mr. DAVIS [continuing]. Everybody would just drop the ball at that point. Some States, though, are acting on that. Nevada and some others are treating it almost like an act of God.

Mr. STEINBERG. Those States, most of those are calling for safe harbor for themselves but not for businesses within that State. It's just you can't sue the State of Nevada.

Mr. DAVIS. Let me ask, walk me through where the legal ramifications of this could be down the road.

Mr. STEINBERG. I would be afraid to speculate on what's going to happen in Nevada. What always happens when something contentious gets enacted is somebody contests it. Now——

Mr. DAVIS. On a nationwide basis, walk through some of the failures, both the private sector and Government's ability to get the people losing credit, losing deals. This could have very serious ramifications, obviously.

Mr. STEINBERG. Yes, well, if in a State the State says you can't sue us and, because of that, they fail to get things done in time, or it may not even matter if they get it done in time, but people will end up blaming those legislatures for their——

Mr. DAVIS. You have elections that can resolve that.

Mr. STEINBERG. Pardon?

Mr. DAVIS. Elections can resolve that.

Mr. STEINBERG. Elections can resolve that after the fact. You can't roll back the clock by voting somebody out of the office. The damage will already have been done.

Mr. DAVIS. What would be your advice? There are some private companies, some banks that are ahead of the curve. There are still some that don't have a clue, particularly a number of the small businesses. We obviously—as you get the word out, what message would you send to these in terms of this?

Mr. STEINBERG. They have to disclose their risks. First, they have to go find out what their risks are, particularly the risks with their trading partners, and they have to disclose them so that people can't turn around and sue them for being foolish.

Mr. DAVIS. All right. Let me just ask, to Mr. Simpson, are you suggesting that we should undertake a public relations campaign?

Mr. SIMPSON. Yes. It started——

Mr. DAVIS. It started a little bit, the media is starting to pick this up.

Mr. SIMPSON. The last thing we want is a panic. Domestically, the last thing we want around the world is everyone pointing their

fingers and saying, IBM, Microsoft serve this junk. They should fix it, and they should take the consequences. So, yes, I think not so much a public relations campaign than an awareness campaign from the very top.

Mr. DAVIS. Are there any computer simulations that have been done with some of the utilities and are there results of what happens at this point?

Mr. SIMPSON. There's quite a lot, yes. We have a simulation, not very sophisticated, I'm afraid. And one of the scientists called me up and said, your model is flawed. You're looking at the electricity industry and the telecommunications industry in isolation. They are not. They are interconnected. If one goes down, the other goes down. And when you start getting deeper and deeper, it gets worse and worse.

Mr. DAVIS. I just—with the committee's indulgence, just one question as a followup. Right now, for example—let's make it easy. You have an elevator and, all of a sudden, it reads the wrong year. Several things can happen. The elevator can crash. It can get stuck between floors. It can go down to the first floor.

Isn't one of the problems that we really don't know what happens on that day and in some of these testings we could at least find out what the ramifications would be if there's a failure?

Mr. SIMPSON. The elevator situation is slightly odd, because the elevator's compliant. Operators will tell all the elevators are perfectly compliant. They are, until they were installed in a building, and it is the support systems that attach to the elevator within the building that are the problems. And the problem with buildings, elevators and phones is not themselves. It's the ramifications of having a building with no emergency telephone. The fire marshal won't let you in there.

Mr. DAVIS. I agree. What I'm getting at is not so much to pick on elevators is as much as to give the concept. We don't know what happens in a failure, if it goes to the first floor, if it crashes or if it stays between floors. Isn't that one of the problems with all of this? We're not even sure—we know it's not a good result, but we're not sure exactly how bad it can be in some of these cases?

Mr. SIMPSON. That's true. On the other hand, with an elevator, you don't ride the elevator until they see what they do.

That's not the real problem. The problem is, what are the other things? Elevators—a lot of people are paying attention to that and say, what about elevators? Don't ride them at midnight.

Mr. DAVIS. If you're on an airline, that's not very good news.

Mr. SIMPSON. Well, that's true. There are traffic control systems. That's a whole different ball game, yes.

Mr. DAVIS. We will get you in the next round, thanks.

Mr. HORN. I thank the gentleman from Virginia. He used 13 minutes, so I'm delighted to yield 13 minutes to Mr. Kucinich, the ranking Democrat. We're delighted to have him with us.

Mr. KUCINICH. Thank you very much, Mr. Chairman.

I would like to direct a question to Mr. DeSeve, since there has been discussion about the contact with the various States. I think it occurs to all of us that one of the significant functions of State government is to hold elections. The year 2000 is a Presidential election year.

Has anyone in the Government begun the task of assuring that all 50 States are going to have their election procedures in order so that we don't end up with a constitutional crisis in the year 2000 as a result of not being able to certify in any particular State the results of the Presidential election, not to mention election for Members of the Senate and the House?

Mr. DESEVE. Those are the kinds of things we've been talking to both NASI and the National Association of Governors about—and the Federal Election Council is certainly aware of their need to provide appropriate monitoring. I would be happy to get you more information. I haven't been involved personally in that, but I will have to get you more information about what we've been doing with both the State information officers, who have the primary technical oversight, as well as the Governor's Association, which has involved in it the folks who would be running for reelection at that point.

Mr. KUCINICH. If it goes back to 1900, we could end up with McKinley again.

Mr. DAVIS. If the gentleman would yield. We had a Republican Congress at that point.

Mr. KUCINICH. I'm focusing intensely on this.

Mr. DESEVE. I've heard of jurisdictions which dead people could vote, but I think that's carried a little bit too far.

Mr. KUCINICH. We're not in Cook County.

Mr. HORN. If the gentleman would yield for 10 seconds.

The problem isn't the Presidential election. In 2000, people will have plenty of people to attack if they don't do something to help us on this. The problem is the Iowa primary in January, the New Hampshire primary in February, and the regional South primary in March. This might well affect the counts there.

Mr. KUCINICH. That's a good point.

The reason I bring up the election is that our choosing of our officials is set up by the Constitution of the United States. When we go further down to the end of the game, we're talking about the electors who need to cast their votes, and if they don't have proper guidance, then it ends up a President could end up being chosen by the House of Representatives. I mean, there's always all kinds of interesting implications.

So what I would ask you to do, Mr. DeSeve, is to—with the permission of the Chair—is to provide a definitive report as to what is happening State by State to prepare for the year 2000's elections, as the chairman said, the primaries, general election, and State-by-State accounting from the Secretaries of State of the respective States as to their readiness, because I think that's what we need.

We need to know that they're ready, and we need to know that their accounts can be effectively tabulated, and that there's not going to be any question about the validity of those counts, because all—or, you know, in the alternative, we may need to go back to paper ballots for that election, which could get me real excited about some possibilities that were mentioned here earlier. But, you know, we have to know. Because if the computers aren't going to work, we have to be ready with an alternative plan.

Mr. DESEVE. We will be happy to collect that information for Mr. Kucinich.

Mr. KUCINICH. It would be useful for the committee.

Now, are there any particular tools, Mr. DeSeve, or resources that are needed for the agencies to meet the deadlines? I mean, do you have the resources which you need? Is Congress—you know, there has been discussion about an appropriation being made. Do you feel that—was that done in consultation with your office? Are you going to have the resources you need?

Mr. DESEVE. Again, we've had good success in prior years. Fiscal year 1997, fiscal year 1998, we included a little over $1 billion in the President's budget as well as a contingency fund. We've had good response from the House Appropriations Committee and from the Senate. The chairman assures us that that will continue, and that will give us the ability to do the work we need. We thank GAO for the work they're doing in testing as well as the work the inspectors general are doing in testing.

Mr. KUCINICH. The FCC, for one, has indicated that there could be problems with the communications systems. They noted that—one report that I've seen specifically noted that there's a risk of failures in local television stations that could lead to a failure of emergency alert systems, not to mention the broadcast itself. Do you have any information that would suggest whether or not the Nation's broadcast systems may be at risk because of the Y2K problem?

Mr. DESEVE. What we've done—you've just highlighted it—is we've asked the FCC to provide that coordinative responsibility in the sector in which they work. So the information you have is from the FCC about the current status, as well as their oversight and their regulatory function as they look at licensing and making people aware of the things that they have to do. The FCC is working very closely on this issue. They're 1 of the 30 sectors that John Koskinen identified. And so the FCC has taken responsibility in this area.

They're assisted by other partners like the Department of Commerce where we've got a lot of communication infrastructure that we work on, or in the Defense Department. But their word, the FCC's word is the administration's word in this area, by design.

Mr. KUCINICH. How about wireless communication at the local levels with respect to police, fire?

Mr. DESEVE. We've met with representatives of chiefs of police, representatives of cities and counties to make them aware of what may happen and cause them to test their own communication systems, whether wireless or 911 systems. They're in the process of doing that now.

I can't give you a definitive report on that, but I think that may be a subject, as Mr. Davis indicated, for a hearing here to ask the local and State governments to come in and talk about how they're doing.

Mr. KUCINICH. Have you set up protocols in terms of, one step at a time, how you solve a Y2K problem? You know, where do you begin? An analysis of their code? The—do you know, for example, that entire industries are affected out of hand? Then do you send

somebody in to analyze the code? Then do you hire a programmer to reprogram? What are the steps here?

Mr. DESEVE. I think when we work, we start, again, within the Federal Government. We start by inventorying the nature of the existing systems, determining which of those are mission critical, determining which of those are compliant, and begin the process of actually fixing the code or replacing the entire system—there are some cases where it's just better to replace the system—or changing the way we do the function.

Mr. KUCINICH. Because when you fix the code, some of these, as it was with many systems, you have code that's written specially. You have codes altered to deal with specific tasks. And so the reengineering of those codes can be daunting, even without the pressure deadlines.

Mr. DESEVE. That's correct. And, as a result, in many cases, we make the decision to replace the system, rather than to repair it. Although, as we go further, there are cases where we find out that that's not going to be possible. We literally won't be able to replace it quickly enough. We don't have enough assurance that what exists out there is itself Y2K compliant. So we make a decision to move in that direction.

We also then move into a phase once the work has been done and assessment of compliance or replacement has been put in place with the testing phase, and this is—these are not purely sequential, but there would be some systems that are in testing while other systems are in remediation. The testing phase is designed to include independent bodies, independent verification and validation groups, as well as the work of the inspectors general to make sure that the claims asserted are, in fact, correct.

I appreciate GAO's testimony that GAO found that the inspectors general found that, in fact, some of the claims were not correct. That's why we do the testing. That's why we bring independent parties in.

Finally, we then place those systems in operation and use them for a period of time following March 1999, which is the date that the systems are supposed to be in compliance and see how they work, make sure that they still work properly. So that's it, that set of steps.

Mr. KUCINICH. As you identify step by step and you are able to certify that there is Y2K compliance, those personnel that have worked on that problem, are they then able to transfer over within the Government to other divisions so that they can help solve the problem?

Mr. DESEVE. Yes, they are. We've tried to make the personnel rules as flexible as possible, and we've identified some of the pools of personnel and some of the agencies.

DOD is doing it very effectively internally. They've got a series of teams, I've forgotten the number of teams, who are able to move from solution to solution. They're not Army teams or Navy teams or Air Force teams, but they're Defense Department teams, and they're designed to move from problem to problem over time. The Defense Department has also indicated, to the extent that they get some surplus capacity, they will be happy to make that available to domestic agencies.

The Year 2000 Council led by the Social Security Administration is doing some of the same kind of work.

Mr. KUCINICH. Thank you very much.

Thank you, Mr. Chairman. I yield back.

Mr. HORN. I thank the gentleman for those very helpful questions.

Let me ask some general questions of all of you here, if I might.

Mr. McCabe, you raised the question in your testimony regarding testing areas and the alarms that would raise. How long does it take to adequately perform tests or retests?

Mr. MCCABE. Mr. Chairman, generally in a project, it will take 50 or 60 or 70 percent of the total effort dedicated to the testing. That's the general guideline. In this particular case, there's a real anomaly, and that is the people for good reason or concern with safety want to test thoroughly.

The mistake being made, however, is that, as general testing, when the remediation is very specific to dates. And there are techniques that are now particularly being used whereby one can pinpoint the number of date tests and then really focus on that. The good news, if there is any in all of this problem, is that the date is not that dense. The dates are typically between maybe 5 and 12 percent of the line of code, and the number of tests specifically for the dates for the whole—within the whole system is likewise about maybe 10 percent of the total tests.

So a mistake a lot of well-intended agencies and companies are making is testing all of the above, the whole system, when, in fact, there's a whole lot less to test. So they are both testing too much. And then, if you look in the inside, they're testing too little. Because with the buckshot approach, the fact is you miss a lot of the core things and dates that you should be testing.

Mr. HORN. Do you all agree with Mr. McCabe?

I see Mr. Simpson nodding approval.

How about you, Mr. Webster?

Mr. WEBSTER. Yes, I do. Testing is—this is an issue I've been involved in as well. It is challenging to come up with a test that exercises those portions of the code where the problems lie. Indeed, everything Mr. McCabe has had to say about coverages is extremely applicable to the year 2000 problem.

And my own observation and experience is that most firms tend to neglect testing. It is where they think to cut back or cut short, and it's where the greatest risks are at.

Mr. HORN. Mr. Steinberg.

Mr. STEINBERG. Well, I'd like to be able to agree, but in my ancient experience as a programmer and my wife's experience as a Y2K tester, you can't depend on programmers to tell you where to put dates. So if you want to test dates, you have to test everything just to make sure you haven't missed one. And that's the unfortunate reality.

Probably we still have to go with Mr. McCabe's suggestion, because it's the only way we have, testing everything to the best of our ability. But no matter what you do, we're going to still miss dates and still have some failures, because we can't test everything.

Mr. HORN. Mr. Grabow.

Mr. GRABOW. Yes, I agree. I would add that, as the time gets smaller and smaller, testing people will shrink the amount of testing they do just because of the finite date constraint.

I would go on and say that when you go on to the productive capacity and you look at a powerplant, to speak to Mr. Davis' earlier question about the utility industry, be successful in a powerplant, there have been many failures that have been demonstrated already.

But to be successful, you have to do end-to-end system testing. So even though you identify particular segments or subsystems within a powerplant and you're able to begin to fix them or remediate them, until you actually have the plant in a position to do end-to-end testing, you can't be assured of the actual result.

So, therefore, I think it's very important that the time allowed for testing to be there and be available and what may occur, if facilities are not remediated in time, they're going to have to be shut off, as we come to this date, because of the concern of the outcome, quite frankly.

So when you look at the electric utility industry—we have studied this at great length, and we see that it's very likely that we will have brownouts in this country, and possibly some intermittent blackouts, as we make the turn, only because if you look at the entire grid, there are—it's basically an end-to-end system that has to be tested.

There are 6,000 powerplants out there that all have to be remediated; and, unfortunately, as we look at the work from our analysis, we don't see that all that is being done in every case. To remediate a particular powerplant, it can take anywhere from 5 months to 12 months; and, in some cases, they're still trying to determine that. So I think the testing is going to be very, very critical as we get into the end of this year.

Mr. HORN. Dr. Stillman, your thoughts on testing, are they the same as Mr. McCabe's and the other panelists?

Ms. STILLMAN. I think yes and no. We agree in large measure, I'd like to clarify some things.

There are lots of kinds of test tools, including the test tools Mr. McCabe has been working on for years called coverage test tools. I think they're very useful in making sure that you test critical portions of the code. But no combination of test tools and no combination of testing approaches, such as stress testing, performance testing, or end-to-end testing, will guarantee you that you don't have problems.

So, especially in a situation like this where time is limited, each organization will have to assess its risks and determine what tests will be most effective and what metrics it needs to determine how thorough its tests are. There is no one answer to doing that. It's like any other complex problem. You can give a simple answer, and it's usually wrong.

Mr. HORN. Mr. DeSeve, any thoughts on testing?

Mr. DESEVE. First, there's always safety sitting next to Dr. Stillman and agreeing with her. And so I really would like to agree, and I would have said the same thing about the one size does not fit all.

But I think the independent validation, whether by an external consulting firm or a consulting firm, together with the IG is critical. We need to have at least two pairs of eyes looking at this, whichever set of testing regimes is chosen within an agency.

Mr. HORN. Now, the administration has picked one month as when they want testing to begin, and when do they want testing to end?

Mr. DESEVE. Testing should be continuous as soon as the system is thought to be compliant. Testing should be part of that.

So if you look at a vin diagram, it will be continuous; and all systems are to be compliant by March 1999. Your point over here, the final end of the hard work is March 1999, so we hope that that's when the in-service testing, if you will, begins, when the formalized testing process gives way to in-service testing and use.

Mr. HORN. In other words, you're saying if everybody does most of the job by March 1999, we can have extensive testing in terms of government computers, and you feel the last three quarters are sufficient to do that?

Mr. DESEVE. That's why we actually moved—we advanced the date. There had been a later date. We actually under Frank Raines' leadership advanced the date to give us that extra time to test. And it will be a real acid test of the agencies, how many meet the March 1999 date. That's the one, like you, we're very much focused on.

Mr. HORN. Obviously, have you had any experience so far to know if the testing you've done in some of the areas, such as Social Security, how much time did they need to test after they had ascertained whether the code needed revamping, adjusting, whatever you want to call it?

Mr. DESEVE. I hate to be prolix, but it will really vary depending on the type of system. If you have a very large system, as Mr. McCabe testified, that it is not date dense then, as a result, it has no particular problems.

We tested an OMB, for example, and because we have been running our systems across the year 2000 for many budget years, we find a very high degree of our systems were compliant and could easily do it.

As you might imagine, the smaller percentage, less than 3 percent of the systems where we're going to have to annually update, we would have always have to annually update. These will be updated next March to take care of that problem.

But then the question is, how do they run in the environment? We're going to have to test their ability to run with other systems in departments and agencies who use them. So the end testing comes in.

So for a specific set of codes and the revamping, the testing can be very brief, but the in-service can take significantly longer, depending on how well our partners are able to handle the problem.

Mr. HORN. Assuming something goes wrong and we don't have enough time in three quarters or they don't get to the position where they can test, does that mean contingency planning is a critical need? If so, what is the administration's approach on dealing with contingency planning where you might say, "the heck with the computer. We're going to do something else"?

Mr. DESEVE. Contingency planning is indeed critical. And we're working with GAO to develop the next level of their guidance, together with ours, in contingency planning. But for completing business operations as well as an alternative path, if you will, for the computer technology, we know that there will be a need for contingency planning. It may be something as simple as we have to wait an extra month or an extra 2 months to have something happen.

If that's not mission critical, if it's not going to affect the economy, that can be an easy choice along the way. But where it is mission critical and it's going to affect the economy, we're going to begin in the next quarterly report indicating the nature of the contingency plans for both systems and for business operations. We really care about business operations.

So you will see in the September quarterly report the beginnings of the agencies reporting on their contingency planning.

Mr. HORN. Now, when Dr. Raines came in, we had an agreement that we would use reprogrammed money to do as much of the job as we could. But, despite that, some appropriations subcommittees felt there was need for additional money beside reprogrammed money. And Mr. Kolbe's subcommittee, which includes the Executive Office of the President and OMB, is putting appropriations money in there for not simply those offices but for the rest of the administration.

What do you estimate the total cost will be on the Federal Government? Do we have a figure on that?

Mr. DESEVE. Our latest quarterly report contains a figure, including money already spent, of approximately $5 billion. Of that, about $3.4 billion will be spent through fiscal year 1998; about $1.3 billion will be spent in fiscal year 1999, and about $300 million will be spent in fiscal year 2000. That should, if my arithmetic is good, add up to just about $5 billion. And that was all in our last quarterly report.

Mr. HORN. Now, with the predicted higher and higher costs for human resources as we get near the deadline, and some of your top people have already expressed the fact that they set up a center, they bring these people out of retirement, they train them for the job to be done, and the next thing they know is they're gone, either to other Federal agencies, State agencies, or private corporations. What's your feeling on the rising cost, just based on people?

Mr. DESEVE. I think what we've seen so far is that the problem is very much like dealing with an older home, an older home is perhaps the best analogy. As we begin learning more about some of the systems in that older home, we find it becomes more expensive. When we didn't have the wallboard off, we didn't know what was behind the wallboard. So I think that no one is projecting that the costs will come down.

As a result, in the President's budget this year, we suggest that a flexible contingency be available for dealing with those unknowns as they come due.

Mr. HORN. You listened to a lot of the testimony of the other panelists. Some of them were very pessimistic about the Federal Government's prospects. What's your view?

Mr. DESEVE. I hope I'm realistic. We're very concerned, as you are, about what we call the tier 1 agencies. And we want to continue to work very hard with them and to monitor what's going on.

The other thing I heard, I think, here today is that in terms of planning, the kind of process that we in this committee have had in place of oversight is probably as good as any around the world. That doesn't guarantee success, but it does guarantee the kind of vigilance that you've given and the vigilance that the administration has been trying to give.

For the tier 2 agencies and the tier 3 agencies, we feel fairly comfortable in the tier 3's. But we're from Missouri, so we're going to want to continue to test them in use. And the tier 2's, they're making progress, but we want to make sure that they continue to make progress. So, as a result, we will have monthly reports in the tier 2's, as well as the tier 1 agencies.

Mr. HORN. You mentioned a letter from the World Bank to various member nations. And, as a result, there was no conclusive response from 65 countries, which was mentioned by you and others. What do you feel that reflects? They just don't understand it? Should we be worried? Because some of those computers might well be interacting with subsidiaries of American corporations. How do you take that and what can we do or what should the administration do to get them focused a little more on this?

Mr. DESEVE. Yes, I think we're continuing to work with our partners in the IMF, our partners in the World Bank, our partners in the G–8. There were a series of conversations at the G–8 bank earlier in the spring on these issues. I think it's working along with the Federal Reserve, with Mr. Greenspan and others continuing to raise awareness, whether it's Mr. Simpson's public awareness campaign or other campaigns, we believe very strongly in that, and we encourage this committee to continue its focus to increase that awareness.

Mr. HORN. Well, we wrote the Secretary General of the United Nations 2 years ago. He, presumably, was going to do something about it. Whether he has or not, I don't know.

Mr. Gorbachev contacted us. He was very interested in it. He talked to the Russian Government. He had the right approach. But then he just got sort of fed up when he couldn't get much help from some of the people he wanted to get help from.

So you're saying the President has talked, or Treasury will tell us tomorrow, the degree with which they talked to the G–8 or whatever it is now?

Mr. DESEVE. And the President, along with Mr. Blair and others at the G–8, had a series of colloquies that resulted in a series of statements. I will be happy to give you those in addition to what the Secretary of State has done and others.

[The information referred to follows:]

THE WHITE HOUSE

Office of the Press Secretary
(Birmingham England)

For Immediate Release May 17, 1998

FACT SHEET
The G-8 Birmingham Summit
"Securing the Benefits of Integration"

At Birmingham, President Clinton advanced his strategy of securing the benefits of global integration by making sure these benefits are shared more widely among the American people and within all peoples in all regions. Following the economic and political discussion on Friday and the progress made on fighting transnational crime on Saturday, President Clinton led the discussion on how to move forward on several key global challenges of the 21st century: promoting sustainable development, particularly through trade, political and economic reform, and targeted debt relief; protecting the global environment; and combating the spread of infectious diseases. The Leaders also discussed the difficult challenge of the Year 2000 Bug, and pledged to work together, and with industry, to address it.

Development: Africa
Promoting integration, reform and targeted debt relief

President Clinton led the discussion on Africa which continued and built on those at the Lyon and Denver Summits. Encouraged by the progress being made by some countries in Africa during his recent trip to the Continent, the President pushed for more effective support for indigenous efforts to build democracy, good governance and a stronger civil society.

Countries Emerging from Conflict: recognizing that poor nations emerging from conflict have special needs -- for rebuilding political economic and social institutions in a manner consistent with democratic values and respect for human rights -- the Leaders agreed that strengthening the local ability to prevent and ease conflict is also integral to Africa's development.

The World Bank and multilateral institutions were called upon to play a special coordination role in these efforts. Leaders also agreed on the critical importance to the reform efforts of developing countries of replenishing the soft loan window of the African Development Bank and the new resources for the IMF's Enhanced Structural Adjustment Facility, along with delinking development bilateral assistance.

Debt Relief: Relieving the debt burden of the poorest countries' continues to be a priority for President Clinton. To promote

development, improve the quality of life and foster integration into the global economy, the Leaders pledged their support for the current initiative to eliminate up to 80% of the debt for needy countries that have undertaken bold economic reforms. They encouraged all eligible countries to join the initiative by the year 2000. To support these countries initial reform efforts, the President pushed the other Leaders to work with the international financial institutions (IFI) to cover debt service payments and to forgive poor countries' bilateral debt.

Infectious Diseases: Also following on last year's Denver Summit discussions, Leaders agreed to enhance their cooperation to fight infectious and parasitic diseases. President Clinton and Prime Minister blair led the G-8 in voicing support for the WHO's "Roll Back Malaria" campaign to significantly reduce the death rate from malaria. The G-8 Leaders expressed their continued support for UNAIDS' efforts to fight the spread of HIV/AIDS, and agreed to pursue efforts to prevent and treat AIDS.

Protecting the Global Environment: Climate Change and Forests

Climate Change: Birmingham marked an important shift in efforts by industrialized nations to work together to address the challenge of climate change. The Eight agreed to elements of a common approach on "the work that is necessary to ratify Kyoto" -- an important step forward on building a globally solution to this global problem. In the past, industrialized nations have different on how best to address climate change. Yesterday, the Eight Leaders spoke of the significant domestic steps they are each taking to address climate, and together recognized the need and difficulty of building a global system to address this problem. officials from G-8 governments will meet to make progress on these issues prior to the next climate change negotiating round, which will be held in Buenos Aires this November.

The Eight agreed on the need for cooperation in two key areas. First, they pledged to develop effective rules and principles for market-based emissions trading and other flexibility mechanisms to "ensure an enforceable, accountable, verifiable, open and transparent trading system." Significantly, the Eight also agreed to work as a group with developing nations to secure participation and commitments from all nations. Recognizing that this is a critical step needed to make Kyoto a reality -- especially since developing nations are likely to be most effected by climate change, that these nations' share of emissions is growing, and that commitments must be tailored to these nations' considerable development needs.

leaders also endorsed a G-8 Forest Action program, committing themselves to reporting on concrete steps to protect forests at home and in developing nations. They also discussed the importance of establishing common environmental guidelines for export credit agencies -- such as those adopted by the U.S.

Export-Import Bank -- but were unable to reach agreement on common standards.

Employability

the LEaders also focused on enhancing opportunities for workers to make sure nobody falls through the cracks during this time of global integration. President Clinton underscored the importance of strong, sustained macroeconomic growth as a means to bring more people into the work force and help raise living standards for all people. Over the past five years, America's strong, sustained economic expansion has helped lower unemployment to record lows for disadvantaged groups and raise the incomes of the poor.

President Clinton highlighted the success of the Earned Income Tax Credit (EITC) in making work pay and providing strong incentives for work over welfare. In particular, he noted recent research that shows that the EITC lifts more than 4 million people out of poverty each year and encourages single mothers with children to enter the work force.

The Leaders also renewed their support for global progress towards the implementation of internationally recognized core labor standards. In particular, they emphasized support for the adoption of the ILP declarations and implementation mechanisms of core labor standards at the ILO ministerial next month and the collaboration between the ILO nd WTO in carrying forth this agenda.

Year 2000

The Leaders discussed the urgent need to coordinate efforts to deal with the international challenge of the Year 2000 computer problem. President Clinton raised this issue as one of the premier challenges at the beginning of the next two years, and discussed the U.S. effort to address the issue. The Eight agreed to work with the private sector and organizations working in the areas of defense, transport, telecommunications, financial services, energy and the environment to solve the problem and prevent potential disruption.

###

G8 BIRMINGHAM SUMMIT

15-17 MAY 1998

COMMUNIQUE

Introduction

1. We, the Heads of State or Government of eight major industrialised democracies and the President of the European Commission, met in Birmingham to discuss issues affecting people in our own and other countries. In a world of increasing globalisation we are ever more interdependent. Our challenge is to build on and sustain the process of globalisation and to ensure that its benefits are spread more widely to improve the quality of life of people everywhere. We must also ensure that our institutions and structures keep pace with the rapid technological and economic changes under way in the world.

2. Of the major challenges facing the world on the threshold of the 21st century, this Summit has focused on three:

- achieving sustainable economic growth and development throughout the world in a way which, while safeguarding the environment and promoting good governance, will enable developing countries to grow faster and reduce poverty, restore growth to emerging Asian economies, and sustain the liberalisation of trade in goods and services and of investment in a stable international economy;

- building lasting growth in our own economies in which all can participate, creating jobs and combating social exclusion;

- tackling drugs and transnational crime which threaten to sap this growth, undermine the rule of law and damage the lives of individuals in all countries of the world.

Our aim in each case has been to agree concrete actions to tackle these challenges.

Promoting sustainable growth in the global economy

3. In an interdependent world, we must work to build sustainable economic growth in all countries. Global integration is a process we have encouraged and shaped and which is producing clear benefits for people throughout the world. We welcomed the historic decisions taken on 2 May on the establishment of European Economic and Monetary Union. We look forward to a successful EMU which contributes to the health of the world economy. The commitment in European Union countries to sound fiscal policies and

continuing structural reform is key to the long-term success of EMU, and to improving the prospects for growth and employment.

4. Overall global prospects remain good. However, since we last met, the prospects have been temporarily set back by the **financial crisis in Asia**. We confirm our strong support for the efforts to re-establish stability and growth in the region and for the key role of the International Financial Institutions. Successful recovery in Asia will bring important benefits for us all. Therefore:

- we strongly support reforms underway in the affected countries and welcome the progress so far achieved. With full implementation of programmes agreed with the IMF we are confident that stability can be restored. The underlying factors that helped Asia achieve impressive growth in the past remain in place. Implementation of agreed policies together with the action taken by ourselves and other countries to avoid spillover effects provide the basis for a firm recovery in the region and renewed global stability;

- we believe a key lesson from events in Asia is the importance of sound economic policy, transparency and good governance. These improve the functioning of financial markets, the quality of economic policy making and public understanding and support for sound policies, and thereby enhance confidence. It is also important to ensure that the private sector plays a timely and appropriate role in crisis resolution;

- we are conscious of the serious impact of the crisis in the region on the poor and most vulnerable. Economic and financial reform needs to be matched with actions and policies by the countries concerned to help protect these groups from the worst effects of the crisis. We welcome the support for this by the World Bank, the Asian Development Bank and bilateral donors and the increased emphasis on social expenditure in programmes agreed by the IMF;

- we are concerned that the difficulties could trigger short-term protectionist forces both in the region and in our own countries. Such an approach would be highly damaging to the prospects for recovery. We resolve to keep our own markets open and call on other countries to do the same. We emphasise the importance for the affected countries of continued opening of their markets to investment and trade.

5. Looking ahead to the **WTO's** celebration of the 50th anniversary of the founding of the GATT next week, we:

- reaffirm our strong commitment to continued trade and investment liberalisation within the multilateral framework of the WTO;

- call on all countries to open their markets further and resist protectionism;

- strongly support the widening of the WTO's membership in accordance with established WTO rules and practices;

- agree to promote public support for the multilateral system by encouraging greater transparency in the WTO, as in other international organisations;

- reaffirm our support for efforts to complete existing multilateral commitments, push forward the built-in agenda and tackle new areas in pursuing broad-based multilateral liberalisation;

- confirm our wish to see emerging and developing economies participate fully and effectively in the multilateral trade system; commit ourselves to deliver early, tangible benefits from this participation to help generate growth and alleviate poverty in these countries; and undertake to help least developed countries by:

    - providing additional duty-free access for their goods, if necessary on an autonomous basis,
    - ensuring that rules of origin are transparent,
    - assisting efforts to promote regional integration,
    - helping their markets become more attractive and accessible to investment and capital flows.

6. The last point highlights one of the most difficult challenges the world faces: to enable the **poorer developing countries, especially in Africa,** develop their capacities, integrate better into the global economy and thereby benefit from the opportunities offered by globalisation. We are encouraged by the new spirit of hope and progress in Africa. The challenges are acute, but confidence that they can be overcome is growing. We commit ourselves to a real and effective partnership in support of these countries' efforts to reform, to develop, and to reach the internationally agreed goals for economic and social development, as set out in the OECD's 21st Century Strategy. We shall therefore work with them to achieve at least primary education for children everywhere, and to reduce drastically child and maternal mortality and the proportion of the world's population living in extreme poverty.

7. To help achieve these goals, we intend to implement fully the vision we set out at Lyon and Denver. We therefore pledge ourselves to a shared international effort:

- to provide effective support for the efforts of these countries to build democracy and good governance, stronger civil society and greater transparency, and to take action against corruption, for example by making every effort to ratify the OECD Anti-Bribery Convention by the end of 1998;

- to recognise the importance of substantial levels of development assistance and to mobilise resources for development in support of reform programmes, fulfilling our responsibilities and in a spirit of burden-sharing, including negotiating a prompt and adequate replenishment of the soft loan arm of the World Bank (IDA 12) as well as providing adequate resources for the Enhanced Structural Adjustment Facility of the IMF and for the African Development Fund;

- to work to focus existing bilateral aid and investment agency assistance in support of sound reforms, including the development of basic social infrastructure and measures to improve trade and investment;

- to work within the OECD on a recommendation on untying aid to the least developed countries with a view to proposing a text in 1999;

- to support the speedy and determined extension of debt relief to more countries, within the terms of the Heavily Indebted Poor Countries (HIPC) initiative agreed by the International Financial Institutions (IFIs) and Paris Club. We welcome the progress achieved with six countries already declared eligible for HIPC debt relief and a further two countries likely to be declared shortly. We encourage all eligible countries to take the policy measures needed to embark on the process as soon as possible, so that all can be in the process by the year 2000. We will work with the international institutions and other creditors to ensure that when they qualify, countries get the relief they need, including interim relief measures whenever necessary, to secure a lasting exit from their debt problems. We expect the World Bank to join the future financial effort to help the African Development Bank finance its contribution to the HIPC initiative;

- to call on those countries who have not already done so to forgive aid-related bilateral debt or take comparable action for reforming least developed countries;

- to enhance mutual cooperation on infectious and parasitic diseases and support the World Health Organisation's efforts in those areas. We support the new initiative to "Roll Back Malaria" to relieve the suffering experienced by hundreds of millions of people, and significantly reduce the death rate from malaria by 2010. We will also continue our efforts to reduce the global scourge of AIDS through vaccine development, preventive programmes and appropriate therapy, and by our continued support for UNAIDS. We welcome the French proposal for a "Therapeutic Solidarity Initiative" and other proposals for the prevention and treatment of AIDS, and request our experts to examine speedily the feasibility of their implementation.

8. We see a particular need to strengthen Africa's ability to prevent and ease conflict, as highlighted in the UN Secretary General's recent report. We will look for ways to enhance the capacity of Africa-based institutions to provide training in conflict prevention and peacekeeping. We also need to consider further ways to respond to the exceptional needs of poor post-conflict countries as they rebuild their political, economic and social systems, in a manner consistent with democratic values and respect for basic human rights. In addition to immediate humanitarian assistance:

- we recognise the need for technical and financial assistance in creating strong democratic and economic institutions, supporting good governance alongside programmes of macroeconomic and structural reform supported by the IMF and World Bank. We call on the World Bank to play a strong role in co-ordinating bilateral and multilateral assistance in these areas;

- we also agree on the need to consider ways for debt relief mechanisms, including the HIPC initiative where appropriate, to be used to release more and earlier resources for essential rehabilitation, particularly for those countries with arrears to the IFIs.

9. A crucial factor in ensuring sustainable development and global growth is an efficient energy market. We therefore endorse the results of our Energy Ministers' Meeting in Moscow in April. We shall continue cooperation on energy matters in the G8 framework. We recognise the importance of soundly based political and economic stability in the regions of energy production and transit. With the objective of ensuring reliable, economic, safe and environmentally-sound energy supplies to meet the projected increase in demand, we commit ourselves to encourage the development of energy markets. Liberalisation and restructuring to encourage efficiency and a competitive environment should be supported by transparent and non-discriminatory national legislative and regulatory frameworks with a view to establishing equitable treatment for both government and private sectors as well as domestic and foreign entities. These are essential to attract the new investment which our energy sectors need. We also recognise the importance of international co-operation to develop economically viable international energy transmission networks. We shall pursue this co-operation bilaterally and multilaterally, including within the framework and principles of the Energy Charter Treaty.

10. Considering the new competitive pressures on our electric power sectors, we reaffirm the commitment we made at the 1996 Moscow Summit to the safe operation of nuclear power plants and the achievement of high safety standards worldwide, and attach the greatest importance to the full implementation of the Nuclear Safety Account grant agreements. We reaffirm our commitment to the stated mission of the Nuclear Safety Working Group (NSWG). We agreed to deepen Russia's role in the activities of the NSWG, with a view to eventual full membership in the appropriate circumstances. We acknowledge successful cooperation on the pilot project of the International Thermonuclear

Experimental Reactor (ITER) and consider it desirable to continue international cooperation for civil nuclear fusion development.

11. The greatest environmental threat to our future prosperity remains **climate change.** We confirm our determination to address it, and endorse the results of our Environment Ministers' meeting at Leeds Castle. The adoption at Kyoto of a Protocol with legally binding targets was a historic turning point in our efforts to reduce greenhouse gas emissions. We welcome the recent signature of the Protocol by some of us and confirm the intention of the rest of us to sign it within the next year, and resolve to make an urgent start on the further work that is necessary to ratify and make Kyoto a reality. To this end:

- we will each undertake domestically the steps necessary to reduce significantly greenhouse gas emissions;

- as the Kyoto protocol says, to supplement domestic actions, we will work further on flexible mechanisms such as international market-based emissions trading, joint implementation and the clean development mechanism, and on sinks. We aim to draw up rules and principles that will ensure an enforceable, accountable, verifiable, open and transparent trading system and an effective compliance regime;

- we will work together and with others to prepare for the Buenos Aires meeting of COP4 this autumn. We will also look at ways of working with all countries to increase global participation in establishing targets to limit or reduce greenhouse gas emissions. We will aim to reach agreement as soon as possible on how the clean development mechanism can work, including how it might best draw on the experience and expertise of existing institutions, including the Global Environment Facility. We look forward to increasing participation from developing countries, which are likely to be most affected by climate change and whose share of emissions is growing. We will work together with developing countries to achieve voluntary efforts and commitments, appropriate to their national circumstances and development needs. We shall also enhance our efforts with developing countries to promote technological development and diffusion.

12. The recent devastating forest fires in south-east Asia and the Amazon, threatening not only our environment but even economic growth and political stability, illustrate the crucial importance of global cooperation, and of better and more effective frameworks and practical efforts designed to sustainably manage and conserve forests. In the year 2000 we will assess our progress on implementation of the G8 Action Programme published last week. We strongly support the ongoing work on forests under the auspices of the United Nations, and we look forward to continuing these efforts.

Growth, employability, and inclusion

13. All our people, men and women, deserve the opportunity to contribute to and share in national prosperity through work and a decent standard of living. The challenge is how to reap the benefits of rapid technological change and economic globalisation whilst ensuring that all our citizens share in these benefits by increasing growth and job creation, and building an inclusive society. To accomplish this, we recognise the importance of modernising domestic economic and social structures within a sound macro-economic framework. To these ends we strongly endorse the seven principles agreed by the G8 Finance, Economic, Labour and Employment Ministers at their London Conference in February on "Growth, Employability and Inclusion". We also welcome the conclusions of the Kobe Jobs Conference of November 1997, with their particular focus on active ageing.

14. We discussed and welcomed the Action Plans we have each produced to show how the seven principles of the London Conference are being implemented. By sharing national experiences and best practices in this area, we can improve our policies and responses. We underlined the importance of the involvement of employers and unions in securing successful implementation of these Plans.

15. The Action Plans show that individually we are all making new commitments to improve employability and job creation in our countries. In particular, we have committed ourselves to:

- measures to help young, long-term unemployed and other groups hard hit by unemployment find work;
- measures to help entrepreneurs to set up companies;
- carrying out structural reforms, including making tax and benefit systems more employment friendly and liberalisation of product markets;
- measures to promote lifelong learning.

16. Each country confirmed its determination to introduce the measures set out in its Action Plans and to pursue the concept of active ageing. Measures on active ageing should explore what forms of work are appropriate to the needs of older workers and adapt work to suit them accordingly.

17. These measures will help generate soundly-based and equitable growth. We are also willing to share our principles and experiences, including in the relevant international institutions particularly the ILO, OECD and the IFIs, to help foster growth, jobs and inclusion not only in the G8 but throughout the world. We renew our support for global progress towards the implementation of internationally recognised core labour standards, including continued collaboration between the ILO and WTO secretariats in accordance with

the conclusions of the Singapore conference and the proposal for an ILO declaration and implementation mechanism on these labour standards.

Combating drugs and international crime

18. Globalisation has been accompanied by a dramatic increase in transnational crime. This takes many forms, including trafficking in drugs and weapons; smuggling of human beings; the abuse of new technologies to steal, defraud and evade the law; and the laundering of the proceeds of crime.

19. Such crimes pose a threat not only to our own citizens and their communities, through lives blighted by drugs and societies living in fear of organised crime; but also a global threat which can undermine the democratic and economic basis of societies through the investment of illegal money by international cartels, corruption, a weakening of institutions and a loss of confidence in the rule of law.

20. To fight this threat, international cooperation is indispensable. We ourselves, particularly since the Lyon summit in 1996, have sought ways to improve that cooperation. Much has already been achieved. We acknowledge the work being done in the UN, the EU and by other regional groupings. We welcome the steps undertaken by the G8 Lyon Group to implement its 40 Recommendations on transnational organised crime and the proposals G8 Justice and Interior Ministers announced at their meeting in Washington last December. By working together, our countries are helping each other catch criminals and break up cartels. But more needs to be done. There must be no safe havens either for criminals or for their money.

21. We have therefore agreed a number of further actions to tackle this threat more effectively:

- We fully support efforts to negotiate within the next two years an effective **United Nations convention** against transnational organised crime that will provide our law enforcement authorities with the additional tools they need.

- We agree to implement rapidly the ten principles and ten point action plan agreed by our Ministers on **high tech crime**. We call for close cooperation with industry to reach agreement on a legal framework for obtaining, presenting and preserving electronic data as evidence, while maintaining appropriate privacy protection, and agreements on sharing evidence of those crimes with international partners. This will help us combat a wide range of crime, including abuse of the internet and other new technologies.

- We welcomed the FATF decision to continue and enlarge its work to combat **money-laundering** in partnership with regional groupings. We place special emphasis on the issues of money laundering and financial crime, including issues raised by offshore financial centres. We welcome the proposal to hold in Moscow

in 1999 a Ministerial meeting on combating transnational crime. We agreed to establish Financial Intelligence Units (FIUs) where we do not already have them, in line with our national constitutions and legal systems, to collect and analyse information on those engaged in money laundering and liaise with the equivalent agencies in partner countries. We agreed on principles and the need for adequate legislation to facilitate **asset confiscation** from convicted criminals, including ways to help each other trace, freeze and confiscate those assets, and where possible, in accordance with national legislation, share seized assets with other nations.

- We agree on the need to explore ways of combating official **corruption** arising from the large flows of criminal money.

- We are deeply concerned by all forms of **trafficking of human beings** including the smuggling of migrants. We agreed to joint action to combat trafficking in women and children, including efforts to prevent such crimes, protect victims and prosecute the traffickers. We commit ourselves to develop a multidisciplinary and comprehensive strategy, including principles and an action plan for future cooperation amongst ourselves and with third countries, including countries of origin, transit and destination, to tackle this problem. We consider the future comprehensive UN organised crime convention an important instrument for this purpose.

- We endorse **joint law enforcement** action against organised crime and welcome the cooperation between competent agencies in tackling criminal networks. We agree to pursue further action, particularly in dealing with major smuggling routes and targeting specific forms of financial fraud.

- We endorse the Lyon Group's principles and action plan to combat illegal manufacturing and trafficking of **firearms**. We welcome its agreement to work towards the elaboration of a binding international legal instrument in the context of the UN transnational organised crime convention.

22. We urge the Lyon Group to intensify its on-going work and ask our Ministers to report back to our next Summit on progress on the action plan on high tech crime, the steps taken against money laundering and the joint action on trafficking in human beings. We also welcome the steps agreed by our Environment Ministers on 5 April to combat **environmental crime.**

23. There is a strong link between **drugs** and wider international and domestic crime. We welcome the forthcoming UNGASS on drugs. This should signal the international community's determination in favour of a comprehensive strategy to tackle all aspects of the drugs problem. For its part, the G8 is committed to partnership and shared responsibility in the international community to combat illicit drugs. This should include reinforced cooperation to curb illicit trafficking in drugs and chemical precursors, action to

reduce demand in our countries, including through policies to reduce drug dependency, and support for a global approach to eradicating illicit crops. We welcome the UNDCP's global approach to eliminating or significantly reducing illicit drug production, where appropriate through effective alternative development programmes.

Non-Proliferation and Export Controls

24. The proliferation of weapons of mass destruction and their delivery systems threatens the security of every nation. Our countries have been in the forefront of efforts to prevent proliferation, and we have worked closely together to support international non-proliferation regimes. We pledge to continue and strengthen this co-operation. As a key element of this co-operation, we reaffirm our commitment to ensure the effective implementation of export controls, in keeping with our undertakings within the non-proliferation regimes. We will deny any kind of assistance to programmes for weapons of mass destruction and their means of delivery. To this end, we will where appropriate undertake and encourage the strengthening of laws, regulations and enforcement mechanisms. We will likewise enhance amongst ourselves and with other countries our co-operation on export control, including for instance on the exchange of information. We will ask our experts to focus on strengthening export control implementation. And we will broaden awareness among our industrial and business communities of export control requirements.

Year 2000 Bug

25. The Year 2000 (or Millennium) Bug problem, deriving from the way computers deal with the change to the year 2000, presents major challenges to the international community, with vast implications, in particular in the defence, transport, telecommunications, financial services, energy and environmental sectors, and we noted the vital dependence of some sectors on others. We agreed to take further urgent action and to share information, among ourselves and with others, that will assist in preventing disruption in the near and longer term. We shall work closely with business and organisations working in those sectors, who will bear much of the responsibility to address the problem. We will work together in international organisations, such as the World Bank to assist developing countries, and the OECD, to help solve this critical technological problem and prepare for the year 2000.

Next Summit

26. We accepted the invitation of the Chancellor of the Federal Republic of Germany to meet again next year in Köln on 18-20 June.

17 May 1998

THE WHITE HOUSE
WASHINGTON

For Immediate Release
June 26, 1998

Contact: Jack Gribben
(202) 456-7010

STATEMENT OF JOHN KOSKINEN
Assistant to the President and
Chair, President's Council on Year 2000 Conversion

I am very pleased with today's United Nations vote adopting the resolution on the year 2000 problem. It is an important step in our efforts to increase awareness of Y2K outside of the United States and to encourage other nations to take immediate measures to address the problem.

Y2K is a global challenge that highlights the growing importance of information technology in the daily exchanges between countries. It is crucial that all nations work to reduce the risk of system failures in key areas such as telecommunications, banking, and transportation, where failures in one country could significantly affect the world community. The President's Council on Year 2000 Conversion is committed to continuing its work with our international partners to raise awareness and share information on this important issue.

I would like to thank Ambassador Richardson, Ambassador Sklar, Ambassador Kamal of Pakistan, and the UN Informatics Working Group, with whom I was pleased to work on the draft of the proposed resolution, for their efforts, and I look forward to continuing an active dialogue with the United Nations on the year 2000 problem.

###

UNITED STATES MISSION TO THE UNITED NATIONS

799 United Nations Plaza
New York, N.Y. 10017

Tel. 212-415-4050
FAX 212-415-4053

PRESS RELEASE

FOR RELEASE UPON DELIVERY
CHECK TEXT AGAINST DELIVERY

USUN PRESS RELEASE #112-(98)
JUNE 26, 1998

Statement by Ambassador Richard Sklar, United States Representative for United Nations Reform and Management, on the Resolution on the Global Implications of the Year 2000 Problem, in the General Assembly, June 26, 1998

Mr. President, I am pleased to express the United States' support for the resolution on the global implications of the year 2000 problem.

In a world vastly dependent upon electronic systems for the processing and exchange of financial and other data, it is imperative that nations address the year 2000 problem now. Those which fail to do so risk serious disruptions to critical business and government functions. And with the inflexible December 31, 1999 deadline fast approaching, there truly is no time to waste.

This is an international problem that has implications for every nation. More than any other technological challenge we face, the year 2000 problem highlights the interconnectedness of today's world. Year 2000-related system failures in key areas such as international telecommunications, banking and transportation in any one country could have significant effects on many other countries. Nations need not only to address the problem within their own borders but to share information and expertise on possible solutions internationally. The need for this kind of cooperation was one of the key reasons we worked hard to raise the issue at the recent Birmingham G-8 summit, and were so pleased to work closely with the UN Informatics Working Group on the year 2000 resolution. We also look forward to the elaboration of Guidelines for Member States to be set forth by ECOSOC at its upcoming substantive session.

The resolution recognizes that the problem affects more than just large mainframe systems. Electronic devices with date-sensitive microprocessors, or embedded chips, are also at

risk. Unchecked, this so-called "growth industry" of the problem has the potential to cause failures in everything from manufacturing equipment to traffic signals. We believe that, in addition to system challenges, countries need to pay close attention to this important aspect of the year 2000 problem.

We also encourage every nation to examine its year 2000 readiness, and not just in governmental systems. Government officials should be making inquiries on the status of preparations in the private sector, especially with regard to key infrastructure areas including energy, telecommunications, transportation and financial institutions. Member States should appoint national year 2000 coordinators. We have already done so. A coordinator can help countries to raise awareness of the problem among public and private sector organizations.

Finally, we encourage every nation to think about contingency plans for critical business processes as we move toward the new millenium. By this fall, we will have reached a point where, despite all of the best efforts to prepare, some systems for which no year 2000 remediation efforts have begun will not be ready by January 1, 2000. We encourage nations to develop contingency plans for those critical business processes that are most at risk of experiencing failures.

I would like to thank Ambassador Kamal and the Informatics Working Group for all their hard work on this important resolution and for raising the level of awareness of the year 2000 problem generally within the United Nations.

Thank you Mr. President.

* * * * *

United Nations A/52/L.75/Rev.1

General Assembly

Distr.: Limited
17 June 1998

Original: English

Fifty-second session
Agenda item 95 (c)

Macroeconomic policy questions: science and technology for development

Pakistan: revised draft resolution

Global implications of the year 2000 date conversion problem of computers

The General Assembly,

Recognizing that the effective operation of Governments, companies and other organizations is threatened by the year 2000 date conversion problem of computers, or "millennium bug",

Underlining the need for effective action to address the problem to be taken well in advance of the inflexible date of 31 December 1999, beyond which important systems might cease to function,

Recognizing the potentially serious impact that the year 2000 problem could have in all countries whose economies are increasingly interdependent,

Emphasizing that the year 2000 problem could affect both computer systems and much electronic control equipment containing embedded chips and internal clocks, with wide-ranging effects on such important areas as power supplies, telecommunications, financial systems, transport, public health, building and factory systems, food supplies, emergency services, the organization of social welfare and utilities,

Emphasizing also that coordinated efforts by Governments and private, public and international organizations are required to address the year 2000 problem,

Appreciating the establishment of a Trust Fund by the World Bank to assist in the efforts to resolve the year 2000 problem and the voluntary contributions made to it by the member States,

Appreciating the efforts of the Ad Hoc Open-ended Working Group on Informatics of the Economic and Social Council in raising the level of awareness of the year 2000 problem,

98-17104 (E) 170698

1. *Requests* all Member States to attach a high priority to raising the level of awareness, both by ensuring that the private sector is fully engaged in addressing the year 2000 problem and by tackling the problem in those systems within their own control, and to consider, *inter alia*, the appointment of a nationwide coordinator for this purpose;

2. *Appeals* to all Member States to forge global cooperation to ensure a timely and effective response to the year 2000 challenge;

3. *Calls upon* Governments, public and private sector organizations and civil society to share locally, regionally and globally their experiences in addressing the year 2000 problem;

4. *Requests* the Secretary-General to take steps to ensure that all parts of the United Nations system take measures to ensure that their computers and equipment with embedded microprocessors are year 2000 compliant well before the target date by drawing up a plan of action for the United Nations system;

5. *Calls upon* the Economic and Social Council to prepare at its substantive session of 1998 guidelines on which Member States will be able to draw in addressing the diverse aspects of the year 2000 problem;

6. *Requests* the Secretary-General to ensure that the United Nations system closely monitors actual and potential sources of funding to support the efforts of the developing countries and countries with economies in transition to address the year 2000 problem, and to facilitate the dissemination of relevant information on those funding possibilities to the Member States;

7. *Requests* the Secretary-General to report to the General Assembly at its fifty-third session on the steps taken within the United Nations system and with Member States to resolve this problem;

8. *Decides* to include in the provisional agenda of its fifty-third session an item entitled "Global implications of the year 2000 date conversion problem of computers" and to complete its action under that agenda item before the deadline of 31 December 1999.

PRESIDENT CLINTON CHALLENGES BUSINESSES TO ADDRESS THE YEAR 2000 COMPUTER PROBLEM

VICE PRESIDENT GORE DOCUMENTS FEDERAL EFFORTS TO DATE

July 14, 1998
National Academy of Sciences

Today, President Clinton will review the Federal Government's efforts to prepare its critical systems for the year 2000 century date change and challenge businesses to take responsibility for making sure that their systems are ready for the new millennium. The President will announce Federal initiatives to promote information sharing on year 2000 efforts and to connect people who have skills for addressing the problem with employers who are in need of their services.

Order of Speakers:

Dr. Bruce Alberts, President, National Academy of Sciences
Vice President Gore
President Clinton

See attached fact sheet.

PRESIDENT CLINTON CHALLENGES BUSINESSES TO ADDRESS THE YEAR 2000 COMPUTER PROBLEM

VICE PRESIDENT GORE DOCUMENTS FEDERAL EFFORTS TO DATE

July 14, 1998

THE YEAR 2000 PROBLEM. In the second half of the twentieth century, information technology has made possible advances ranging from the ability to invest electronically in markets halfway around the world to satellite tracking of approaching weather systems to ground breaking research to find cures for the most complex diseases.

The year 2000 problem (Y2K) is a threat to that progress. It stems from the use in many computer systems of a two-digit dating method that assumes 1 and 9 are the first two digits of the year. Without programming changes, the systems will recognize 00 not as 2000 but as 1900, which could cause the computers either to shut down or to malfunction on January 1, 2000.

THE CHALLENGE. Y2K is a problem that affects organizations around the world. While the Federal Government is responsible for fixing its critical systems, government and business leaders here and abroad must take responsibility for fixing their systems if we are to succeed in minimizing year 2000-related disruptions. The President and Vice President are leading the Federal efforts and encouraging other governments and private sector organizations to do their part.

PRESIDENT CLINTON ANNOUNCES NEW INITIATIVES TO ADDRESS Y2K CHALLENGE. President Clinton today announced initiatives to help organizations in their efforts to address the year 2000 problem. These initiatives are designed to promote information sharing on Y2K efforts, connect people who have skills for addressing the problem with employers who are in need of their services, and increase awareness of the problem in developing countries.

- Year 2000 "Good Samaritan" Legislation. The Administration will submit to Congress proposed legislation to promote a more open sharing of year 2000-related information by protecting those who carefully share information on Y2K solutions or on whether a product or service is Y2K-compliant, from liability claims based on the sharing of that information. The proposed legislation does not, however, address liability that may separately arise from actual Y2K failures of systems or devices, nor is it intended to alter existing contractual rights.

  Example—Today, leaders of a national industry association might choose not to develop a website on Y2K solutions gathered from several sources for fear that the organization might be held liable for displaying inaccurate information. With the legislation in place, association executives will be more willing to take on this vital clearinghouse function. Unless they know the information is false, their only obligation is to disclose that the information is a republication.

  Example -- Today, a Y2K project manager who tests a particular system and finds it to be non-compliant may be hesitant to share this finding with colleagues in other firms because his company attorney has warned him that spreading such information could lead to product disparagement suits. With the legislation in place, this manager could feel confident in relaying his experiences to others because he will have additional protections against liability. The legislation protects anyone sharing such information unless they act with knowledge that the information was false or with reckless disregard as to the truth or falsity of the information.

• Labor Department World Wide Web Y2K Job Bank. The Labor Department today established a Y2K information technology (IT) version of America's Job Bank/America's Talent Bank (AJB/ATB) at http://it.jobsearch.org in order to concentrate the supply (workers) and the demand (jobs) in the IT industry in a single place. The product of a unique partnership between the Department and the States, AJB/ATB, at www.ajb.dni.us, already provides a significant penetration into the area of computer and high-tech jobs and talent, with approximately 40,000 resumes and 120,000 IT jobs listed.

• World Bank Contribution. The United States will contribute $12 million to support the World Bank's efforts to increase awareness of the year 2000 problem in developing countries, where Y2K information is scarce. The Bank is holding 20 regional Y2K conferences around the world to increase awareness and provide information about the problem to developing countries.

• National Campaign for Year 2000 Solutions. Later this month, the President's Council on Year 2000 Conversion will kick off its "National Campaign for Year 2000 Solutions" to promote public and private sector action on Y2K and to foster information-sharing about solutions.

PRESIDENT CLINTON'S COMMITMENT TO INCREASING AWARENESS OF Y2K. President Clinton is committed to encouraging businesses to focus on fixing their year 2000 problems.

In February, he established the President's Council on Year 2000 Conversion to coordinate the Government's efforts to increase awareness of the problem and encourage action in public and private sector organizations. The Council's 34 agency working groups are focused on areas that range from energy to telecommunications to financial institutions.

• The Small Business Administration, chair of the small business working group, is focused on increasing awareness of the problem among the Nation's more than 20 million small businesses. As part of its "Are You Y2K OK?" campaign, SBA is encouraging small business owners to determine their Y2K risk by conducting a self-assessment test available on SBA's Internet Y2K web page (www.sba.gov/y2k/).

• The Energy Department and the Federal Energy Regulatory Commission, co-chairs of the energy working group, are working with industry associations such as the North American Electric Reliability Council, the American Petroleum Institute, the Natural Gas Council, and the Gas Industry Standards Board to ensure that the energy industry is addressing the problem as it relates to electric power and oil and gas supplies.

• The Federal Communications Commission, co-chair of the Council's telecommunications working group, is meeting with domestic and international telecommunications carriers and equipment manufacturers to discuss Y2K, and has written to major companies and organizations in all sectors of the industry to emphasize the importance of addressing the problem.

• The Federal Reserve, chair of the financial institutions working group, and other Federal financial regulatory agencies are making year 2000 progress a key component of their examinations of banks and other financial institutions and promoting industry-wide systems testing.

President Clinton is also committed to increasing international awareness of the problem.

• The President has discussed Y2K with heads of state at both the G-8 Birmingham summit and the Summit of the Americas. Also, under the President's leadership, the Year 2000 Council worked closely with the United Nations on the draft of a recently passed UN resolution that calls upon all member states to act on the problem.

United States Information Agency

Transcript, Digital Video Conference with John Koskinen

John Koskinen, Chairman of the President's Council on the Year 2000 (Y2K) Conversion, held this digital video conference (DVC) with reporters in Moscow July 16.

I'm delighted to have a chance to join you this morning and inaugurate this wonderful program that the United States Information Agency has put together to allow us to reach out to countries around the world to discuss the problem presented by the transition from the 1999 date to the year 2000. As Jonathan noted, the President asked me to come back to organize the United States Federal Government's response to this problem. As I have told our federal agencies, we view this as a three-tiered problem.

Our first problem, and the one we have most direct control over, are our own federal systems. And those are, in many cases, very large, very complicated, and in a lot of cases, somewhat antiquated. In the 1950s and the 1960s, the federal government was one of the first, and really the largest, developer of software and information technology. Which means that most of those programs were custom-designed, not standard, and were built on over time, as we expanded the processing.

So our first problem is to ensure that basic government services, particularly to the public, are maintained. We are focused on benefit payments, both for retirees as well as for health care payments. We're concerned about unemployment insurance payments, payments to our veterans, and of course, are very concerned about the operations of our Internal Revenue Service, which collects and processes a trillion-and-a-half dollars worth of payments every year.

All of the systems behind those programs are very complicated and we've been working on them, in some cases, in our Social Security retirement benefit program, as long as nine years. As a result, the Social Security benefit payment system appears to be nearing completion in its work. Unfortunately, in a number of other federal agencies, we still have substantial work to be done, even though every federal agency has been working on this problem since the end of 1995.

The second tier, from our perspective of the problem, is the systems that we exchange data with around the country and around the world. Because it's clear, in this interconnected world we all live in, that if our federal systems are able to function, but the systems with which they exchange data or financial information are not able to function, we will have a difficult problem for the economy and for the American public.

When I met with all of the heads of the major federal agencies when I started, and I've had 43 meetings with 43 different agency heads with their senior staffs, and talked to them about the three-tiered problem, they hedged and were focusing their time on the first tier, their systems. They had begun and the government had begun

to look at the second tier problem of the interfaces of those systems outside the government. And what I spent time talking to them about was the third tier of the problem, which is reaching out beyond their normal activities to those operating in the country and around the world in their areas of interest, where a failure would create an insignificant problem either for the economy or for the public.

And it's that third tier that we are talking about here today. Because we are very concerned that even if the federal systems work and even if the systems they exchange data with work, but other significant systems around the world do not work, there will be great difficulties, not only for those who depend directly on those systems, but for us as well. So while we do not control those systems, we cannot tell those people, either in our private sector or of any of those of you around the world, what to do, we are very anxious to reach out and to provide whatever support and assistance we can to encourage people to deal with this problem effectively. Our biggest concern, both within the United States and internationally, are those organizations that are not paying significant attention to the problem or any attention to the problem. Our experience is that organizations that are focused on this issue, that have strong leadership from the head of the organization, and are devoting resources to the program and making it their top priority, obviously have the greatest chances of success in dealing with the problem. Where we are concerned are where we do not have that kind of organization in place. In the United States, our major concern are small to medium-sized organizations, both in industries around the United States, but as well as in state and local government. Abroad, we are concerned about the at least 50 percent of the countries in the world that have barely begun to pay attention to this or are not paying attention at all. And that's one of the reasons I was delighted to receive the materials that Russia has put together in May, organizing an approach to dealing with this problem. Because I think of all the steps you can take, that is the most critical one, which is to provide an organized approach to bringing everyone in the government systems together, starting to work and focus on the problem.

Our concern and our analysis is that many of the small to medium-sized organizations, and even some of the countries around the world who have not begun to pay attention to the problem, have not done so because they assume that this is not their problem. If they are not running major mainframe application programs, they assume that the year 2000 problem does not affect them. What they are overlooking is what I'd call the growth industry of the problem, which is the problem of imbedded chips or integrated circuits.

And it turns out that numerous operating systems, manufacturing plants, transportation systems, communication systems, all operate on the basis of integrated circuitry or embedded chips in their hardware, that in effect, monitor and control the operations of those processes. Now, fortunately, only a very small percentage of the chips in their applications have the potential to malfunction on January 1 of the year 2000. That percentage has been estimated, as a general matter, to be between 1 and 2 percent. It could be as high, in some applications, as 5 percent.

And that's a small percentage, but one year recently we shipped almost 5 billion chips into commerce around the world. So with a 2 percent risk rate, that means there are 100 million chips, in that year alone, that are capable in their applications to create difficulty. And we know that around the world, we are running oil refineries, power plants, manufacturing facilities, large transportation facilities, and cargo ships with people sitting at computers responding to the information that is produced by those integrated circuits or embedded chips.

And so therefore, we are concerned that many organizations, many governmental organizations in the United States have not really focused on that aspect of the problem as it directly affects them. So with our state and local governments, for instance, we are telling them they need to do an assessment to ensure that their mobile communication systems will be up and operating, to ensure that their emergency equipment will operate, to ensure that their local utilities will operate, to ensure that their local transportation systems and traffic lights will operate effectively.

In many ways, it would be an easier problem to deal with if we could guarantee people that everything would stop. Because then, everyone would go out and fix everything. In this case, and certainly with the imbedded chips, the vast majority of the systems will be unaffected. And so, it's important for people not to waste money replacing or renovating systems that don't need to be replaced. And therefore, the most important step after you become organized is to actually do an inventory and an assessment of all operations, both the application systems and software systems, but also manufacturing and operating systems, to determine whether there are areas that need to be pursued further and whether there are areas that need to be tested to ensure that there will not be a difficulty as we move across those borders.

The way we have organized the federal government to deal with these three tiers of operations is, we have created what we call the President's Council on the Year 2000 Conversion, which I chair. It has a single representative from 35 different agencies across the federal government, including all of our regulatory agencies that regulate our financial markets and our financial institutions, as well as agencies including, obviously, the Defense Department, even the CIA. Because it is critical for us to be able to share information across those borders.

We have organized and analyzed all the sectors of the American economy and governmental operations, including international operations into -- and we have now 34 sectors, which are headed, each of them, by a separate agency. Sometimes the same agency has more than one sector and they head up a working group of appropriate federal agencies dealing with that area and reaching out to those operating in that sector. So, for instance, internationally, our international communications sector involves several federal agencies. It is chaired by Jonathan Spalter and USIA and charged with doing whatever we can to communicate through both our embassies and our operations of law, but directly with countries around the world, to demonstrate our concern.

Our basic, ultimate list, we think, is from our increasing dependency on international cooperation. Not only is it a global village, it's a global economy that depends increasingly on the exchange of data and financial services electronically. So that we are concerned, yet as an old adage says, the chain is only as strong as its weakest link. And we are looking at the chains in financial transactions internationally and telecommunications internationally and transportation internationally. Because we are concerned that all of those chains are at risk if there are any weak links. So it is in our own interest, as well as in our interest in the welfare of those operating around the world, to do whatever we can to try to provide assistance to those operating in those areas.

And I think the first thing we are focused on in trying to provide assistance is to increase the level of awareness and activity around the world. We have worked closely with the United Nations. I worked with Ambassador Kamar of Pakistan, who heads the United Nations working group to pass the recent resolution. In a resumed session, the United Nations called on all member states to take action with a report back to the general assembly in October. I have met with Mr.

Wilkenson, the head of the World Bank which is now, thanks to a contribution from Prime Minister Blair of England, holding 20 regional conferences around the world to provide information to countries across the globe.

The President made a major address on this subject on Tuesday with the Vice President and announced that we will be contributing $12 million to support the World Bank's efforts to reach out around the world. I have met with the head of the International Monetary Fund, who has agreed that they will use whatever influence they have to encourage countries around the world to pay attention to this problem and to devote the appropriate resources to it. I've also met with Intelsat, which runs the major communication satellite network around the world.

One of the rare pieces of good news is that the satellite system is fine. The problem is access through ground stations around the world and Intelsat, which is basically owned by 143 countries, is concerned that many countries, if they do not pay attention to this problem, will lose their access to the international communication network. So it's a major challenge. It could even be called a crisis. We are anxious not to cause people to panic and take unproductive or counter-productive activities, such as deciding to take all of their money out of financial markets or out of banks. We'd like to not have everyone show up at the end of next year trying to fill up their gas tanks.

But at the same time, we need to get everyone around the world to treat the problem seriously and to focus on the appropriate resources to deal with it. As Jonathan said, as the President said on Tuesday, this is the greatest management challenge that the world has ever, in a concerted effort, had to face. And we are prepared to do whatever we can to provide assistance to those operating and working in this area around the world.

So that's the short form background of where we are, our approach to the problem. And I would be happy to answer any questions you might have about anything I've said or anything else that you have a question about.

Q: What is the price or the cost to the U.S. federal government? We have heard different figures of fill-in dollars. What do you think about the cost of the solution to this challenge?

A: That's a good question. It's one of the few questions I have a clear answer to. The cost for the federal government to fix its own systems over the period from fiscal year 1996 through fiscal year 1999 is almost exactly 5 billion U.S. dollars. Of that amount, about 1.2 billion U.S. dollars will be spent in the fiscal year that begins October 1st of this year and about $2 1/2 billion is being spent this year. So, well over half of the $5 billion will be spent in 1998 and 1999 and we are, as we say, confident in those numbers because we ask the agencies every three months to provide us progress reports on how they're doing and also their present cost estimates.

Now, we are asking the Congress, because we are getting close to the year 2000, in the appropriations that they are now considering, to create a contingency or emergency fund for any additional, unexpected expenses that may occur. And it will not surprise me at all, because of the unknown nature of this problem and the unique nature of it, for our $5 billion number to increase by as much as another 10 to 15 percent.

Q: What is the percentage of world chips available that you expect to fail in the year 2000? Do you think it is impossible to deal with all the possible unexpected failures within this brief period of time?

A: With regard to the percentage of chips that will fail, as I noted, there is no one who knows the absolute answer to that. The experts have estimated that about 1 to 2 percent of the chips will fail. In some forms of applications, that could be as high as 5 -- some people have even found that 7 to 8 percent fail. I would note, having met with the Chip Manufacturers Association recently to talk with them about this problem, that often the chips -- generally, the chips themselves are not the problem. They are basically neutral about the date. The problem comes when the chips are installed in either a circuit board or in an operating system and programmed by whoever is manufacturing it. And if they program it to be date-sensitive, that's where the problem is created.

So, the difficulty is that the chip manufacturers often don't know what use the intermediate suppliers have made of those chips and in terms of whether or not they will fail. But as a general matter, our experience thus far has been that a very small percentage of the chips will fail. But it's a small percentage of a very large number of chips.

With regard to the software, one of the reasons these problems exist is that when programmers 30 to 35 years ago began to program trying to save space by only identifying the year with the last two digits -- for instance, 1965 was identified as 65 because it saves significant memory space -- their assumption was that the programs they were designing would never be in use later on, so it would not be a problem. That assumption continued to carry through even into the early 1990s, when people assumed that the software they were programming would only be in use three to four years and then would be replaced by new software and the problem could be solved near the end.

Part of the problem with that is that many companies and many people, as a result, paid little attention to this problem until very recently. Because their assumption was that it would be an easy solution simply to buy new software. And in some cases, that will be the solution and if that's all that's involved, you can solve the problem very easily in the time remaining. The difficulty is, with anyone running anything that looks like a very complicated system -- and most financial management systems, tax management systems, financial transaction systems, are very complicated. They aren't a single-software system and they aren't a system that we've just bought recently. So banks, insurance companies, brokerage houses, all have large systems that have been built over time in a process of evolution, where the newest software was added into or on top of an existing system. And it's that older existing system with all of its software systems and all of the custom design that is the core of the problem. And that is why, if you only have a personal computer and you simply need a new upgrade, you'll be able to solve the problem easily. But if you're a large institution, particularly a large bank or a large insurance company, you've got a lot of software systems that you need to upgrade and renovate because there is no easy replacement for them. That's the difficulty.

With regard to the time, obviously some large financial institutions in the United States have been working for over two years already on this problem, so that by definition, if you started today, there aren't two years left. In fact, there are 533 days left, for those of us who are forced to keep track. And therefore, one of the things we are trying to do is encourage the sharing of information wherever we can, so that organizations starting to deal with this problem can take advantage of and get the benefit of the work that's already been done by others around the world.

And the President announced on Tuesday that one of the things we're now working on is to limit the liability of companies that exchange information about how to

deal with this problem, in case all of their information isn't a hundred percent accurate, so that they won't be sued because of the information. They can still be sued because of the systems that don't work, but what we're trying to do is make sure that everyone has the ability to share and provide the benefits of the work they've done thus far.

Q: A few days ago, the American defense department decided to share information with the Russian defense forces with the view of ensuring the perfect functioning of the early warning systems....How well is the American administration aware of what is being done in Russia that will meet the challenge to deal with the problem...?

A: Well obviously, all of us have a high level of concern. Not only about nuclear weapons, but nuclear power plants and other issues that could be a great threat to people anywhere in the world as a result of accidents. So, I have met with the secretary of defense and the deputy secretary and we talked about their initiative to try to ensure that at a minimum, there are no misunderstandings as we move toward the year 2000. And either our system's or your system's early warning systems, or the early warning systems of other countries -- if they have a difficulty with the transition, don't generate mistaken information that people would then respond to.

So we are very anxious, at the first step, to make sure that we share information, that there is mutual comfort, that if there is a problem with an early warning system, we'll have backup ways of checking with each other to ensure that we have accurate information. But we are also concerned about a significant other set of problems.

As you know, by the president's recent strong support of the International Monetary Fund program with Russia, we have a great interest in and hope for the continued expansion and growth of the democratic system in Russia. We are anxious to support the stabilization of the Russian economy and its expansion because we feel that everyone will benefit with a successful, active, democratic but economic system in Russia, working as a major partner with us going into the future.

We also have concerns in other countries if there are major economic difficulties in any country as a result of the year 2000 problem, and we view that as a problem for the world community. We trade with countries, we have increased trade with Russia, with other countries. We depend upon those countries both for our supplies and products, as well as their markets, so that we clearly do believe that there is no country anymore in the world engaged in international commerce and interchange that can stand by itself and be unaffected by the problems elsewhere. So, while we have the highest concern to make sure there are no accidents with either nuclear weapons or nuclear power, we have an equally high concern to do whatever we can to make sure that there are no other major economic or social difficulties as a result of information technology failures.

Q: What about the law proposed legislation by President Clinton to limit liability in the sharing of technical information about Y2K? Do you think that law sould be adopted in Russia?

A: We hope that legislation will pass this summer in the United States. We think that it is an important concept, and it would be important in Russia as well. I'm not familiar with the details of your legal system. We have a very complicated system where people have a lot of legal rights to bring disputes into the court system. That is what concerns us because here companies are afraid to either discuss their

experiences with a certain software or hardware product in terms of whether it works or not, or to share information about how they fixed a system, for fear that if they say, this is how we fixed our system," and someone else relies on that and it turns out it doesn't work in their system, the first company will be sued because of that exchange of information. As a result, we have many large companies here who have a lot of information that they do not feel they can tell anybody about or share.

So, we think it's important here. We think, especially with the fact that your organized program in Russia is coming together late, that it will be critical for you, for industries and government agencies and everyone working on the problem, to view this as a community effort and to try to share information as much as they can. Obviously, you don't want people putting out information with no basis whatsoever. And so, you want them to have some standard of care. We're talking about -- you have to do it in good faith and without gross negligence. But beyond that, we think on balance we do better with a free flow of as much information as we can get, rather than trying to hold people very strictly accountable if their information isn't totally accurate.

Part of the reason we feel that way is that no one can guarantee anything in this area. So when a company says they are ready to deal with the year 2000, they are saying that on the basis of the best information they have. But because this is a unique problem, there's no way to know until we get to January 1, 2000, whether all the systems that have been fixed will actually work. So therefore, I would urge you, in your approach, to try to get people to understand this not a time for competitive advantage. This is a time for a community effort to try to ensure that the basic infrastructure in your society and your country works, that the basic ability to conduct financial transactions as well as personal transactions are not interfered with to the extent possible.

Q: What other powers of the committee you're heading? Who are its members? And has it got a definite plan? Is it one of the committee's functions to control the activity of the government agencies and departments in handling the Y2K problem?

A: That's a very good question. Each of the major federal agencies has one member on the committee. I told the heads of the agency they could select a member, but there were two criteria for membership. One is, whoever was selected had to be senior enough in the organization to know what the agency was doing internally and externally in its outreach programs to deal with the problem. I needed someone who knew what the agency's activities were. The second criteria was, I needed someone with enough authority in the agency to be able to commit the agency to taking action in the course of a committee meeting without having to check back with the agency.

As I told the council, "The only words that will be unacceptable in any of our meetings will be, `I'll have to check on that.'" So that means that basically, the members of this council are either the deputy secretaries, the number two person in the department, or the chief information officer, the senior technological person in the department. And the agency heads have all agreed that if the council decides an action needs to be taken, that the members of the council from the agencies have the authority to agree on behalf of their agency to take that action.

We are monitoring the activities of the agency. In the White House, according to the President, we have an Office of Management and Budget. That is, the budget and management arm of the government. I used to be the deputy director for management at that organization. When I was in the government before, we set up

a quarterly reporting process to the Office of Management and Budget, which the agencies provided standardized reports for the level of their progress; what percentage of assessment had they done of their mission critical systems, what percentage of renovation -- fixing those systems had they done, what percentage of testing had they done, and ultimately, what percentage of their systems were implemented with the year 2000 compliant operations.

And those quarterly reports come into OMB every quarter and they come to the council and to me as well. And I am now working with a half a dozen large federal agencies who are not making sufficient progress, we think, to be able to deal with the problem in the time remaining. So I now meet with them on a monthly basis with their senior management reviewing their monthly progress. We have, in terms of our power, an executive order that calls upon the agencies to cooperate with the council.

But my power and the council's power is primarily because everyone knows the president and the vice president personally asked me to serve. And so therefore, they know I can call the resident and the vice president back if I need to. But my management style is not to issue edicts; it is rather to work in a collaborate, consultative basis with everyone so that we feel that we're working in it together rather than I'm telling them what to do.

Similarly, in our reaching out to the private sector organizations, where we clearly have less authority in many cases to tell them what to do, our strategy is to work with them in a partnership, where we exchange information with them and they with us, and we provide them support where we can. The request for the Good Samaritan legislation limiting liability came from some of those private sector industry groups who are concerned about their inability to exchange information. And they asked us, as part of our meetings with them, could we address that problem, which we hope to be able to do this summer.

In terms of our planning, we have a set of benchmarks for the federal agencies that are set up in that quarterly reporting process. They are supposed to be complete with all of their fixes of the systems, all the remediation by September 30th of this year. They are supposed to be complete with all testing of those systems by December 31st of this year and they are supposed to have all implementation done by March 31 of 1999.

And the reason that deadline, which used to be November of '99, was moved to March of '99, was because everyone recognizes when you've fixed the system, you've tested it, and you've implemented it, then you still have to go back and test and run it again -- because this is a complicated, unique problem and there are always more things that people think they've fixed, that when you start testing them in operation with other systems, have not been fixed.

Now, not every agency is going to meet those deadlines. And the six large agencies that I'm meeting with are the ones we think that are at risk of not meeting some or all of those deadlines. But we have some area of comfort in the sense that if they do not meet the March 31 '99 deadline, we hope that they will be able to, within a month or two thereafter, meet that deadline. My advice and experience is that it is important not only to have general deadlines like that. Also we have now asked the agencies to do is to develop a management plan from now until they're finished, with a monthly set of benchmarks as to how many systems they propose to have through the process each month. And then to report, on a monthly basis, against their progress against those benchmarks.

Because every agency will be in different circumstances with different systems

and different challenges and if you're trying to manage the process and see where your difficulties are, the most important information is who is falling behind their monthly management plan. So, we have moved to that direction because we're trying to make sure we get an early warning of where people are falling behind their own plan.

The other thing you will find in any organization that's through around the world, is if you ask someone, are they going to be ready by the deadline, they will always say yes. Everyone's optimistic. No one wants to say they can't do it. But what we're doing with the monthly benchmarks now, which we just started doing two or three months ago, is try to check to make sure that what we don't have is people making sort of flat progress for the first several months and then at the end all of a sudden the graph goes up. And it, you know, generally won't make sense to say that we're going to do 70 percent of the work in the last month before the deadline.

So, one of the reasons we ask them to share with us their plans, on a monthly basis throughout the entire process, is to test the reasonableness of those plans and to try to get them to understand that they need to manage against a reasonable set of expectations each month. The other thing that we have discovered, when you're managing a difficult problem for people to deal with, is to attach the highest priority to this problem. You will find that organizations will set up an organization to deal with this, it will be important to them, but they will have other priorities that are important and no one will disagree with what they're working on in the information technology area. They will be upgrading systems, they will be adding the systems, they will be dealing with other problems of the agency or the organization. But if this work is going to get done, this project has to be the most important.

So in two or three major federal agencies in the last three months, we have succeeded in getting the Congress and the agency management to understand that some policy initiatives and some changes in programs that we think are important will have to be delayed so that we can devote the appropriate time and resources to solving this problem. Because what it turns out to be is there's only so much space and time available to work on a system. And often times, the people who are providing new policies and programming new policies into the system are the same people who have to actually fix the system. And they can't do both things at the same time.

So, it's not a question of just hiring more people. There's only so much availability of the systems to be able to be worked on. So, one of the things we're doing now is to get concerned about some of the federal agencies and their ability to meet the deadlines -- is getting them to delay some of the things that they or the Congress or even the president would like to have implemented sooner. And we're going to delay some of those things to try to make sure that the systems operate.

For instance, in our Medicare health benefits program, we have changes that the Congress has asked to make in the way the benefits are calculated and the amount of benefits. And the organization/agency running that program announced two weeks ago that some of those changes, in some cases increasing benefits, will be delayed because the system otherwise would not be able to function effectively on January 1, 2000. And as the head of the organization said, if the system doesn't operate at all, it doesn't matter what the policies are, so that it would be a great mistake to have a good, new policy and have to program it into the systems and by virtue of that, have the system shut down.

Q: What steps have already been taken to date, particularly steps to coordinate with the Russian side?

A: Well, I assume that you'd like to know steps are we taking internationally, particularly with the Russian side. As I noted, we are working with the United Nations and the economic and social committee there to provide as much information as we can to countries around the world. We are financially now supporting the World Bank effort to work with developing countries and those starting late on the problem, to provide information and expertise about how to deal with that problem.

We have asked American embassies and ambassadors around the world to begin to engage in discussions with each of their host countries about the level of their activities and what problems they are having, so that we will begin to, with other countries, develop a picture of where each country in the world is, because all of us will have interest in knowing where the difficulties are likely to be and where countries are making progress.

With regard to our direct relationships with Russia, as someone noted earlier, the secretary of defense has already offered to share information with regard to the early warning systems. We are also anxious to provide expertise and information wherever that is appropriate. We are working with the International Bank for International Settlements, which is organizing financial, central bankers around the world to deal with the problem. Our Securities and Exchange Commission is working with the international securities market regulators, trying to provide information to financial market regulators and operators around the world.

So that we are trying to provide as much information as we can, our Federal Aviation Administration, which runs our air traffic control system, is working and pushing the International Transportation Association to work with air traffic control systems around the world. We are, in fact, anxious to provide whatever assistance we can to the air traffic control system in Russia because obviously we have much air transport and traffic, not only with Russia but all of Asia does as well.

So, in each of the sectors, we have asked our agencies here to work with their international organizations to reach out and provide assistance.

[end transcript]

THE WHITE HOUSE

Office of the Press Secretary

For Immediate Release July 14, 1998

REMARKS BY THE PRESIDENT
CONCERNING THE YEAR 2000 CONVERSION

National Academy of Sciences

11:13 A.M. EDT

THE PRESIDENT: Thank you very much, Mr. Vice President, Dr. Alberts, to all of our platform guests, Senator Bennett, Senator Dodd, Congressmen Horn, Kucinich, LaFalce, and Turner, and members of the administration who are here, and all the rest of you who are committed to dealing with this challenge.

This is one of those days that I never thought would ever arrive, where Al Gore has to listen to me give a speech about computers. (Laughter.) Being President has its moments. (Laughter.)

I have to ask your indulgence because this is my only opportunity to appear before the press today, and I need to make a brief comment about something that is also of importance to all of you, and that is the agreement that was reached yesterday between Russia and the International Monetary Fund to stabilize the Russian economy.

I think all of us understand that a stable and democratic and prosperous Russia is critical to our long-term national interests. Ever since the fall of communism there, there has been a strong bipartisan consensus in our national government, and I believe in our country, to working toward that end.

The commitments that Russia made in connection with yesterday's agreement will substantially advance economic reform and stability there. Now it is critical that those commitments be implemented to strengthen confidence in their economy.

It is clear, I think, to all of us now that our prosperity here at home in America is deeply affected by the economic conditions elsewhere in the world. About a third of our economic expansion that the Vice President referred to, which has given us 16 million new jobs and the lowest unemployment rate in 28 years with the lowest inflation rate in 32 years, has come from our exports and our economic relations with the rest of the world. We, therefore, have a clear interest in playing a leading role to advance freedom and prosperity and stability.

One of the most cost effective ways of doing that is through the International Monetary Fund, the world's financial firefighter. For the first time in 20 years now, the IMF has had to draw on special emergency reserve to underwrite this Russian financial package, because its resources were stretched dangerously thin due to the financial difficulties throughout Asia, principally.

To protect our economic strength, therefore, it is imperative that Congress act now to promote global economic stability by paying in America's share to the IMF. Earlier this year the Senate, in an overwhelming bipartisan vote, endorsed legislation to strengthen the IMF and to pay our fair share into it. Since then, the legislation has languished in the House. If we fail to act responsibly at a time when there is so much financial uncertainty in the world, we will be putting our farmers, our workers, and our

businesses at risk. This is a time to put progress ahead of partisanship, and I ask Congress to proceed to do so. (Applause.) Thank you.

Let me also say at the outset, I want to say a special word of thanks, as the Vice President did, to John Koskinen and his whole team for the work they are doing and to all the people that are working with them. We have just on this platform representative people from utilities, from transportation, from finance, from telecommunications, and from small business. And this really is a joint effort we are all making.

But I thank you, John. You know, before I became President, John Koskinen was a personal friend of mine -- I doubt if he still is now that I got him to do this. (Laughter.) But what's a friendship to save the country's wires, so I thank him. (Laughter.)

I asked Bruce Alberts this -- I remembered that Richard Berks' magnificent statue of Albert Einstein is right outside here, and I wish we could bring him to life for this moment. But I'll drive by it on the way out for inspiration.

It seems unbelievable that it's only 535 days from now, at the stroke of midnight, when we will usher in a New Year, a new century, a new millennium. It will be, to be sure, an astonishing age of possibility, of remarkable advances in science and technology, a time when information clearly will widen the circle of opportunity to more people in the world than ever before, and when technology will continue to shrink our small planet and require us to deal with challenges together, including that climate change challenge that Dr. Alberts referred to.

It is fitting, if more than a little ironic, that this same stroke of midnight will pose a sharp and signal test of whether we have prepared ourselves for the challenges of the Information Age. The Vice President discussed the design flaw in millions of the world's computers that will mean they will be unable to recognize the year 2000. And if they can't, then we will see a series of shutdowns, inaccurate data, faulty calculations.

Because the difficulty is as far flung as the billions of microchips that run everything from farm equipment to VCRs, this is not a challenge that is susceptible to a single government program or an easy fix. It is a complex test that requires us all to work together -- every government agency, every university, every hospital, every business, large and small.

I came here today because I wanted to stress the urgency of the challenge to people who are not in this room. So often one of the wry and amusing aspects of the nature of my work is that when I give a speech like this I am typically preaching to the choir, as we say back home. But hopefully the sermon is heard beyond the four walls of this room because, clearly, we must set forth what the government is doing, what business is doing, but also what all of us have yet to do to meet this challenge together. And there is still a pressing need for action.

The consequences of the millennium bug, if not addressed, could simply be a rash of annoyances, like being unable to use a credit card at the supermarket, or the video store losing track of the tape you have already returned -- has that ever happened to you? It really is aggravating. (Laughter.) It could affect electric power -- I just want to remind you that I used to have a life and I know about things like that. (Laughter.) It could affect electric power, phone service, air travel, major governmental service.

As the Vice President said, we're not just talking about computer networks, but billions of imbedded chips built into everyday products. And it's worth remembering that the typical family home today has more computer power in it than the entire MIT campus had 20 years ago. An oil drilling rig alone may include 10,000 separate chips.

The solution, unfortunately, is massive, painstaking, and labor intensive. It will take a lot of time to rewrite lines of computer code in existing systems, to buy new ones or put in place backup plans so that essential business and government services are not interrupted.

With millions of hours needed to rewrite billions of lines of code and hundreds of thousands of interdependent organization, this is clearly one of the most complex management challenges in history. Consider just one major bank, Chase Manhattan. It must work through 200 million lines of code, check 70,000 desktop computers, check 1,000 software packages from 600 separate software vendors.

The government's Health Care Financing Administration, known affectionately by the governors and others as HCFA, which runs Medicare, processes almost 1 billion transactions a year. It' s computer vendors must painstakingly renovate 42 million lines of computer code.

All told, the worldwide cost will run into the tens, perhaps the hundreds of billions of dollars, and that's the cost of fixing the problem, not the cost if something actually goes wrong.

Already extraordinary efforts are underway by the people on the platform -- many of you out here and others -- but more must be done. We know first we have to put our own house in order, to make certain that government will be able to continue to guard our borders, guide air traffic, send out Social Security and Medicare checks, and fulfill our other duties. We've worked hard to be ready. I set a government-wide goal of full compliance by March of 1999. John Koskinen is heading our council on the Y2K problem. I've met with the Cabinet and charged them personally to produce results and report quarterly to OMB on progress. We're working with state and local governments to do the same thing.

We have made progress. As has already been said, the Social Security Administration has more than 90 percent of its critical systems ready. Other agencies, like EPA, FEMA, and the VA, are well on their way to meeting our goal. But not every agency is as far along as it should be. I have made it clear to every member of my Cabinet that the American people have a right to expect uninterrupted service from government and I expect them to deliver.

I want to thank the thousands of individuals who are working to prepare our government and to make sure we can stay open for business. I especially want to thank the Vice President and John Koskinen and the people who are working with them at OMB and elsewhere. And I very much appreciate these members of Congress who are here and the extraordinary bipartisan interest and support meeting this challenge has engendered.

In my proposed balanced budget for 1999, I asked Congress to fund this initiative on a one-time basis, because it is literally a once-in-a-lifetime challenge. I urge the Congress to fully fund it and to provide contingency funding so that we can respond the unforseen difficulties that are sure to arise as we near January of 2000. We have worked closely with Senators Bennett and Dodd and Congressman Horn and Congressman Kucinich and the other members who are here -- Congressmen LaFalce and Turner and others in the Congress. As I said, there has been a heartening amount of

interest in this by people who actually know quite a lot about it in the Congress, and that's a very good thing.

I think we all understand that this is a case where we cannot allow, even in this election season, any shred of partisanship to impinge on the national interest. We, after all, only have 17 months to go.

I believe we also have a role to play in helping to meet this challenge around the world. Surely we can't be responsible for the preparedness of other countries, but I can make the same argument I just made about the IMF and Russia -- if increasingly our prosperity is tied to the well-being of other nations, it would obviously have adverse consequences for us here at home if a number of our trading partners had major malfunctions.

When I was meeting with the world's major industrial organizations in Birmingham, England, a few months ago, I brought this up and I found that we had become far more invested in this and involved in this than some other major nations. When I was in Santiago, Chile, at the Summit of the Americas, I brought it up in our private meeting and a number of countries had literally only begun just to think about the problem.

So I think it is important that the United States recognize that the more we can do to help other countries meet this challenge in a timely fashion, the better off our own economy is going to be and the more smoothly our own businesses will be able to function as we pass over into the new millennium. The United States, to try to help, will provide $12 million to support the World Bank Year 2000 fund for developing countries.

I also want to say what we all know and what you can see from the platform, which is this is not a government problem alone. By far the most significant potential risks fall in the private sector. Large firms already have spent hundreds of millions of dollars to make sure their systems are ready. Many have spearheaded remarkable efforts to make sure their firms and their whole industries are ready. We're encouraged that dozens of firms and thousands of people on Wall Street last night began a simulation to test whether they are ready. And the telecommunication, banking, electric power, and airline industries all deserve praise for the seriousness with which they are taking the challenge.

I want to compliment one person back here in particular. Steve Wolf came all the way back from Africa, got here at 3:00 a.m. in the morning to show up to manifest his understanding of the importance of this challenge to the airline industry, and he is still breathing the rarefied era of Kilimanjaro, so we thank him especially for doing that. (Applause.)

But let me say, in spite of all this progress, in the business sector just as in the government sector, there are still gaping holes. Far too many businesses, especially small- and medium-sized firms, will not be ready unless they begin to act. A recent Walls Fargo bank survey shows that of the small businesses that even know about the problem, roughly half intend to do nothing about it. Now, this is not one of the summer movies where you can close your eyes during the scary parts. (Laughter.) Every business, of every size, with eyes wide open, must face the future and act.

So today I would issue three challenges to our business community. First, every business must take responsibility for making sure it is ready. Any business that approaches the New Year armed only with a bottle of champagne and a noisemaker is likely to have a very big hangover on New Year's morning. (Laughter.) Every business should assess its exposure, asks vendors and suppliers to be ready as

well, and develop contingency plans, as we are, in case critical systems or systems of vendors fail as we move into the year 2000.

I want to especially thank Aida Alvarez and the Small Business Administration and its supporters in Congress. And I thank you, Mr. LaFalce, in particular, for the work that has been done to spread the message in the small business community.

And I'd like to salute one firm represented here, the Torrington Research Company, which makes fans for cars and computers. It has only 55 employees, but they've taken the time to check their system and by the end of this year they will be ready --by the end of this year. I want every small business in America to follow their lead. (Applause.)

As the Vice President said, we need literally an army of programmers and information technology experts to finish the task. Many of the computers involved are decades old; some of them use programming language no longer used or even taught. There is a wealth of knowledge in America's tens of thousands of retirees who once worked in the computer industry or government as programmers or information technology managers. I'm pleased to announce that the Department of Labor will expand its jobs bank and talent bank to help to meet this challenge. And I thank Secretary Herman and Deputy Secretary Higgins for that.

The AARP has also agreed to help out. And we're reaching out to civilian and military retirees who did this work for government before. I will ask these older Americans to set aside their well-earned rest and help our nation to meet this challenge.

Second, businesses should exchange and pool information among themselves. It makes no sense for every firm to have to reinvent the digital wheel. Businesses should be able to benefit from the experiences of other firms in the same situation that have found solutions or identified new obstacles.

Today, too many businesses are understandably reluctant to share information, fearing legal complication. We have to take prudent steps to clear away any legal barriers to effective action. Earlier this month the Justice Department stated that competitors who merely share information on how to solve this problem are not in violation of the nation's anti-trust laws. We need to get that message out there loud and clear: no one should be afraid to help another company to deal with this challenge.

There is more we can do. This week I will propose good Samaritan legislation to guarantee that businesses which share information about their readiness with the public or with each other, and do it honestly and carefully, cannot be held liable for the exchange of that information if it turns out to be inaccurate. And here, too, time is of the essence.

Our third challenge to business is that you should take responsibility to accurately and fully tell your customers how you're doing and what you're doing. By letting customers know they are on top of the problem, businesses can help to maintain confidence and override overreaction. This is very important. It is important that we act and not be in denial; it is also very important that we avoid overreaction from people who hear, oh my goodness, this problem is out there. And so we have to do both things.

The proposed Good Samaritan law will give companies the confidence they need to ensure that they keep their customers informed. If ordinary citizens believe they're being told the full story, they'll be far less likely to act in ways that could themselves hurt our economy.

We can do more to help businesses reach these goals. Later this month our Council on the Year 2000 Conversion will launch a national campaign for year 2000 solutions, to promote partnerships between industry groups and government agencies, with the goal of sharing information about what actually works and to prod organizations at every level to get ready, making certain government services are not interrupted, minimizing disruption to commerce, encouraging businesses to share with each other and report honestly to customers, and above all, every business in America taking responsibility for being a part of the solution in the year 2000 conversion. These are the ways we, the American people, can be prepared to meet this challenge.

Now, no one will ever find every imbedded microchip, every line of code that needs to be rewritten. But if companies, agencies, and organizations are ready, if they understand the threat and have backup plans, then we will meet this challenge.

The millennium bug is a vivid and powerful reminder of the ways that we are growing ever more independent as we rise to the challenges of this new era. When our founding fathers urged us to form a more perfect union, I don't think they had this in mind, but they might be quite pleased. The powerful forces of change that have created unimagined abundance also bear within them, as is consistent with human nature, the possibilities of new and unexpected challenges.

But if we act properly, we won't look back on this as a headache, sort of the last failed challenge of the 20th century. It will be the first challenge of the 21st century successfully met. That is the American way, and together we can do it.

Thank you very much. (Applause.)

END 11:35 A.M. EDT

Mr. DESEVE. Mr. Koskinen, the Assistant to the President, has met with the United Nations. I believe that they're either in the middle or going to have a resolution in that arena to try to make their folks more aware as well.

But we can use your help, please. Mr. Davis is right. The administration—the buck stops here. But it doesn't mean that we can't forge a good awareness partnership with the Congress as well.

Mr. HORN. Well, we thank you for that. And we will be back with some more questions, but I'm going to yield Mr. Davis 13 minutes.

Mr. DAVIS. I just need a couple more minutes.

Mr. DeSeve, let me say one more thing. Mr. Kucinich brought up the election. If this thing fails, the elections in 2000, the voters will have their say, and we don't have to look very far. I think the administration is going to have to do some fast dancing if this doesn't go well.

We all have an interest in making it work, because they're probably going to take it out on whoever is there, anybody that's been adversely affected.

Let me ask a question. It seems, even after testing, systems still fail with some frequency, with some percentage. This is why contingency planning is so important. Let me start with Mr. McCabe, and we will go on.

Mr. MCCABE. Yes, sir. Mr. Davis, our state of practice and perfection of the software testing normally is abysmal; and with this particular problem, it's really scary. And one reason why systems fail after testing is testing is last in the phase, and it's usually—it usually runs out of money as cut. And that's particularly true when you have a fixed date like the year 2000.

I just want to come back to a couple of points I was trying to make before. It is such a broad problem. I'm taking a fairly singular view, and the reason is that I feel very strongly about—and just a couple of points.

Our published metrics about how you measure the stuff made it available to what used to be the National Bureau of Standards, now NIS, and also GAO. It is true that no particular kind of testing will guarantee success, but it's also true that systems are not being tested. The job is both bigger than what it seems, because the key things are not being tested, and smaller than what it seems, because often 95 percent of the testing is being wasted.

Now, another point I would like to make——

Mr. DAVIS. Can you elaborate on that?

Mr. MCCABE. Sure, the fact is, when you build or change a general system, you have to test all of it, all the permutations, all the interfaces, and so forth. It happens to be the case with the year 2000 that is date specific and the dates are only of the order of maybe 5 to 10 percent dense within the code. That means, when you change them, you have to test exactly that. Really what it means is you have to quantify and visualize where that testing is, and that's not particularly being done. So the mistake that is being made is to try to get rigorous testing at the unit or smaller level companies are trying to test all of the transactions, when, in fact, 95 percent of it is wasted and indeed the core testing is not being done.

Now my other colleagues have mentioned, for example, that there's no replacement for end-to-end testing. That's absolutely true. However, Mr. Davis, when the foundation isn't strong or effective, when it's particularly weak, what happens is, as your question alluded to, is you think you've done your testing and you're testing end to end and it doesn't work and you regress because the foundation was nowhere near where it should have been.

So this comes from our experience—I'm kind of in the trenches with this. We've seen a lot of systems, Federal and commercial systems, that have been claimed to be correctly tested, including the ones that the IG did.

Mr. DAVIS. Let me ask this, when fixed and tested systems are later truly tested, what percent failure are we getting?

Mr. MCCABE. We're getting very, very high percent failure, just normally.

Mr. DAVIS. Do you have any specific examples you can share with us?

Mr. MCCABE. There's statistics that something like with projects that are over $4 or $5 million, about 80 percent of them fail. An enormous failure rate with very, very high dollar projects.

Mr. DAVIS. In fact, you could test it and it can go perfectly and once you get into real life experiences, you can't test for every contingency. That's also a problem, isn't it?

Mr. MCCABE. That's also a problem. It happens in this particular case we have leverage, and the leverage is that the dates are not that dense. The dates are relatively infrequent, as of the order of maybe 5 or 10 percent. So the leverage one can use is to test specifically at that.

And look at it another way, sir. If you don't test those things, there's no hope that this stuff is going to work. So what it really comes down to is directed testing to be sure that that foundation is right and then build upon that.

Mr. DAVIS. How would you run a test on something like international trade?

Mr. MCCABE. The way you would run a test is: first find out within the software systems that perform where the dates are. And then, second—actually, you test before you change the code. Because the reason why you do that is you put errors in changing the code that you may or may not know if they were legacy errors. So you establish them on the tests you have, which ones are going to hit the dates, and then you exchange it and repeat the test on those dates. And a set of tests, that would consist of, Mr. Davis, among all the tests is perhaps about 10 percent.

Mr. DAVIS. Let me ask Dr. Grabow the same question. How do you test for international trade?

Mr. GRABOW. I would like to—I understand where Mr. McCabe is coming from in terms of a technologist, but as a businessman, which I am——

Mr. DAVIS. We've got all of these experts, and you can't agree on all of this stuff.

Mr. GRABOW. We agree very much. I agree with his principles and testing completely. However, when you look at a trade transaction, one individual trade transaction where a Chicago company is purchasing goods from China, in that one trade transaction there

are anywhere, as I mentioned earlier, 10 to 12 different organizations in both countries, at least, maybe even other countries.

So picture in your minds the globe, and you have two, a buyer and a seller, you have two port authorities, maybe a railroad, you have a couple of trucking companies, two banks, an insurance company, warehousing facilities, insurance companies, and I think I've covered the waterfront. But all of those participants are involved in the purchase and sale to get goods back to Chicago, IL.

The second part of this trade transaction is the sequential steps—the flow of paper, the purchase orders, the releases, the shipping documents, the money, the Customs inspections. All of this is done electronically.

Where I beg to differ a little bit is on how you cannot test a trade transaction——

Mr. DAVIS. You have the financing, all of those things?

Mr. GRABOW. All this stuff has to work—just picture in your mind's eye all of these different technologies, all these different companies trying to communicate back and forth, and if you start to have some system failures—it is impossible, as you look at the business transaction, to test it, and that's my point.

But from a businessman's point of view, that's why I'm very concerned about foreign trade. Foreign trade is 20 percent of our GDP. And what I'm saying, in two key elements, 20 percent of GDP in foreign trade and approximately 19 percent of the Federal Government, and if you come into the public sector, you're over to one third, and you've got half the economy that is at risk of this issue.

The other point that I'd like to stress very significantly is the timeline is not 18 months. In our research, we see system failures increasing substantially as this year comes.

Mr. DAVIS. You see them right now with transactions?

Mr. GRABOW. We see them right now and increasing substantially where they're going to be very visible. Our concern is that the American people be prepared.

Now one of the things they don't like are surprises, and what frustrates our participants, our investors, and others is the lack of focus. Because I still have people that I talk to that are, "knowledgeable," and they still don't think there's a problem. Yet all of us can sit in the room together today and agree that we're facing some very significant issues.

And so what frustrates me, as I sit here, is why can't we break through this little barrier? Why can't we take this to the people and tell them what we see?

Because the point I would see as a practitioner of technology and as a businessman, if you gave me all the systems that you're showing me in the Federal Government, 24 agencies, and you're trying to tell me they're going to be ready by sometime next year, I would challenge that. I don't mean to be argumentative, but——

Mr. DAVIS. You're talking about critical missions versus others, and I think we just keep running. I hear you.

Mr. GRABOW. Yes.

My other concern is the quarterly report that came out last quarter where you listed 15 of the agencies that reported out; 24 said they didn't know what an embedded system was or they didn't know if they had any problems.

Mr. DAVIS. That sounds like the agency where somebody said, well, it couldn't be that complicated. We're only doing 1900 in that case.

Mr. GRABOW. The problem that I see is we don't have a clear definition of what is year 2000, and all of this discussion today is—again, I come back to information processing. Let's talk about oil refineries. Let's talk about pipelines. Let's talk about——

General Motors came out and made a very clear statement, unequivocal, in Fortune Magazine in April 1997—excuse me, 1998, where Segenda indicated that they had catastrophic problems at 85 of their manufacturing plants around the world.

Now, let's look at the auto industry as a business. They have approximately 85,000 suppliers globally that take care of those plants. What we're saying, to have auto production continue not only does GM have to have all of their information systems and embedded systems working properly, but the entire network of vendors that support it with all the infrastructure has to be working properly. And as I'm looking at this issue and understanding the technology, to me that seems like a very, very difficult challenge.

And I love challenges, but I think it's also practical that we start to say, this isn't going to probably work that smoothly. So what do we need to do, how do we prepare the American people? Again, we're forecasting unemployment to start rising in 1999, and everybody is enjoying a great time right now.

Mr. DAVIS. We always are asking for specific anecdotes. And I did read about the company in England where their corned beef inventory showed 02 as the expiration date, and it was destroyed before they discovered it, because they thought it was 96 years old.

Do you have any specifics of where this is going on in—we know it's going on every day, but——

Mr. GRABOW. I've heard of it in drug manufacturing, for example; food processing which you brought up. In the case of powerplants where they have advanced the system date——

And what we haven't talked here yet today is how regulatory intervention is eventually going to cause some disruption also in the economy. By that I mean the 1 year plan is a 550 megawatt plan. They advanced the date, and within a few minutes it shut down because of the flue gas monitoring system right at the top of the stack.

If you can picture that tall stack, there's a monitoring system up there with a sensor and a circuit board and other equipment. It failed. So maybe somebody has to go up there and change that piece of equipment, maybe has to change a sensor or maybe you're fortunate where it's a simple——

Mr. DAVIS. If you fix that there could be another 50 things wrong?

Mr. GRABOW. Exactly, but the point is, when you come back to embedded system—and what I would encourage the committee to do some work on is the production side of embedded systems. It's far more difficult to remediate. It takes a longer time. And it's, in our view, going to have greater economic consequence.

Mr. DAVIS. Thank you.

Mr. MCCABE. Mr. Davis, just a comment. I think we're agreeing. The point Mr. Grabow was making when you modify system X, Y, Z, you have to integrate across and do the other testing.

The point I'm trying to get is system X doesn't work; system Y doesn't work; and system Z doesn't work. Until they work in some reasonable fashion when we do some reasonable testing, the integration testing is no doubt not going to work.

Just to add to all of this. I think DOD has done a number of good things, and there are some examples where it's being done well. One is STRICON within the Army. I think they got relatively—focused on the RACON of day testing and so forth, and they've done quite, quite well.

We always get in the defensive within the Government when, in a lot of cases, the work the committee leads is, in fact, exemplary.

Mr. DAVIS. We won't read about the success stories. We will read about the failures. That's the problem with this.

I yield back.

Mr. HORN. I thank the gentleman.

Let me ask a couple of questions.

In terms of the discussion we've heard here and the degree of pessimism, does that mean that the market has also discounted the year 2000 problem? Do you see particular industries where there seems to be a discounting of this, or are people more likely to wait till the end of 1999?

Do you want to just start down the line with Mr. Webster? Any thoughts on that?

Mr. WEBSTER. If you can explain what you mean by the market discounting the year 2000 problem? I mean, have they already taken into account, or are they simply ignoring it? I'm not sure I understand what you're asking.

Mr. HORN. Well, I'm just saying, do you already sense movements in the market based on the extent of computerization that, one, the industry might depend on, as opposed to another one, or their sensing of a failure to solve the problem? Is there any evidence of that at this point?

Mr. WEBSTER. I have seen no evidence of that actually.

Mr. HORN. OK. Mr. Simpson.

Mr. SIMPSON. I don't know if the window is there yet. There's a moving window of awareness. I don't think it has reached that. When it reaches that, certainly overnight everyone will panic and then you'll see some serious problems.

Mr. HORN. Mr. McCabe.

Mr. MCCABE. Yes, we have seen a couple of industries where, in fact, there are maybe four or five major competitors, and maybe four of them are not going to make it, which is typical, and one is. And everybody thinks about this as a negative investment—that is, it just makes us survive—when, in fact, what they're doing is inventorying all their systems, which you have to do, and figuring out the architecture of the system, changing them, remediating them, testing them and, again, getting them ready for client server, for interfaces and so forth.

The bottom line is, they will be surviving. The transactions will run. They will be in business in the year 2000 when, in fact, to a

certain degree, all of the competitors will not. So, in truth, they will be in better shape.

And they did some analysis, and it took so much money in terms of advertising and so forth that—by market share in normal times—and it turns out to fix the year 2K problem there's substantially less than that amount of money. So there's positive ways in which you can think of this.

Mr. HORN. Mr. Steinberg.

Mr. STEINBERG. I'd love to be more optimistic about it, but I don't think, if we're talking about awareness and the need for disclosure, that corporations have come to grips with it enough for the market to recognize that they have a discount to make. I think that stage will come 6 months to a year from now.

Mr. HORN. Well, you're saying it will come in 1998?

Mr. STEINBERG. Pardon?

Mr. HORN. It will come in 1998? A year ahead?

Mr. STEINBERG. I am not an economist by training, so that's just my wild guess, based on the amount of work that's being done to raise the awareness and forged disclosures. Because you can't have a market discounting something that they don't know about.

Mr. HORN. Well, people aren't stupid. They watch this stuff pretty carefully.

I remember in 1954 Professor Galbraith came down from Harvard and suggested to a congressional committee that they increase the margins. They were hardly nonexistent, up to 90 percent. The market fell $1 billion worth, and that was a real billion in those days. And Professor Galbraith got a postcard addressed to the Communist, Cambridge. Somehow the Post Office delivered it to Professor Galbraith. And he took some pride in that, and it was on his bulletin board for all of his class to see. Anyhow, that's 1954. We're a little more sophisticated, presumably, in 1998.

Mr. STEINBERG. Well, as an outsider to the market, I haven't seen any indication that it has gone down. Again, this is not——

Mr. HORN. It's interesting.

Mr. Grabow, any thoughts on that?

Mr. GRABOW. Yes, Mr. Chairman. There's actually three points I would like to make on your question.

The first is talking about the equity market. At this point, I do not believe that there is any indication going on with investors, a recognition of this problem. And it stems—and for a couple of reasons, one is, which the SEC acknowledged just a few days, even though they put out Staff Legal Opinion No. 5 some months ago, it hasn't been working well enough.

It goes back to my earlier comments that many corporations still don't have in their mind what the definition of year 2000 is. Although, they're trying to abide by Staff Legal Opinion No. 5, there's some confusion as to their actual disclosure.

And Ms. Unger, I believe, one of the SEC commissioners, spoke just a few days ago, and they're going to try to tighten up these standards.

So once more information does come out. I believe there will be a correction in the U.S. equity market; and what's going to happen, in our view, is a contraction of PE multiples. We're at this historic high over the last basically 40 years. And just in terms of the nor-

mal course of events, a correction would be healthy. But when you add in what's going on in Asia right now and then when you begin to look at the fact that there are declining corporate profits occurring, a natural correction is about, in our minds, to unfold.

And this is part of this scenario. When we come to a global economic recession, we're looking at Asia as kind of the precursor to this happening. And I might add that what's going on in Asia, the focus there right now is trying to,"make payroll." And the anecdotal and direct evidence that we're finding is not a lot of remediation occurring in some of those countries and so that brings further concern to us.

The second area that I would like to bring out, which was very important, is the credit markets, the fixed income markets, which get very little discussion but are very substantial in size and volume. What we see happening later this year and clearly in 1999 is that companies are going to be denied access to credit. We see credit rationing and potentially a credit crunch, somewhat like we saw in the 1980's when we had the real estate crisis, and that money is not going to be lent by financial institutions, by commercial banks, by finance companies and pension funds to those institutions that are not going far enough along in the process of compliance.

Would you want to lend money if you were the chairman of a financial institution if you didn't believe in their compliance program? And so what we're saying is that behavior is going to change in those financial institutions, and they're going to choose to invest in Government bonds as a safe harbor, much like they did in 1980.

And the other thing that we would be looking at is that, in the commercial banking industry, that most likely the Federal regulators—and this is my own speculation—but at some point will probably cause the financial institutions to have greater reserves required for those loans made by the banks to corporations that are not doing enough to protect those investments.

The last thing I would like to bring up, that I think is also important that comes right into the area of Government, that is in our due diligence. With many State and local governments, as well as our own Federal Government, a lot of our revenue is due to the high employment levels we have had and the high tax revenues and the high capital gains. This same concept has worked in States and cities and counties. Many of these governments are flushed with money, and what we see happening in the next 18 months or so, if you start to get a change in the economic conditions, is that their coffers will start to run dry or to slow up in terms of the ability to receive revenues from this aspect of the economy.

At the same time, they are going to be running into a position of having increased cost from social services, and they are going to be possibly in a pinch in terms of financing, depending on where they are in their overall capital program, and some States I have talked to are not far enough along in terms of actual spending, and if that becomes a problem and they are out trying to raise credit, out trying to raise financing when their credit quality is declining, it could be a significant issue on their ability to finance.

Mr. HORN. I won't subject the Government officials to this, unless you want to comment. What I do want, for one last question

on my part, and then back to Mr. Kucinich and Mr. Davis, and that is, if you have got to prioritize what must be done for sure, let's start talking about the power grid, be it electric or nuclear, solar or windmill or whatever it is, going into that system. Would that be No. 1 on your list, and if that isn't No. 1, because it seems to me everything is affected by that in terms of the economy running and the homeowners protection, and all the rest of it, if the grid is not No. 1, what should be, or are there two No. 1s?

Mr. DeSeve, any thoughts on that?

Mr. DESEVE. I don't know if there are two or three or four, Mr. Chairman. You certainly, in terms of the power grid, identified something we are extremely concerned about. I also would associate myself with Mr. Simpson's remarks on Telcom and the effects on international trade. I think those are the three things we spend the most anxiety on, and not the most time on necessarily, but the most anxiety on.

Mr. HORN. Dr. Stillman.

Ms. STILLMAN. There is no question that the power grid and telecommunications infrastructure are the base on which everything else rests. When you think of conducting a war, the first objective is to destroy the enemy's power and their telecommunications. They are the sine qua non, without which nothing. They are critical.

Mr. HORN. How about it, Mr. Grabow.

Mr. GRABOW. First thing is, I always want to be friendly to a lady, because if she is going to go to war, I want to be careful here. But I would agree. The one thing I would add is water. The basic infrastructure is very critical, along with water, and as I mentioned, the Government itself and its ability to function properly.

Mr. HORN. Do you agree with that, Mr. Steinberg?

Mr. STEINBERG. Well, I am from the frozen north, and as some of you may know, we had freezing rain last winter. I lived through it. It was a pain in the butt. You can't do very much without electricity and telecommunications. And in many cases, that also includes water because without the electricity, you don't have pumps flowing. There is nothing more important right now.

Mr. HORN. Mr. McCabe.

Mr. MCCABE. I don't have much to add. I think phones, water, electricity, and I live nearby, so air conditioning as well.

Mr. HORN. Well, if we give you power, you have to have an air conditioner you can turn on or off.

Mr. MCCABE. I am not sure, but the air-conditioners may not work.

Mr. HORN. Mr. Simpson.

Mr. SIMPSON. I would say power is the primary one. Telecommunications, there is always a backup. The problem we have with telecommunications, when you speak to them, they say we have backup generators. Backup generators are designed to run for 5 minutes or 5 hours. The city of Oakland learned, to its cost, the backup generators will not run for 24 hours and beyond. They fail. The fuel to power backup generators is in the ground, you can't get it out to refresh them because there is no electricity for the pumps. There is always another way another message can get through. Power, without it, everything goes.

Mr. HORN. OK. Mr. Webster.

Mr. WEBSTER. The only thing I would add to this is in our focus on power grid, per se, we have to look long and hard at the oil issue, oil production, shipping and so on because that can grind things to a halt very quickly as well, even if the power grid itself is working.

Mr. HORN. Did I call on you, Mr. McCabe?

Mr. MCCABE. Yes.

Mr. HORN. OK. I think we got everybody's answer on the record then. I will now yield 13 minutes to the gentleman from Ohio.

Mr. KUCINICH. I wanted to go back to some of these questions that deal with the power grid, in particular, focusing on nuclear power. Since so many of the safety features which exist on nuclear powerplants are programmable, and that is simply due to the watchful eye of the inspectors onsite, have any of the panel members who have looked at the power issue also looked at the implications for the safety of nuclear powerplants?

Mr. SIMPSON. The safety of the nuclear powerplants I don't think is a real major concern. The regulatory systems are very strong, they have a good oversight. If all else fails, they will fail safe, that isn't the problem. The problem is if they are not producing, the whole grid is gone. We rely, especially in the Northeast, on nuclear power, and if they go out for safety reasons and the lawyers are currently saying, hey, let's take them off line and bring them on slowly, if that happens, there will be a rolling blackout. So we need to test them well before the event and keep our fingers crossed. That is the one thing with 2000, we don't really know what is going to happen. We can have computer models, we can have predictions, we will not know until real time 2000 clicks over.

Mr. KUCINICH. Let's go, then, to real time 2000. What kind of readiness preparation does the Government have, starting on that day; what kind of task force or task forces do you have set up beginning on that day?

Mr. SIMPSON. Can I just address the communications one here? It concerns me an agency that is responsible for the foreign affairs of this Nation has got an F. The communications from embassies and even more so from consulates rely on the phone systems of that country. When the twist au pairs go out of the building, they are not on AT&T, they are not on Baby Bell, they are on the Botswana Power, Light and Ice Cream Co., or whatever the local one is. We need to have a plan B so that if there are any bangs on the ground or if Pakistan and India start playing games, we are alerted.

The last thing, as I said, the President needs to find out is that war has been declared in Pakistan and India from CNN. We have got to get this communications network around the world up and running and tested, the backup circuits tested, and the supplies to all nations, not just the United States, well before 2000.

Mr. KUCINICH. I can readily accept the logic of that as common sense. I guess maybe Mr. DeSeve could answer on behalf of OMB. Let's go right to the year 2000. We are there. What will you have in place, as of that date, for problems that come up? Here we are, January 1, what do you have ready, do you have teams of people

ready to go into mission critical, as well as other areas of the economy?

Mr. DESEVE. We are working in two directions simultaneously. Direction one is with the Federal Government's own responsibilities. We will have a series of contingency plans for what we call business operations, including the operations of the Federal Emergency Management Agency and others, to be able to respond as necessary to any situations that might occur.

Mr. KUCINICH. OK. Let's stop right there. Let's talk about the Federal Emergency Management. What will their role be beginning on January 1, the year 2000?

Mr. DESEVE. They will have the same role they have had up until now; that is, first, education of the State emergency offices as to what the problems might or might not be. I can't speculate that there would or wouldn't be any, but the first role is always to work in counterpart with their State emergency offices.

Second, to coordinate the Federal resources. They coordinate with the folks at SBA on loans and the folks at HUD on housing and so on, to be able to be sure. They coordinate, also, with voluntary agencies. So they bring to the area, to whatever area whatever, supplies that are needed. That is just an example.

Mr. KUCINICH. Will there be, for example, disaster relief programs for Y2K?

Mr. DESEVE. You have taken me to a level of speculation in which I really can't engage on a wholesale basis.

Mr. KUCINICH. But, wait a minute. If I may, a lot of this is speculative, but unless we agree that everyone is going to be Y2K compliant in the year 2000, you know, we don't have to be too concerned. But since we have an understanding that there will be areas that will not be Y2K compliant, we are not really sure which ones those are, we have a role for the Federal Emergency Management. How broad will their powers be? I mean, it would be nice for us to know. Are they being prepared to take a leadership role in direction of the manifest problems that could occur during the transition at the year 2000?

Mr. DESEVE. Right. FEMA again is 1 of the 30 sectors we work with, and they have been very responsive, as they have been over the course of the last 5 years, in preparing themselves for dealing with each of these eventualities. I don't have the specific plan for that in front of me today, but they have been very much focused and have worked very closely with the President's Year 2000 Conversion Council; they are an active member of that Council.

Mr. KUCINICH. I understand in your presentation, you are talking about proceeding simultaneously on a number of tracks. I mean, one, would you say, obviously, we are talking about deterrence, which is prevention, preparation; all those things are in one category. The other part is where do you get to 2000. We don't have a Pollyanna notion that somehow there won't be any problems, but if we prepare for that particular eventuality, as I know so much of the work that Mr. Horn has been involved in points to that, it enables us to quell the panic, which we certainly don't want to happen, because it's likely that panic could happen. I think it is very important for the Federal Emergency Management, at some point, Mr. Chairman, to come before this committee and talk specifically

about what its role will be starting from the year 2000 and coordinating the direction, perhaps, of specialized teams to help go in and grapple with the difficulties that an industry might be having or a major company or concern or State and local government, because this is a different kind of emergency. If we knew, for example, that weather reports portended, you know, serious storms, we would get ready. If, you know, like in the movie Deep Impact, even though it's one of those fables that is nice to watch because you don't think it will ever happen, implied a degree of preparation that people could make, knowing that this society could still survive, but knowing that there would have to be certain types of extraordinary relief.

I mean, Federal Emergency Management has been primarily involved in dealing with weather-related disasters, I think for the most part, but now this is a technologically anchored disaster, so that could occur. Not will, could. It's like a weather report.

Mr. DESEVE. I think the other side relates to something Mr. Grabow was talking about; that is, in each of the individual sectors, whether it's the Energy Department or the FCC or the FTC, the primary regulator, the primary oversight is provided by a Federal agency who worries about those things, and getting it right. The SEC causing there to be full disclosure in 10Ks and 10Qs, FERC and the Nuclear Regulatory Commission having the kind of oversight that gives Mr. Simpson confidence in nuclear plants, are our first line of defense, so they will be out there in addition to anything else that goes on.

Mr. KUCINICH. Yes, Mr. Simpson.

Mr. SIMPSON. If I can just make one point. On telecommunications, this is in the written statement, not in the oral one, is the third one in 1999, 2000, for our space assets. The satellites have to go through the micro meteorite storm, which if you look on NASA's web site, you will see predicted. That may knock out some satellites. It may knock out weather satellites, it may knock out communication satellites, it may knock out nothing. Later on in the year, around about November, we have solar max 23, with the key peaks of it on history. That may knock out satellites, it may knock out power grids, we don't know. We are going to wait and see what happens. So we may enter 2000 from a communications point of view with depleted space assets, less communications capability than we are at now.

One of the things in contingency planning for FEMA and all these other agencies, Defense and State, they have to look at the "what if" scenarios. If the meteorite storm and the solar max take out the backup satellites, what level of communications do you need to go to? Galaxy IV, one satellite, which we knew was a little bit faulty, went off. Well prepared, it took how many days to get it back on again. What happens if all the satellites or some of the satellites go down? We need to look at that as well. So year 2000, as far as communications are concerned, especially on the global scale, weather satellites as well, you may have a depleted level of service from space.

Mr. KUCINICH. Thank you, Mr. Chairman.

Mr. HORN. If the gentleman will yield. His pursuit of the question is a very excellent one. I just happened to remember here that

in May 22, 1998, on a slow news day, the White House issued Presidential Directives 62 and 63, which set up, looking at various aspects of our infrastructure, and with infrastructure officers, chief infrastructure assurance officers in various departments, the abbreviation for that is C-I-A-O, or CIAO. Which, I guess, is a doomy gloomy part that might just mean good-bye, so we are not sure what that means. But if we look at the White House like the CIA looked at the Kremlin, we might read something into this. Anyhow, it's vulnerability analysis, remedial plans, warnings response, et cetera. Along with the gentleman from Ohio's point, I would say it's as one of our contingency plans that we just say sorry, Bulemia Air, you can't use U.S. air space because you are not 2000 conformant. What do you suggest, Mr. DeSeve, is there any meaning in this that relates to what we are talking about?

Mr. DESEVE. I think the meaning is very closely related. I think the Commission on Critical Infrastructure, from which those reports were drawn, anticipated things like the year 2000, as well as other potential threats, whether they be technological or threats performed by enemies. So I think that putting that in place, the critical infrastructure assessment in place, was a step toward Mr. Kucinich's problem in 2000.

Mr. HORN. Very good. Any other questions?

Mr. KUCINICH. No. I yield back.

Mr. HORN. OK. Well, we thank you all for coming. It's been a very enlightening dialog and I appreciate the exchange.

I might add that last week, the Speaker did announce that this committee, along with Mrs. Morella's committee, would be the equivalent of the Bennett committee in the Senate, and work together on that which we have already worked together. He designated me as chairman and Mrs. Morella as cochairwoman.

Let me thank the staff now for the fine job they did in putting this panel together. J. Russell George, the staff director and chief counsel, in back of me, to my left, your right. Bob Alloway, professional staff member, that is particularly involved in this hearing. Matthew Ebert, our clerk. Mason Alinger, staff assistant. Betsy Damus, Mark Urciuolo and David Graff, interns. And for the minority, we have Faith Weiss, the counsel for the minority. Brian Cohen, Julie Moses, professional staff members. Earley Green, minority staff assistant, and our court reporters have been Cindy Sebo and Katrina Wright.

With that, I adjourn this hearing. Thank you.

[Whereupon, at 3:21 p.m., the subcommittee was adjourned, subject to the call of the Chair.]

○