AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

THE YEAR 2000 PROBLEM: STATUS REPORT ON THE FEDERAL, STATE, LOCAL, AND FOREIGN GOVERNMENTS

JOINT HEARING

BEFORE THE

COMMITTEE ON GOVERNMENT REFORM

AND THE

COMMITTEE ON SCIENCE

HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

FIRST SESSION

JANUARY 20, 1999

Committee on Government Reform and Oversight

Serial No. 106–40

Committee on Science

Serial No. 106–42

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

Available via the World Wide Web: http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

60–491 CC WASHINGTON : 1999

COMMITTEE ON GOVERNMENT REFORM

DAN BURTON, Indiana, *Chairman*

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

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
PATSY T. MINK, Hawaii
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, Washington, DC
CHAKA FATTAH, Pennsylvania
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
ROD R. BLAGOJEVICH, Illinois
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
JIM TURNER, Texas
THOMAS H. ALLEN, Maine
HAROLD E. FORD, JR., Tennessee

BERNARD SANDERS, Vermont (Independent)

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

COMMITTEE ON SCIENCE

HON. F. JAMES SENSENBRENNER, JR., (R–Wisconsin), *Chairman*

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

GEORGE E. BROWN, JR., California, RMM**
RALPH M. HALL, Texas
BART GORDON, Tennessee
JERRY F. COSTELLO, Illinois
TIM ROEMER, Indiana
JAMES A. BARCIA, Michigan
EDDIE BERNICE JOHNSON, Texas
LYNN C. WOOLSEY, California
ALCEE L. HASTINGS, Florida
LYNN N. RIVERS, Michigan
ZOE LOFGREN, California
MICHAEL F. DOYLE, Pennsylvania
SHEILA JACKSON-LEE, Texas
DEBBIE STABENOW, Michigan
BOB ETHERIDGE, North Carolina
NICK LAMPSON, Texas
JOHN B. LARSON, Connecticut
MARK UDALL, Colorado
DAVID WU, Oregon
ANTHONY D. WEINER, New York
MICHAEL E. CAPUANO, Massachusetts
VACANCY
VACANCY

CONTENTS

	Page
Hearing held on January 20, 1999	1
Statement of:	
Gershwin, Lawrence K., Ph.D., National Intelligence Officer for Science, Accompanied by Norman Green, Deputy National Intelligence Officer for Science and Technology, National Intelligence Council; Michael Harrington, Ph.D., principal technical staff, MITRE Corp.; Mary Walsh, Year 2000 Issues Manager, Directorate of Intelligence, Central Intelligence Agency; and Joel Willemssen, Director of Civil Agencies Information Systems, Accounting and Information Management Division, General Accounting Office	55
Koskinen, John, chairman, President's Council on the Year 2000 Conversion	15
Letters, statements, etc., submitted for the record by:	
Gershwin, Lawrence K., Ph.D., National Intelligence Officer for Science:	
Information concerning international litigation	115
Information concerning reactors	117
Prepared statement of	59
Horn, Hon. Stephen, a Representative in Congress from the State of California, prepared statement of	4
Koskinen, John, chairman, President's Council on the Year 2000 Conversion:	
Information concerning the Senior Advisors Group	17
Prepared statement of	22
Morella, Hon. Constance A., a Representative in Congress from the State of Maryland, prepared statement of	8
Ose, Hon. Doug, a Representative in Congress from the State of California, prepared statement of	14
Willemssen, Joel, Director of Civil Agencies Information Systems, Accounting and Information Management Division, General Accounting Office, prepared statement of	72

THE YEAR 2000 PROBLEM: STATUS REPORT ON THE FEDERAL, STATE, LOCAL, AND FOREIGN GOVERNMENTS

WEDNESDAY, JANUARY 20, 1999

HOUSE OF REPRESENTATIVES, COMMITTEE ON GOVERNMENT REFORM, JOINT WITH THE COMMITTEE ON SCIENCE,

Washington, DC.

The committees met, pursuant to notice, at 11:15 a.m., in room 2154, Rayburn House Office Building, Hon. Dan Burton (chairman of the Committee on Government Reform) presiding.

Present from the Subcommittee on Government Management, Information, and Technology of the Committee on Government Reform: Representatives Horn, Biggert, Ose, Miller, Maloney, Norton, and Turner.

Present from the Subcommittee on Technology of the Committee on Science: Representatives Morella, Gutknecht, and Jackson Lee.

Staff present from the Subcommittee on Government Management, Information, and Technology: J. Russell George, staff director and chief counsel; Matt Ryan, senior policy director; Bonnie Heald, director of information and professional staff member; Matthew Ebert, clerk; Mason Alinger, staff assistant; Paul Wicker and Kacey Baker, interns; Faith Weiss, minority professional staff member, Committee on Government Reform; and Earley Green, minority staff assistant, Committee on Government Reform.

Staff present from the Subcommittee on Technology: Richard Russell, staff director; Ben Wu, professional staff member; and Joe Sullivan, clerk.

Mr. HORN. A quorum being present, the joint hearing of the Committee on Government Reform and the Committee on Science will come to order. We are here to receive a status report on the effort to overcome the so-called "Millennium Bug," Y2K, year 2000. Whatever you want to call it, it has got the same problem. During today's hearing, administration officials will report on the efforts of the government at the Federal, State and local levels, as well as at the international community to remedy the year 2000 problem.

The year 2000 problem is the result of decisions made in the 1960's and the 1970's when many computer systems were developed. At that time, computers had limited storage capacity. In an effort to conserve memory, programmers designated the year by the two digits; in other words, instead of 1967, they put in a 6 and a 7.

Now, until recently that worked. However, when confronted by the zero-zero of the year 2000, these computer systems and microchips may not know if the year 2000 is up or we are back to the year 1900.

This confusion could result in the transmission of corrupted data, computer malfunctions, system breakdowns.

There are only 345 days left to assure the public that the computer systems which are critical to our lives and getting the job done, whether in business or in government, are year 2000 compliant. Unfortunately, even today, many private organizations and governmental entities are only beginning to recognize the potential impact of this problem. Some are just starting to fix their system. Some are leaving little, if any, time for one of the most important aspects of the remediation effort, which is adequate testing.

The problem is real; the consequences are serious; and the deadline is unmovable.

The House Subcommittee on Government Management, Information, and Technology, which I chair, has focused on the potential problem since early 1996. In April of that year we conducted the first congressional hearing. In July 1996, the subcommittee issued its first report card grading the 24 major Federal agencies on the status of their efforts to address the year 2000 problem.

Since then, the Subcommittee on Government Management, Information, and Technology along with Congresswoman Morella's Subcommittee on Technology of the Committee on Science has held numerous hearings, both in Washington and across the country, on Y2K.

On November 23, 1998, the Government Management Subcommittee issued its sixth report assessing the executive branch's year 2000 status. Unfortunately, the overall grade received was a "D." We hope that changes. Most Federal departments and independent agencies have responded much too slowly to this problem.

However, there are two notable exceptions: the Small Business Administration and, as the President again noted in his State of the Union Address last night, the Social Security Administration. Both agencies report that their mission-critical systems are 100 percent year 2000 compliant.

It is noteworthy that the Social Security Administration spent 10 years achieving that goal. Even with that effort, the agency has yet to perform comprehensive end-to-end testing of its system. Although Social Security calculates benefit payments, it relies on the Treasury Department and the banking system to distribute them.

No Federal entity is an island and no Federal entity can be complacent, regardless of its Y2K status, until its partner organizations are also adequately prepared for the new millennium.

I also remain deeply concerned about the Department of Defense. The Department reported last week that it was making great progress on the year 2000 problem, despite the "D-minus" it earned on the subcommittee's recent report card. I look forward to today's testimony which will allow for elaboration on the Department of Defense's progress.

Much of our focus has been and will remain on the Federal Government's year 2000 readiness. Mrs. Morella's subcommittee will go beyond that into many of the private areas in this country. But

Federal agencies do share information with State, local and international governmental agencies as well as many organizations in the private sector.

We are unsure of the consequences on Y2K compliant Federal systems if this shared information is corrupted by a noncompliant system.

On December 11, 1998, the United Nations held its first conference on the international ramifications of the year 2000 problem. Over 120 nations sent representatives to discuss their countries' approach to the problem. According to U.N. officials, many nations had not started their efforts until this conference was announced.

In today's hearing we will receive testimony on these and other important Y2K issues from three key witnesses. First, John Koskinen, chairman of the President's Council on the Year 2000 Conversion, and Assistant to the President, will present the status of public and private sector efforts to address the year 2000 problem. He will be followed by Dr. Lawrence K. Gershwin, National Intelligence Officer for Science and Technology at the National Intelligence Council, who will report on the status of foreign efforts to deal with the Y2K problem.

We are unsure of the consequences which exist abroad and one of our perennial expert witnesses will be finally Mr. Joel Willemssen, Director of Civil Agencies Information Systems at the General Accounting Office, and he will provide the General Accounting Office's assessment of the readiness of key public infrastructure and economic sectors.

So we welcome all of these expert individuals, and we particularly are delighted to see Mr. Koskinen, who has brought a lot of order to this effort within the executive branch since he assumed the problem in February 1998.

I now yield to the chair of the Subcommittee on Technology of the Committee on Science, and the co-chair of this task force, Mrs. Morella.

[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

Congressman Horn - Opening Statement
"The Year 2000 Problem: Status Report on the Federal, State, Local and Foreign Governments"
January 20, 1998

A quorum being present, the joint hearing of the Committee on Government Reform and the Committee on Science will come to order.

We are here to receive a status report on the effort to overcome the "Millennium Bug." During today's hearing, Administration officials will report on the efforts of government at the Federal, State, and local levels, as well as those in the international community, to remedy the Year 2000 problem.

The Year 2000 - or Y2K – problem is the result of decisions made in the 1960s and 1970s, when many computer systems were developed. At that time, computers had limited storage capacity. In an effort to conserve memory, programmers designated the year by using two digits instead of four. For example, the year 1967 was represented by the digits "6 and 7."

Until recently, the method worked. However, when confronted by the zero-zero ("00") of the year 2000, these computer systems and microchips may not know if the year is 2000 or the year 1900.

This confusion could result in the transmission of corrupted data, computer malfunctions, or system breakdowns.

There are only 345 days left to reassure the public that computer systems, which are critical to our lives, are Year 2000 compliant. Unfortunately, even today, many private organizations and governmental entities are only beginning to recognize the potential impact of this problem. Some are just starting to fix their systems, leaving little, if any, time for one of the most important aspects of the remediation effort – adequate testing.

The problem is real; the consequences, serious; and the deadline, unmoveable.

The House Subcommittee on Government Management, Information and Technology, which I chair, has focused on the potential problem since early 1996. In April of that year we conducted the first Congressional hearing on the problem. In July 1996, the subcommittee issued its first report card grading the 24 major Federal agencies on the status of their efforts to address the Year 2000 problem.

Since then, the Subcommittee on Government Management, Information and Technology along with Chairwoman Morella's Subcommittee on Technology of the Committee on Science has held numerous hearings, both in Washington and across the country, on Y2K.

On November 23, 1998, the Government Management subcommittee issued its sixth report card assessing the Executive Branch's Year 2000 status. Unfortunately, the overall grade received was a "D." Most Federal departments and independent agencies have responded much too slowly to the problem.

There are, however, two notable exceptions: the Small Business Administration and, as the President again noted in his State of the Union Address last night, the Social Security Administration. Both agencies report that their mission-critical systems are 100 percent Year 2000 compliant.

It is noteworthy, that the Social Security Administration spent 10 years achieving that goal. Even with that effort, the agency has yet to perform comprehensive end-to-end testing of its system. Although Social Security calculates benefit payments, it relies on the Treasury Department and the banking system to distribute them. c

No Federal entity is an island. And no Federal entity can be complacent – regardless of its Y2K status – until its partner organizations are also adequately prepared for the new millennium.

I also remain deeply concerned about the Department of Defense. The department reported last week that it was making great progress on the Year 2000 problem, despite the "D-minus" it earned on the subcommittee's most recent report card. I look forward to today's testimony, which will allow for elaboration on the department's progress.

Much of our focus has been, and will remain, on the Federal government's Year 2000 readiness. But Federal agencies share information with State, local and international government agencies, as well as many organizations in the private sector.

We are unsure of the consequences on Y2K compliant Federal systems if this shared information is corrupted by a non-compliant system.

On December 11, 1998, the United Nations held its first conference on the international ramifications of the Year 2000 problem. More than 120 nations sent representatives to discuss their countries' approach to the problem. According to U.N. officials, many nations had not started their Y2K fixes until the conference was announced.

At today's hearing we will receive testimony on these and other important Y2K issues from three key witnesses. First, John Koskinen, Chairman of the President's Council on the Year 2000 Conversion, will present the status of public- and private-sector efforts to address the Year 2000 problem. He will be followed by Dr. Lawrence K. Gershwin, National Intelligence Officer for Science and Technology at the National Intelligence Council, who will report on the status of foreign efforts to deal with the Y2K problem.

Finally, Joel Willemssen, Director of Civil Agencies Information Systems at the General Accounting Office, will provide GAO's assessment of the readiness of key public infrastructure and economic sectors.

We welcome today's witnesses and look forward to their testimony.

Mrs. MORELLA. Thank you, Mr. Chairman and co-chair of the task force. I am pleased to welcome everyone to the latest in a series of ongoing year 2000 hearings held jointly with the Science Committee's Technology Subcommittee, that I chair, and the Government Management, Information, and Technology's Subcommittee chaired by my distinguished colleague from California, Congressman Horn.

It was, as you probably all know, well over 2½ years ago when our two subcommittees, which last Congress was designated by the Speaker as the House Y2K Task Force, first began joint hearings on the year 2000 computer problem, and that was back in the 104th Congress.

In the past, our oversight activities and legislative initiatives have pushed for the creation of a national Y2K strategy, greater governmental management, legal protection for Y2K information that is exchanged in good faith within industry, and the establishment of a high-level senior administration official to lead our Nation's Y2K efforts.

Now, as we begin the 106th Congress, facing just 345 days before the immovable January 1, 2000 deadline, there is a greater sense of urgency to ensure that our Nation's public and private sectors will be ready for the beginning of the new millennium.

It is clear that we cannot move forward to meet the priorities and challenges of the next century if our Nation's computers are moving backward.

We intend to vigilantly continue our congressional oversight responsibilities, press wayward Federal agencies that are behind schedule, and work collaboratively with the administration on industry initiatives so that we can provide the American public with full confidence that our Nation will not suffer from any lasting catastrophic Y2K failures.

Earlier this month, the bipartisan chairs of the House Y2K Task Force wrote the President urging him to use his bully pulpit and to personally play a significant role in leading this effort. We asked the President to use his State of the Union Address to emphasize the importance of fixing the problem in order to ensure that our Nation will take direct, effective, and timely action.

And that is why I was frankly delighted when the President said last night that we need every State and local government, every business, large and small, to work to make sure that this Y2K computer bug will be remembered as the last headache of the 20th century and not the first crisis of the 21st.

It seems appropriate, then, that we continue our Y2K hearings by reviewing today the Y2K impact on State, local and foreign governments, and we have before us today a very strong panel, and I am looking forward to hearing their testimony.

I want to welcome back to our subcommittees the chair of the Year 2000 Conversion Council, John Koskinen, who has accomplished a great deal since he was named the Y2K Czar less than a year ago.

I also want to welcome back Joel Willemssen from the General Accounting Office, who has worked diligently and kept us informed since we began our Y2K efforts.

I am especially interested in the issue of how American industry in this global marketplace may be affected by the year 2000 efforts, or the lack thereof, of our international trading partners.

I am deeply troubled by the potential for Y2K disasters in a number of foreign countries. I am concerned that any potential Y2K economic and social instability across the globe will ripple through to the United States, so I very much anticipate the testimony of both the National Intelligence Council and the Central Intelligence Agency and their declassified assessment of the status of year 2000 efforts among foreign governments.

I have looked at the testimony. It does indicate that we do have some major international problems. And, frankly, I just returned yesterday from Korea, Indonesia, Hong Kong, and Tokyo, and in all instances I mentioned the year 2000 computer problem and asked what was being done. There were times when eyes glazed over and times when they said, "Oh it's being taken care of." There were times when they didn't understand what it was, and then I got an honest appraisal in Hong Kong where they said that it was definitely going to affect the economy.

The economy. Indonesia is sort of a basket case. Korea is trying, but not very well. And members of the Japanese Diet didn't even know what Y2K was. So they promised they would come up with a resolution. That is just a sampling of the immensity of the problem, particularly because of the interoperability and connectiveness.

So we know the end of the millennium knows no international boundaries and, indeed, Y2K is a global problem and as such it requires global coordination. America can lead the way on Y2K but we must make sure the rest of the world follows.

So, Mr. Chairman, I yield back. I did want to mention that we do have—and maybe they will have an opportunity to say something—Judy Biggert, who is a new member, who is here and I think is going to be on the Science Committee. We have not totally organized yet. And Gary Miller, who is also going to be on the Science Committee. I welcome them. And Doug Ose, who I believe is going to be on the Government Reform Committee.

I yield back, Mr. Chairman.

[The prepared statement of Hon. Constance A. Morella follows:]

Opening Statement of
Congresswoman Connie Morella
Chair, Technology Subcommittee
House Science Committee

Oversight Hearing
on the Year 2000 Problem
Wednesday, January 20, 1999
Room 2154, Rayburn House Office Building

I am pleased to welcome everyone to the latest in a series of on-going Year 2000 hearings held jointly by the Science Committee's Technology Subcommittee, that I chair, and the Government Management, Information, and Technology Subcommittee, chaired by my distinguished colleague from California, Congressman Steve Horn.

It was well over two and a half years ago when our two subcommittees, which last Congress was designated by the Speaker as the House Y2K Task Force, first began joint hearings on the Year 2000 computer problem way back in the 104th Congress.

In the past, our oversight activities and legislative initiatives have pushed for the creation of a national Y2K strategy, greater governmental management, legal protection for Y2K information exchanged in good faith within industry, and the establishment of a high level senior Administration official to lead our nation's Y2K efforts.

Now, as we begin the 106th Congress, facing just 345 days before the immovable January 1, 2000 deadline, there is a greater sense of urgency to ensure that our nation's public and private sectors will be ready for the beginning of the new millennium.

It is clear that we cannot move forward to meet the priorities and challenges of the next century if our nation's computers are moving backward.

We intend to vigilantly continue our Congressional oversight responsibilities, press wayward Federal agencies that are behind schedule, and work collaboratively with the Administration on industry initiatives so that we can provide the American people with full confidence that our nation will not suffer from any lasting, catastrophic Y2K failures.

Earlier this month, the bipartisan chairs of the House Y2K Task Force wrote the President urging him to use his bully pulpit and personally play a significant role in leading this effort.

We asked the President to use his State of the Union address to emphasize the importance of fixing the problem in order to ensure that our nation will take direct, effective, and timely action.

That is why I was delighted when the President said last night that we need every state and local government, every business large and small to work to make sure that this Y2K computer bug will be remembered as the last headache of the 20th Century, not the first crisis of the 21st.

It seems appropriate then that we continue our Y2K hearings by reviewing today the Y2K impact of state, local, and foreign governments.

We have with us today a very strong panel and I am looking forward to hearing their testimony.

I would like to welcome back to our subcommittees, the Chair of the Year 2000 Conversion Council, John Koskinen, who has accomplished a great deal since he was named as the Y2K Czar less than a year ago.

I would also welcome back Joel Willemsen from the General Accounting Office, who has worked diligently with Congress since we began our Y2K efforts.

I am especially interested in the issue of how American industry in this global marketplace may be affected by the Year 2000 efforts – or lack thereof – of our international trading partners.

I am deeply troubled by the potential for Y2K disasters in a number of foreign countries.

I am concerned that any potential Y2K economic and social instability across the globe will ripple through to the United States, so I very much anticipate the testimony of both the National Intelligence Council and the Central Intelligence Agency and their declassified assessment of the status of Year 2000 efforts among foreign governments.

The end of the millennium knows no international boundaries.

Indeed, Y2K is a global problem, and as such, it requires global coordination.

America can lead the way on Y2K, but we must make sure that the rest of the world follows.

Mr. HORN. I thank you for introducing those three fine individuals. They are all coming into Congress for the first time, and we are delighted to have them because they bring to this committee and your subcommittee a very strong background in organization and management and caring about some of these problems. So we welcome them all.

Now we have a new ranking member, I am delighted to say, who we have worked with before on the full committee, and that is Jim Turner of Texas. Mr. Turner, would you want to make some opening remarks?

Mr. TURNER. Thank you, Mr. Chairman. First I want to thank you and Chairwoman Morella for your leadership in the technological issues that are facing us in this country, and I am honored to be the ranking member of your subcommittee, Mr. Chairman. You have always been known to have one of the hardest-working subcommittees in the Congress, and I look forward to that challenge. You are also noted for running your committee in a very bipartisan way, which we on this side of the aisle very much appreciate.

Today we are here, of course, to discuss the status of both domestic and international efforts to fix the year 2000 computer problem, commonly known as Y2K, which occurs when computer systems or microchips fail to recognize a four-digit date code.

We have heard from people who warned that Y2K will cause a global financial crisis. On the other hand, we also know that 13 stock exchanges and 29 major brokerage firms have finished extensive Y2K repairs and turned their computers forward to the year 2000 in recent preliminary tests of their system. Fortunately, only 1 percent of stock trades in the tests were affected by computer problems.

We also know that in Maryland, Montgomery County has recently simulated the century date change in a test of its traffic, telecommunication and emergency response systems, all of which functioned properly.

It is important to recognize that in both of these examples it took many months of testing, repair, and preparation and hundreds of thousands of dollars to be successful. These examples point out, as well as many others we could cite, that early preparation, concerted efforts and testing are the answer to the Y2K problem.

Although no one knows for sure what will happen on January 1, 2000, it is important for all of us to try to separate fact from fiction, reality from media hype, and encourage rationality rather than hysteria. Hopefully, preparations will keep disruptions to a minimum and public health and safety and the environment will not be put at risk. Rumors, false fears, and Internet chat can, in fact, change imagined problems into very real ones.

The government and private sector entities that prepare adequately likely will make it through this next year without serious disruptions in their operations and in their activities. The Federal Government, under the leadership of Mr. Koskinen, has been working hard to make sure that it is ready for the date change. Last night President Clinton reassured our senior citizens that Social Security checks and direct deposits will not be disrupted. The Federal Government needs to keep pushing to assure that no Federal

programs are negatively affected by the Y2K problem, particularly those Federal benefit programs that are administered by the States.

We have the mechanisms in place now to track the Federal Government's progress on Y2K and provide the necessary oversight. However, many other governmental entities and private sector industries do not fall within the Federal Government's purview and are at greater risk of failure than are the Federal computer systems. Unfortunately, we are beginning to hear that small and medium-sized companies, and even State and local governments, may not be preparing adequately for Y2K.

We have very little information on international preparations for the date change, and from what we know so far, there appear to be serious problems in many foreign countries, and in particular, the lesser-developed countries. China and Russia may be especially hard hit. International shipping, transportation, telecommunications and financial sectors may be particularly vulnerable to the Y2K problem. Because of the global nature of our modern economy, the United States may be adversely affected by their failure to prepare.

I would like to thank Mr. Koskinen for his leadership and all of our witnesses today for providing us with the benefit of their knowledge on this subject. Working together, I am confident that we will be able to meet the challenge of Y2K. Thank you, Mr. Chairman.

Mr. HORN. I thank the gentleman very much for those constructive comments.

Mrs. Morella has one more point.

Mrs. MORELLA. I wanted to thank Mr. Turner for pointing out the extraordinary work in Montgomery County, MD, which I happen to represent. Thank you.

Mr. HORN. Any comments from our new members or any opening remarks? Mr. Ose.

Mr. OSE. I have no idea what I am doing, Mr. Chairman. I am afraid to say the wrong thing and, apparently, the phrase I want to use is, I yield back my time.

[The prepared statement of Hon. Doug Ose follows:]

DOUG OSE
3D DISTRICT, CALIFORNIA

Congress of the United States
House of Representatives
Washington, DC 20515–0503

January 20, 1999

Statement of Representative Doug Ose
Government Reform Committee Joint Hearing on
Oversight of the Y2K Problem: Status of Federal, State, Local and Foreign Governments

Mr. Chairman, thank you for conducting this hearing today on oversight by federal, state, local and foreign governments of the Year 2000 problem. It is an honor for me to serve on this Committee, and I look forward to addressing this issue at the full and subcommittee level this year.

I am interested in hearing from our witnesses this morning, especially on the issue of Y2K compliance by foreign nations. My biggest concern is the state of nuclear weapons systems in foreign countries.

In a cover story in Time magazine this past week, it was revealed that these systems, including those in Russia, are computer dependent. What is the state of preparedness in these countries? Could a lack of preparedness lead to the accidental launch of a nuclear missile?

In addition, I understand that there have been a couple of hearings on the issue of liability and the need to assess the potential risks of liability for businesses and government agencies for failing to provide compliance services.

While this might be outside the scope of this hearing, I would be interested in hearing from Mr. Koskinen on the issue of insurance exposures to Y2K liability to government agencies and in the private sector. For example, if a Wall Street firm hires a consulting company to bring them into compliance, and on January 1, 2000, that firm is still not compliant, to what extent is the company held liable? Would there be a need for a cap on punitive and economic recovery for this liability?

These are some of the issues and questions I look forward to our witnesses addressing at this hearing.

Once again, Mr. Chairman, thank you for holding this hearing. I look forward to hearing the testimony of the witnesses on this important issue, and I yield back the balance of my time.

PRINTED ON RECYCLED PAPER

Mr. HORN. Mr. Miller, any comments?

Mr. MILLER. Yes, Mr. Chairman, I am honored to be here. I thank you for holding these hearings. I also appreciate the focus we are making on the problem we are going to deal with in the future, and I am looking forward to being an integral part of this committee.

Mr. HORN. Thank you. Mrs. Biggert, any comments to make?

Mrs. BIGGERT. Thank you, Mr. Chairman. I am also very happy to be here and am honored to be on this committee. I have served in the Illinois Legislature and was the sponsor of the Y2K Task Force in Illinois, so this is an opportunity for me to broaden my horizons to the national and the global issues that concern this. So I am very happy to have the opportunity to participate.

Mr. HORN. Well, We are glad to have you here, and we are delighted the chairman of the full committee has designated you as vice chairman of this Subcommittee on Government Management, Information, and Technology. So we look forward to working with you.

Now, Mr. Koskinen, you know the routine that we swear all witnesses that come before us, and you have taken the oath many times, so I am sure you know it by heart.

[Witness sworn.]

Mr. HORN. Thank you very much. Please be seated. Start in. We are going to give you as much time as we can divide between the three of you this morning, because we want to thoroughly get into this. So feel free to educate us.

STATEMENT OF JOHN KOSKINEN, CHAIRMAN, PRESIDENT'S COUNCIL ON THE YEAR 2000 CONVERSION

Mr. KOSKINEN. Thank you and good morning Chairman Horn, Chairwoman Morella. I am pleased to appear again before this joint session of your subcommittees to discuss the activities of the President's Council on Year 2000 Conversion and the status of public and private sector efforts to address the year 2000, or Y2K as it is known, computer problem.

With your permission I will submit for the record my full statement, along with the most recent OMB report on the status of Federal progress and the first quarterly report by the President's Council on the national assessments of progress in critical sectors. With your permission, Mr. Chairman.

Mr. HORN. Without objection it is in the record.

Mr. KOSKINEN. I appreciate the increased visibility you have given to the year 2000 problem through your oversight and regional hearings. The problem presents us with a management challenge unlike any we have ever seen. Businesses and governments across the country are engaged in vigorous efforts to ensure that systems are prepared for the date rollover. The scope of the challenge is vast, and not every system will be fixed by January 1, 2000. While progress is being made in the public and private sectors, continued efforts are necessary if we are to achieve our shared goal of minimizing Y2K-related disruptions.

One aspect of the Y2K problem applies to every public and private sector organization. You are never really done. It is not enough for the Federal Government or any organization just to fix

its own systems. Organizations also need to be concerned about the progress of partners they exchange data with and depend upon as well as progress among other organizations whose failure could have a significant effect upon their operations.

The Council began its work last year using this "three-tiered" model. From the Federal Government's point of view, it means first ensuring that critical Federal systems are ready for January 1, 2000; next, working with our interface partners for important Federal services, primarily States, to ensure they are remediating their systems; and finally, reaching out to those whose failures domestically or internationally could have an adverse effect upon the public.

To reach out beyond the Federal Government, the Council has formed working groups focused on Y2K challenges in over 25 critical sectors such as finance, communications, transportation, electric power, oil and gas, and water supply. The working groups have reached out to form cooperative working relationships with major trade associations and other umbrella organizations representing the individual entities operating in each sector.

We have also created a Senior Advisors Group to the President's Council which will hold its first meeting tomorrow. This group is comprised of Fortune 500 company CEOs and heads of national public sector organizations representing our working groups. I am submitting for the record also the present list of group members.

Mr. HORN. Without objection it will be put in the record at this point.

[The information referred to follows:]

SENIOR ADVISORS GROUP
TO THE
PRESIDENT'S COUNCIL ON YEAR 2000 CONVERSION

as of January 14, 1999

Sector	Name	Title/Organization	National Association
Airlines	Gerald (Jerry) Greenwald	Chairman, United Airlines	Chairman-elect, Air Transport Association
Airports	James A. (Jim) Brough	Chairman of the Board, Birmingham Airport Authority	Chairman of the Board, Airports Council International
Banking	A. Scott Anderson	CEO, Zion National Bank	American Bankers Association
Electric Power	Eric Nye	Chairman of the Board and Chief Executive Officer, Texas Utilities Company	Chairman, North American Electric Reliability Council
Emergency Services	Ellen Gordon	Administrator, Iowa Emergency Management Division	President, National Emergency Management Association
Food Supply	Arnold Langbo	Chairman, Kellogg Company	Chairman, Grocery Manufacturers Association
Hospitals	Frederick (Fred) Lee Brown	Vice Chairman, BJC Health Systems	Chairman-elect, American Hospital Association
Information Technology	John Keane	Chairman/CEO, Keane Inc	Former Chairman of the Board, Information Technology Association of America
Insurance	Bernard Hengesbaugh	Executive Vice President and Chief Operating Officer, CNA Insurance	American Insurance Association
Manufacturing	Calvin A. "Tank" Campbell, Jr	CEO, Goodman Equipment Manufacturers	Chairman, National Association of Manufacturers
Maritime/Shipping	Richard du Moulin	Chairman/CEO, Marine Transport Corporation	International
Pharmaceuticals	Robert C. (Bob) Black	President, Zeneca Pharmaceuticals	Pharmaceutical Research and Manufacturers of America
Police	Chief Ronald Neubauer	Chief, St. Peters Police Department, St. Peters, MO	Chairman, International Association of Chiefs of Police
Port Authorities	H. Thomas (Tom) Kornegay	Executive Director, Port of Houston Authority	Chairman of the Board, American Association of Port Authorities
Postal Service	Postmaster General William J. Henderson	Postmaster General, United States Postal Service	-
Railroads	Robert (Rob) D. Krebs	Chairman, Burlington Northern Santa Fe	Chairman of the Board, American Association of Railroads
Securities	Roy Zuckerberg	Limited Partner, Goldman Sachs	Chairman-elect, Securities Industry Association
State/Local Governments	The Honorable Dan Blue	State Representative, North Carolina	Chairman, National Conference of State Legislatures
Telecommunications	Sol Trujillo	CEO, USWest	National Reliability and Interoperability Council
Surface Transportation	The Honorable Wayne Shackelford	Commissioner, Georgia Department of Transportation	Chairman of the Board, Intelligent Transportation Society of America
Urban Mass Transit	Shirley A. Delibero	President/CEO, Metropolitan Transit Authority, Harris County, TX	Chairperson of the Board, American Public Transit Association
Water Utilities	Randall J. (Randy) Goss	Director, Waste and Wastewater, City of Austin, TX	American Water Works Association

Mr. KOSKINEN. The group will provide the Council with an additional perspective on Y2K challenges that cut across sector lines and will recommend how industries can best work together in critical areas.

As noted, our first challenge is to ensure that Federal systems are prepared for the year 2000. I am pleased to report that the Federal Government continues to make strong, steady progress in solving its Y2K problems.

According to the most recent OMB report released last month, 61 percent of all Federal mission-critical systems are now year 2000 compliant, more than double the 27 percent compliant a year ago. The report also states that of critical systems requiring repair work, 90 percent have been fixed and are now being tested.

The President has established an ambitious goal of having 100 percent of the government's mission-critical systems Y2K compliant by March 31 of this year, well ahead of many private sector system remediation schedules. Although much work remains, we expect well over 80 percent of the government's mission-crictical systems will meet the March goal, and monthly benchmarks for completing the work will be available for every system still being tested and implemented. We expect that all of the government's critical systems will be Y2K compliant before January 1, 2000.

This does not mean that we are without significant challenges. While the Defense Department continues to make progress in addressing its massive Y2K challenge, OMB reported that DOD's rate of progress indicates that not all of its systems will meet the March goal of being 100 percent compliant. At a recent day-long meeting at the Pentagon to review the status of all DOD mission-critical systems, Deputy Secretary Hamre and I were advised that most systems will either meet the March date or be in the process of implementation. And, in fact, as of January 1 of this year, 73 percent of the Department's mission-critical systems are now compliant.

According to the last OMB quarterly report, the Energy Department had completed testing on only 53 percent of its critical systems, below the governmentwide average. Secretary Richardson made clear at the beginning of his tenure at the Department that this issue will receive his personal attention, and recent progress has the Department confident that over 90 percent of its systems will meet the March government deadline.

HHS's Health Care Financing Administration [HCFA] has finished renovating and testing all of its internal systems. Although a tremendous amount of systems work and contingency planning will remain after March, most Medicare contractors are expected to complete renovation and testing by the governmentwide goal.

The State Department also faces a significant challenge in simultaneously managing its complex Y2K project and completely replacing information systems installed around the world. However, as I was informed at my monthly meeting last week with the Department senior managers, the State Department expects that well over 90 percent of its systems will meet the March governmentwide goal.

At the Transportation Department, the FAA's rate of progress has improved dramatically, but the percentage of DOT's critical systems that have been tested and implemented continues to lag

behind the government-wide schedule. Nonetheless I am confident the air traffic system will be totally compliant well in advance of the year 2000.

Our second challenge is the work with the Federal Government's interface partners, primarily the States, as they work to ensure that their systems are ready for the year 2000. As a general matter, most States are making good progress in remediating their systems. But not every State is doing well. A National Association of State Information Resource Executives survey indicated that a handful of States report that they have not yet completed work on any of their mission-critical systems.

Federal agencies are actively working with the States to ensure the Federal-State data exchanges for State-administered programs will be ready for the year 2000. Most Federal agencies and States have now inventoried all of those exchange points and are sharing information with one another to ensure the exchanges will function in the year 2000.

For the February 1999 quarterly report, OMB has asked the Federal agencies to provide assessments of each State's Y2K progress on key State-administered Federal programs such as food stamps and child welfare programs.

The third challenge for the President's Council is to reach out beyond the Federal Government and its partners to those organizations whose failures would have an adverse effect upon the public. As noted earlier, the Council has formed over 25 working groups performing outreach in critical sectors. The working groups, under the leadership of their outside industry group partners, are focused on gathering industry assessments of Y2K preparedness in critical sectors. Earlier this month the Council issued its first quarterly summary of this assessment information, which I have provided for the record.

While many industry groups are just beginning to receive survey data from their members and some report they expect to have such information for the first time within the first quarter of the year 2000, I would like to make three points about what we know thus far.

First, we are increasingly confident there will not be large-scale national disruptions in key infrastructure areas. In particular, the telecommunications and electric power industries have constructed well-organized and comprehensive responses to the problem.

Second, banks, large and small, are well prepared for the year 2000 transition. In the most recent examination by Federal regulators, 96 percent of the Nation's depository institutions were on track to meet the regulators goal of completing Y2K work by June 1999.

The third point is obvious but bears repeating. Our greatest risk lies in organizations that are not paying adequate attention to the problem. The greatest risks therefore at this time, in our view, are in three areas: smaller government entities, small businesses, and internationally.

At the local level, many towns, cities, and counties are aggressively attacking the problem and are making good progress. But according to a December 1998 National Association of Counties survey done for us of 500 counties representing 46 States, roughly half

of the counties do not have a county-wide plan for addressing year 2000 conversion issues, and almost two-thirds of the respondents have not yet completed the assessment phase of their year 2000 work.

Many small and medium-sized businesses are also taking steps to address the problem and to ensure not only that their systems are compliant but that organizations they depend upon are ready for the year 2000 as well. However, a National Federation of Independent Businesses survey released this month indicates as many as one-third of small businesses using computers or other at-risk devices have no plans to assess their exposure to the Y2K problem.

Internationally, there is more activity now than there was a year ago, but it is clear that most countries are significantly behind the United States in efforts to prepare critical systems for the new millennium. Awareness remains especially low among developing countries. While strong international coordination of Y2K efforts has existed for some time in the areas of finance and more recently has begun to take shape for telecommunications and air traffic, we are very concerned about the lack of information and coordination in the area of maritime shipping.

The Council has been working to improve the response among smaller governments, small businesses, and international entities. For smaller governments, we have been working to reach out through groups like the National Association of Counties and the National League of Cities. We are also encouraging State year 2000 coordinators to focus on the efforts of smaller governments within their jurisdictions.

For small businesses, the Council joined the SBA, the Commerce Department, and other Federal agencies in launching National Y2K Action Week last October, to encourage small and medium-sized businesses to take action on the year 2000 problem with educational events that were held across the country. Another week is planned for this spring. And SBA has mounted an aggressive outreach program where, through its Web page and partners in the banking and insurance industries, it is distributing Y2K informational materials to the Nation's small businesses.

Internationally, as the chairman noted, the Council worked with the United Nations to organize last month a meeting of national year 2000 coordinators from around the worlds, perhaps the most important year 2000 meeting to date. More than 120 countries sent representatives to New York, and I was delighted Chairman Horn and Congressman Kucinich attended as well. The delegates at the meeting agreed to work on a regional basis to address cross the border issues. They also asked the steering committee we had created to help organize the meeting to establish an international mechanism for coordinating regional and global activities, including contingency planning. We are now working with this steering committee to create an International Y2K Cooperation Center which will support regional activities and international initiatives in areas such as telecommunications and transportation.

The Federal Government responds to a range of emergencies under the direction of several agencies. One of the challenges of the Y2K problem is that while we do not expect major national failures in the United States, it is possible that we will have a confluence

of demands for assistance and response as the clock turns to January 1, 2000. Therefore, we are working with all of the major emergency response agencies to create a coordinating center to ensure that we can respond effectively to whatever challenges we face moving into the next century.

We will also be discussing with our partners in our varied working groups, under the leadership of the Senior Advisors Group, the status of industry-wide plans for dealing with any emergencies they may confront. While these responses are primarily the responsibilities of each individual enterprise and industry, we clearly will all benefit by coordinated planning and communication.

Let me close by noting that we all continue to confront the challenge of encouraging organizations to take the Y2K problem seriously, remediate their systems, and prepare contingency plans without causing a public overreaction that is unnecessary and unwarranted. Our strategy is based on the premise that the public has great common sense and will respond appropriately when they have the necessary information.

We believe, therefore, that everyone working on this problem, at the Federal level, at the State and local level, and in the private sector, needs to provide the public with clear and candid information about the status of their year 2000 activities. That is why we are making the industry assessments we gather publicly available. That is why the OMB reports on Federal progress are available to the public. That is why we have created the 1–888–USA–4–Y2K information line for consumers. That is why we will provide details of our contingency planning and are encouraging others to do the same for the public.

A corollary principle is that everyone working on this problem has a responsibility to ensure their comments accurately reflect the factual information that is available and that they avoid overgeneralizations that will only play into the hands of those who want to create panic for their own gain.

We remain committed to working with your subcommittees and others in Congress on this critical issue, and I would be pleased to answer any questions you may have at this time.

[The prepared statement of Mr. Koskinen follows:]

STATEMENT OF JOHN A. KOSKINEN
CHAIRMAN
PRESIDENT'S COUNCIL ON YEAR 2000 CONVERSION
BEFORE THE
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY
OF THE COMMITTEE ON GOVERNMENT REFORM AND OVERSIGHT
AND THE
SUBCOMMITTEE ON TECHNOLOGY
OF THE COMMITTEE ON SCIENCE
U.S. HOUSE OF REPRESENTATIVES

January 20, 1999

Good morning. I am pleased to appear again at this joint session of your Subcommittees to discuss the activities of the President's Council on Year 2000 Conversion and the status of public and private sector efforts to address the Year 2000 (Y2K) computer problem.

I appreciate the increased visibility you have given to the Year 2000 problem through your oversight and regional hearings. The Y2K problem presents us with a management challenge unlike any we have ever seen. Businesses and governments across the country are engaged in vigorous efforts to ensure that systems are prepared for the date rollover. The scope of the challenge is vast, and not every system will be fixed by January 1, 2000. While progress is being made in the public and private sectors, continued efforts are necessary if we are to achieve our shared goal of minimizing Y2K-related disruptions.

The Three-Tiered Approach

One aspect of the Y2K problem applies to every public and private sector organization: you are never really done. It's not enough for the Federal Government, or any organization, to fix its own systems. Organizations also need to be concerned about the progress of partners they exchange data with and depend upon as well as progress among other organizations whose failure could have a significant effect upon their operations.

The Council began its work last year using this "three-tiered" model. From the Federal Government's point of view, it means first, ensuring that critical Federal systems are ready for January 1, 2000; next, working with our interface partners for important Federal services, primarily States, to ensure that they are remediating their systems; and, finally, reaching out to those whose failures domestically or internationally could have an adverse affect on the public.

As you know from my appearance before your Subcommittees last spring, the Council's more than 30 agencies, including several independent regulatory agencies, work together to exchange information on agency Y2K progress and shared challenges. They also coordinate

interagency testing efforts for programs that rely upon multiple agency systems and assist each other with contingency planning efforts.

To reach out beyond the Federal Government, the Council has formed working groups focused on Y2K challenges in over 25 critical sectors such as finance, communications, transportation, electric power, oil and gas, and water supply. The working groups have reached out to form cooperative working relationships with the major trade associations and other umbrella organizations representing the individual entities operating in each sector. Working group outreach efforts are designed to increase the level of action on the problem and to promote the sharing of information between entities. The outside organizations in each sector have also agreed to conduct Year 2000 readiness surveys of their members.

We have also created a Senior Advisors Group to the President's Council, which will hold its first meeting tomorrow. This group is comprised of *Fortune 500* company CEOs and heads of national public sector organizations representing our working groups. I am submitting for the record the present list of Group members. The Group will provide the Council with an additional perspective on Y2K challenges that cut across sector lines and recommend how industries can best work together in critical areas.

Federal Agency Progress

Our first challenge is to ensure that Federal systems are prepared for the Year 2000. These are the systems for which we are responsible and have the authority to fix. Consequently, it is the area about which we have the most information. And I am pleased to report that the Federal Government continues to make strong, steady progress in solving its Y2K problems.

According to the most recent OMB report released last month, 61 percent of all Federal mission-critical systems are now Year 2000 compliant – more than double the 27 percent compliant a year ago. These systems have been tested and implemented and will be able to accurately process data through the transition from 1999 into the Year 2000. The report also states that, of critical systems requiring repair work, 90 percent have been fixed and are now being tested.

Let me share a few examples of recent progress. As of November 15, the Small Business Administration (SBA) had completed work on all of its critical systems, ensuring that SBA assistance to the Nation's 24 million small businesses will not be interrupted in January 2000. The Interior Department posted a 50 percent increase in its number of Y2K compliant systems compared to the last quarter that includes the U.S. Geological Survey's National Seismic Network, which provides early warnings of earthquakes. The Education Department's number of critical systems, many of which are an integral part of processing student loans, that are now Y2K compliant increased by more than one-third. And at the end of last month, the President announced that, thanks to the joint efforts of the Social Security Administration and Treasury's

Financial Management Service, the Social Security payment system is now Y2K compliant.

The President has established an ambitious goal of having 100 percent of the Government's mission-critical systems Y2K compliant by March 31, 1999 -- well ahead of many private sector system remediation schedules. Although much work remains, we expect that over 80 percent of the Government's mission-critical systems will meet the March goal, and monthly benchmarks with a timetable for completing the work will be available for every system still being tested or implemented. We expect that all of the Government's critical systems will be Y2K compliant before January 1, 2000.

This does not mean that we are without significant challenges. While the Defense Department continues to make progress in addressing its massive Y2K challenge, OMB reported that DOD's rate of progress indicates that not all of its systems will meet the March goal of 100 percent compliance. At a recent, day-long meeting at the Pentagon to review the status of all DOD mission-critical systems, Deputy Secretary Hamre and I were advised that most systems will either meet the March date or be in the process of implementation. In the Department's case, implementation includes installing completed Y2K-compliant systems across the services.

According to the last OMB quarterly report, the Energy Department had completed testing on only 53 percent of its critical systems -- below the government-wide average. Secretary Richardson made clear at the beginning of his tenure at the Department that this issue will receive his personal attention and recent progress has the Department confident that over 90 percent of its systems will meet the March Government-wide goal.

At HHS's Health Care Financing Administration (HCFA), HCFA has finished renovating and testing all of its internal systems. Although a tremendous amount of systems work and contingency planning will remain after March, most Medicare contractors are expected to complete renovation and testing by the Government-wide goal.

The State Department faces a significant challenge in simultaneously managing its complex Y2K project and completely replacing information systems installed around the world. However, as I was informed at my monthly meeting last week with the Department's senior managers, State expects that over 90 percent of its systems will meet the March Government-wide goal.

At the Transportation Department, the FAA's rate of progress has improved dramatically, but the percentage of DOT's critical systems that have been tested and implemented continues to lag behind the government-wide schedule. Nonetheless, I am confident that the air traffic system will be totally compliant well in advance of the Year 2000.

Let me be clear: Fixing the Year 2000 problem in Federal agencies is not a question of commitment. As you know, since last summer I have been participating in the monthly Y2K meetings of the senior managers in agencies whose systems are most at risk. I can attest that they

and their staffs are focused on getting the job done. It is more a question of doing whatever it takes to overcome obstacles and accelerate progress in remediating systems. I am confident these agencies will be able to do that and ensure that their critical systems will be ready for the Year 2000. I also think all of us will owe a strong and clear vote of thanks to the thousands of Federal employees who will have made that accomplishment possible.

Interface Partners

Our second challenge is to work with the Federal Government's interface partners, primarily the States, as they work to ensure that their systems are ready for the Year 2000.

States administer over 160 Federal programs. These programs provide some of the most recognizable Federal services such as Unemployment Insurance, Medicaid, and Food Stamps. Millions of Americans rely upon these programs, so the Federal Government obviously has a vested interest in requiring that State systems administering them are Y2K compliant.

As a general matter, most States are making good progress in remediating their systems. Virtually every State has an organized Y2K program in place, often led by a designated State Y2K Coordinator. According to a National Association of State Information Resource Executives (NASIRE) survey of State Y2K remediation efforts, several States report that they have completed Y2K work on more than 70 percent of their systems. But not every State is doing well. The same NASIRE survey indicates that a handful of States report that they have not yet completed work on any of their critical systems.

The Council's State and Local Government Working Group is led by the White House Office of Intergovernmental Affairs and includes key groups like the National Governors Association, the National Association of Counties, the National League of Cities, and NASIRE. Last summer, Council members joined the National Governors' Association in a Y2K summit with Year 2000 coordinators from 45 States. To help sustain the momentum generated at that conference, I now participate in a monthly conference call with State Year 2000 executives to discuss cooperative efforts between the Federal Government and the States and how States can help each other to address Y2K challenges.

Federal agencies are also actively working with the States to ensure that Federal-State data exchanges for State-administered programs will be ready for the Year 2000. Most Federal agencies and States have now inventoried all of their data exchange points and are sharing information with one another to ensure the exchanges will function in the Year 2000. However, as of the most recent OMB quarterly report, three States had not yet provided any information on the status of their data exchange activities. For the February 1999 quarterly report, OMB has asked agencies to provide assessments of each State's Y2K progress on key State-administered Federal programs such as Food Stamps and child welfare programs.

Our joint Y2K efforts with the States are bearing fruit. Working together, we recently overcame one of the first major examples of a "look ahead" Y2K problem. The Unemployment Insurance program, a major Federal-State partnership administered by 53 State Employment Security Agencies (SESAs), encountered the Year 2000 problem on January 4. Since new claims are calculated on a 12-month basis, State systems had to process dates going into January 2000. The Labor Department had been working closely with all the States to ensure that they could continue to process claims and provide benefits through this transition, particularly the 16 SESAs that had not completed all of their Y2K system renovation before January 4, 1999. Thanks to this collaborative effort, these SESAs were prepared with, and are now using, temporary fixes to their systems so that they can continue to accept claims and process benefits while they complete their remaining Y2K work. The Department has also instituted special reporting procedures for the Unemployment Insurance program to identify any early problems. Reports have been received from all States and indicate that no Y2K-related service disruptions have occurred.

Beyond the Federal Government

The third challenge for the President's Council is to reach out beyond the Federal Government and its partners to those organizations whose failures would have an adverse effect on the public. As noted, to accomplish this goal, the Council has formed over 25 working groups in critical sectors such as electric power, communications, oil and gas, finance, and transportation. One of the first things our working groups encountered in their relationships with major industry trade associations and others was a reluctance on the part of many to share technical and other valuable information about their experiences in addressing the problem as well as information about the status of their Y2K remediation efforts.

To break this logjam and help associations and other groups collect and share Y2K information, the Administration worked with Congress to enact the "Year 2000 Information and Readiness Disclosure Act." This bipartisan legislation provides protection against the use, in civil litigation, of technical Year 2000 information about an organization's experiences with product compliance, system fixes, testing protocols, and testing results when that information is disclosed in good faith. It also includes important protections for information gathering that is designated as a "special data gathering request" under the Act. These collections of information cannot be reached by private litigants, or used by Federal agencies for regulatory or oversight purposes, except "with the express consent or permission" of the provider of the information.

Using these statutory protections, the working groups, under the leadership of their outside industry group partners, are focused on gathering industry assessments of Y2K preparedness in critical sectors. Earlier this month, the Council issued its first quarterly summary of this assessment information. While many industry groups are just beginning to receive survey data from their members and some report that they expect to have such information within the first quarter of this year, I'd like to make three points about what we know thus far.

First, we are increasingly confident that there will not be large-scale, national disruptions in key infrastructure areas. In particular, the telecommunications and electric power industries have constructed well-organized and comprehensive responses to the problem.

Second, banks -- large and small -- are well-prepared for the Year 2000 transition. In the most recent examination by Federal regulators, 96 percent of the Nation's depository institutions were on track to meet the regulators' goal of completing Y2K work by June 1999.

The third point is obvious but it bears repeating. Our greatest risk lies in organizations that are not paying adequate attention to the problem.

If the head of an organization has fixing the Y2K problem as a top priority, that organization is by definition going to be better prepared -- even if it cannot fix all of its systems before January 1, 2000. It is organizations where the leadership is convinced that the problem doesn't apply to them or that they can simply fix systems when they break that are of most concern. The greatest risks are, therefore, in three areas: smaller government entities, small businesses, and internationally.

At the local level, many towns, cities, and counties are aggressively attacking the problem and are making good progress, but a significant number are not sufficiently organized to prepare critical systems for the new millennium. According to a December 1998 National Association of Counties survey of 500 counties representing 46 States, roughly half of counties do not have a county-wide plan for addressing Year 2000 conversion issues. Almost two-thirds of respondents have not yet completed the assessment phase of their Year 2000 work.

Many small and medium-sized businesses are also taking steps to address the problem and to ensure not only that their own systems are compliant but that organizations they depend upon are ready for the Year 2000 as well. But a significant number of small and medium-sized businesses are not preparing their systems for the new millennium. A recent National Federation of Independent Business survey, released this month, indicates that as many as one-third of small businesses using computers or other at-risk devices have no plans to assess their exposure to the Y2K problem. The survey also indicates that more than half of small firms have not yet taken any defensive steps.

Internationally, there is more activity than there was a year ago, but it is clear that most countries are significantly behind the United States in efforts to prepare critical systems for the new millennium, and a number of countries have thus far done little to remediate systems. Awareness remains especially low among developing countries. While strong international coordination of Y2K efforts has existed for some time in the area of finance and more recently has begun to take shape for telecommunications and air traffic, we are very concerned about the lack of information and coordination in the area of maritime shipping. Lack of progress on the international front may lead to failures that could affect the United States, especially in areas that

rely upon cross-border networks such as transportation.

The Council has been working to improve the response among smaller governments, small businesses, and international entities. For smaller governments, we have been working to reach out through groups like the National Association of Counties and the National League of Cities. We are also encouraging State Year 2000 coordinators to focus on the efforts of smaller governments within their jurisdiction. For small businesses, the Council joined the SBA, the Commerce Department, and other Federal agencies in launching "National Y2K Action Week," last October to encourage small and medium-sized businesses to take action on the Y2K problem with educational events that were held across the country. Another week is planned for this spring. And SBA has mounted an aggressive outreach program where, through its web page and with partners in the banking and insurance industries, it is distributing Y2K informational materials to the Nation's small businesses.

Internationally, the Council worked with the United Nations to organize last month a meeting of national Year 2000 coordinators from around the world, perhaps the most important Year 2000 meeting to date. More than 120 countries sent representatives to New York, and I was delighted that Chairman Horn and Mr. Kucinich were able to attend as well. The delegates at the meeting agreed to work on a regional basis to address cross-border issues (e.g., telecommunications, transportation). They also asked the steering committee we had created to help organize the meeting to establish an international mechanism for coordinating regional and global activities, including contingency planning. We are now working with this committee to create an "International Y2K Cooperation Center," which will support regional activities and international initiatives in areas such as telecommunications and transportation. The World Bank has agreed to support the advisory and planning activities of such an entity.

Contingency Planning and Emergency Response

The Federal Government responds to a range of emergencies under the direction of several agencies. FEMA chairs the Catastrophic Disaster Response Group, which is comprised of a set of Federal agencies and the Red Cross. The State Department and the Treasury Department have responsibilities for foreign civil emergencies while the Defense Department supports both domestic and foreign emergency responses as well as being responsible for national security. The Departments of Energy and Transportation each have emergency command centers to help respond to challenges in their areas.

One of the challenges of the Y2K problem is that, while we do not expect major national failures in the United States, it is possible that we will have a confluence of demands for assistance and response as the clock turns to January 1, 2000. Therefore, we are working with all of the major emergency response agencies to create a coordinating center to ensure that we can respond effectively to whatever challenges we face moving into the next century.

We will also be discussing with our partners in our varied working groups, under the leadership of the Senior Advisors Group, the status of industry-wide plans for dealing with any emergencies that they may confront. While these responses are primarily the responsibility of each individual enterprise and industry, we clearly will all benefit by coordinated planning and communication.

We also are encouraging all organizations, beginning with the Federal agencies, to have contingency plans for the possible failure of their systems as well as the failure of systems they rely on that are run by others. As demonstrated by the Unemployment Insurance experience, the best form of response to a system failure is an effective backup plan.

The Balancing Act

Let me close by noting that we all continue to confront the challenge of encouraging organizations to take the Y2K problem seriously, remediate their systems, and prepare contingency plans without causing a public overreaction that is unnecessary and unwarranted. Our strategy is based on the premise that the public has great common sense and will respond appropriately when they have the necessary information.

We believe, therefore, that everyone working on this problem -- at the Federal level, at the State and local level, and in the private sector -- needs to provide the public with clear and candid information about the status of their Year 2000 activities. That's why we're making the industry assessments we gather publicly available. That's why the OMB reports on Federal progress are available to the public. That's why we have created the 1-888-USA-4-Y2K information line for consumers. That's why we will provide details of our contingency planning and are encouraging others to do the same.

A corollary principle is that everyone working on this problem has a responsibility to ensure that their comments accurately reflect the factual information that is available, and that they avoid over generalizations that will only play into the hands of those who want to create panic for their own gain.

We remain committed to working with your Subcommittees and others in Congress on this critical issue. I would be pleased to answer any questions you may have at this time.

Mr. HORN. Thank you very much for that very thorough testimony. I have simply one question and then we are going to yield to Mrs. Morella for 5 minutes, then yield to Mr. Turner for 5 minutes, then go down the line for each Member with 5 minutes, and if more arrive we will alternate by party.

But let me ask you, one of the key things here that I think worries you as well as worries us, and that is the status of the Federal agencies' data which are based on self-reporting. And I think you will recall that we had a case where the Inspector General of Defense found that—and GAO, I might add—found that the Department of Defense reported certain systems fixed when in fact they were not.

How do you deal with that when you are getting the data and you are not over there, and how do we handle something like that?

Mr. KOSKINEN. It is obviously an important problem across the board. You may recall I chaired the interagency groups of Inspectors General in my prior incarnation when I was at OMB. I have met regularly with the Inspectors General and encouraged them to independently review the status of the agency year 2000 efforts. And, in fact, they have done an excellent job in a number of agencies by revealing areas where there are problems.

OMB has also required all of the agencies to have independent verification and validation. In fact, before the President announced that Social Security was completed, we waited until the Social Security Administration had certified its systems were compliant, we waited until the Treasury Department's Financial Management Service was able to certify that its systems were year 2000 compliant, and we waited until those systems had been tested and worked together. So I think there is an ongoing need to ensure that we continually evaluate and check the information agencies provide.

GAO has also done an excellent job not only in providing general information about how to deal with the problem, but in conducting independent reviews to determine whether or not there are gaps. As the agencies and the Inspectors General understand, the goal here is not to, in fact, find people who have made a mistake and point that out for the sake of pointing it out. The goal is to ensure that as many systems as possible are functioning and are able to function as we move into the year 2000.

Mr. HORN. I thank the gentleman. And now, Mrs. Morella, the co-chairman, 5 minutes.

Mrs. MORELLA. Thank you. Thank you for the progress you are making Mr. Koskinen. We appreciate it and you have to be kind of a wonder man to do it all.

Let me just reiterate the fact that last year I introduced a bill which had three different segments, Mr. Barcia had contributed one of his bills to part of it, and Mr. Leach in my bill, and it passed the House. I am recrafting it because it didn't get out of the Senate because I want you to be involved. I want your support of the bill.

The administration appeared to be in favor of it. We have changed it so that it doesn't have as many requiring mandates within it, which I think was one of your concerns. I don't know whether you have had a chance to look at it, but——

Mr. KOSKINEN. I have not seen any drafts.

Mrs. MORELLA. I would like to work with you on it very soon.

Mr. KOSKINEN. I would be delighted to review the draft and certainly to work with you and your staff.

Mrs. MORELLA. Excellent. I think something is needed. It is not something that is going to be threatening and I think it is something that definitely will help. So I have your assurance we are going to work together soon.

Now, when I was in Tokyo, I remember reading in the newspaper there, the Japan Times, about the fact that China had issued a mandate that on January 1, 2000, every plane was going to be flying. Now, I don't want to fly on one of those planes.

Mr. KOSKINEN. Actually, the mandate is that every senior executive of the airlines be on those planes.

Mrs. MORELLA. Every senior executive will be on those planes. Now, I don't know quite how to respond to what that tells us. I mean I suppose it is a good opportunity to put people on certain planes and take care of changing the governmental leadership, but I wonder how you feel about that, because actually that gets into my question.

I understand that you have detailed Bruce McConnell from OMB to spearhead the Council's international efforts. Can you, not only whatever response you may have to what the Chinese officials are mandating, but also if you could give us more details regarding this effort and then how we in Congress can best assist.

Mr. KOSKINEN. I think the thrust of the Chinese initiative is to ensure that there is a great incentive to make sure their planes are able to fly. As you know, the problem with the planes flying is not safety, it is really whether in fact there are substantial delays. And, in fact, I have been committed for some time to fly to New York on New Year's Eve on a commercial airliner and take the first plane back on January 1st so that I can be in my office, because I do think it is important for the public to understand that we are confident these systems are going to work.

With regard to the International Cooperation Center, as Chairman Horn remembers, when we pulled the 120 countries and their senior year 2000 executives together at the United Nations meeting, we had a couple of goals. One was to get the delegates to commit to going back to their respective countries and to work on a regional basis to address cross-border issues, whether they be in telecommunications, power, shipping, whatever. They also asked the steering committee to set up an International Cooperation Center. Mr. McConnell's detail to the Council will allow him to chair and organize that center.

The center will be a virtual organization with contributions of senior executives from other countries. We already have offers from Mexico, Chile and South Africa. The center will provide support to existing regional activities. There is a major meeting coming up in Manila the first week of March.

It will also help coordinate and support international sector activities in such areas as banking, where the central banks have been supportive; telecommunications, under the International Telecommunications Union; and air traffic, under the International Civil Aeronautics Organization.

Also, as a result of the U.N. meeting, and through the leadership of the Coast Guard, we are creating and organizing a meeting that will also be held the first week in March of all major shipping interests around the world—private and public—to ensure that there is more coordination in that area.

Our goal is to support with other countries a more organized global approach to this problem, not only by countries but by sectors. We went to try to do as much as we can, first to ensure that countries fix as many systems as possible, and second to ensure that there is an organized set of contingency plans and emergency response mechanisms in place around the world.

Mrs. MORELLA. The 120 countries have all indicated that they are going to be part of this conference and be involved?

Mr. KOSKINEN. Yes. We were overwhelmed with the response to the United Nations meeting. We had thought we would do very well if we could get 50 countries. But when we had 120 countries show up and commit not only to do this work but to meet again in June at the United Nations to review progress across the board in great detail, I was convinced it was probably the most significant year 2000 meeting that had been held to date.

Mrs. MORELLA. It certainly is important. And, of course, the resources that are going to have to go into this, too, countries are just not aware of that, nor do they know how to expeditiously do it, since it is so labor intensive.

Just one final question. A number of my colleagues are very concerned about the potential of a deluge of civil litigation for possible Y2K failures. Is the Council going to be working with industries, consumer organizations for legislative remedies?

Mr. KOSKINEN. Liability is not totally within our domain. Our goal, as I have told people, is to have systems function at the end of this year. What happens after this year, once they are functioning, is not within the Council's jurisdiction.

We have worked very closely with Congress, and we genuinely appreciate the committee's support of the Year 2000 Information and Readiness Disclosure Act, because, as you noted, the disclosure of information is critical if we are to have systems function. But within that context we obviously have a wide range of working groups and contacts and we are listening to their concerns about liability. We have asked them to begin to quantify what the reality of those concerns are. There is a lot of hype and overexaggeration in all aspects of this problem. The art form, I think, is to try to figure out what is the reality, or what can we really expect, and then what is an appropriate response to that reality.

At this point, there are a wide range of industry groups focused on this problem who have yet to come together themselves on a common approach, but we are prepared to listen to their suggestions.

Mrs. MORELLA. We are concerned about a cottage industry of lawyers waiting there in advance.

Thank you.

Mr. HORN. I thank the gentlewoman and now yield to the ranking minority member, Mr. Turner, 5 minutes.

Mr. TURNER. Mr. Koskinen, thank you for your report today. I know the Internet is full of doomsday theories. One area I wanted

to particularly inquire about—I have a district with a lot of small towns and rural hospitals—is the suggestion that rural hospitals may be more vulnerable than most with some of the equipment that you find in emergency rooms and in intensive care units that are date-sensitive.

Is that a problem, and do you know what is going on, particularly among rural hospitals, to try to address it?

Mr. KOSKINEN. It is an important question. The rural hospitals are no more exposed to equipment issues than large hospitals. The concern we all have is that in rural areas, or smaller towns and communities, there may not be the same level of attention and focus on this problem or there may not be the same resources available.

We have been working in our health care outreach area with the American Hospital Association, and other health care groups to provide them and encourage them to provide technical information and resources to all of their members and to nonmember hospitals many of which are in rural areas so that they can take advantage of the experience and information that has been gained by large hospitals and major research centers who have been dealing with this problem.

The FDA, the VA, and the Department of Defense have all banded together to provide a Website with updated information on the status of medical devices. Fortunately, it turns out a very small percentage of those devices have a year 2000 problem. For those that do, the problem is generally not that they don't function but, as you noted, that they provide erroneous or incorrect data information, which can be critically important.

These are systems over which we have no direct control, but our goal is to try to do everything we can to increase the amount of information that is available to every rural hospital in this country on how to deal with the problem. Obviously, it is their responsibility to use that information, but our goal is to make sure that no one is unaware of the problem and without access to the best information that we and our working group partners can provide.

Mr. TURNER. I have been told that there are one or more dates during 1999 that could provide opportunities to know whether or not systems will fail on January 1, 2000. Is that the case, and, if so, would you explain that to me a little bit?

Mr. KOSKINEN. There are a range of issues that software programs will confront as we move through this year. First, any system that has to look forward into the year 2000 will obviously be challenged. We have all had experience with credit cards that have expiration dates that for a long time said 1999. Now, many cards expire in the year 2000 or beyond and most card processing systems are able to deal with the year 2000. If you have to make an airline or hotel reservation, if you order inventory and need to track it in the year 2000, the systems have been made to be compliant.

As we noted in December, unemployment insurance is the first major Federal program to encounter the year 2000 problem because those benefits are calculated on a look-forward of 12 months. So starting the first week of January 1999, the State systems running that program had to be able to deal with the first week of

January 2000. Some of the State systems are not yet compliant but, fortunately, those States have good contingency and backup plans so no one is missing an unemployment check while those States are finishing the work.

There are other dates people have focused on, particularly those that involve the number 9. A nonstandard programming practice was to use numbers like 99 to end a program operation. Fortunately, it was not an acceptable practice. But people originally focused on September 9, 1999 to see whether that date would work. People were also interested whether just rolling into the year 1999, whether January 1, 1999 would trigger defaults. Thus far there are only a handful of anecdotal reports from around the world that anyone had a problem with January 1, 1999. Another date will be April 9, 1999, which will be the 99th day of 1999.

Our expectation is that these dates will not cause major problems first, because everybody is aware of them and, second, because it was not a standard programming issue. But countries, governments, and businesses with fiscal years that start before the end of this year, will have fiscal year 2000 issues to confront. Many States have fiscal years starting in April, June or July. The Federal Government's begins on October 1, 1999, and will be operating against a fiscal year 2000 issue.

So all of those dates are important and all of them will give us some indication as to how successful year 2000 remediation has been. But I will tell you that even if you meet the September 9, 1999 and other challenges, it does not necessarily mean that you will not have a problem with the year 2000 transition.

Mr. TURNER. Thank you. I know the Federal Reserve has requested the Treasury Department print an extra $50 billion in cash for potential use at the end of the year. There are a lot of people, I noted in a town meeting I had a week ago, who seem to be aware that it might be important for them to withdraw cash from their bank accounts before January 1, 2000.

I assume that someone determined that the $50 billion in cash would be a sufficient amount, but is that a real problem and should the public be concerned about being able to get cash?

Mr. KOSKINEN. No. As I have said on numerous occasions, we have an obligation to be very candid with the public and tell them what works and what doesn't work, what has been completed and what has not been completed, so they can respond accordingly.

Initially, when people started talking about this and the Fed made that announcement some months ago, there was a concern about whether the ATM machines would work, whether you would have access to your cash, whether the banks would be able to function. The good news is that, at this point, as I noted, 96 percent of the banks are at the highest rating of preparedness in terms of dealing with the year 2000, according to the independent Federal regulators. So we expect the banks will be able to function.

The reason for ensuring that people are confident that the cash is there is not to combat fears that they won't get access to it, but to allay concerns about banks running out of cash if everyone decides to take out some extra money. The calculation was made that, on any basis, it is reasonable that the public should not be concerned about cash availability. And like anything in banking, if

people are confident the cash is going to be there, obviously they will be less likely to actually use it.

It is a long weekend; our general advice is that people, as they normally would, should have cash for that long weekend. What we are anxious to do is to not have the public unnecessarily decide that they need a month's cash or 2 months' cash, which would be a very different problem.

Mr. TURNER. It seems that the public information challenge that you have is enormous. You could make a judgment that to talk about it makes the problem worse. You could say, no, we have to talk about it because people need to know the facts. I find that people are very uneasy about it.

In this town meeting I referred to, we went through a litany of things that I knew from service on the committee were taking place to try to prepare for the year 2000. The group listened, obviously with some skepticism, and at the end they said, "Congressman, what are you going to do on January 1st?" And in a moment of candor I said, "Well, I probably won't fly that day."

Mr. KOSKINEN. I was just going to invite you to join me. But that is an issue. As I said when I testified last spring, if nobody gets off an airplane in Hawaii for 2 weeks, just to be careful, and if that is not necessary, we will have created a very major economic problem for the airlines and for Hawaii. Again, my view is I don't want the public to do anything that is risky. On the other hand, I think it is important for the public not to unwittingly create a problem even if the systems are running fine; that we have a problem with financial markets, we have a problem with banks, or we have our problems with a sector of the economy.

So I think what you are saying, the high wire act from the start has been on the one hand to be able to get people to understand this is a real problem, it is a serious problem that needs to be dealt with without, on the other hand, unnecessarily having them take unnecessary action. So we have an obligation to inform the public, and we are going to work on that. That is why we have the hotline, to provide the public with all the information we have and to give them our best advice as to what they ought to be doing to prepare for whatever the eventualities are.

My bottom line is we are concerned about preparedness at the local level and we are anxious in small and medium-sized cities and counties, to have people asking their governments to discuss with them where they are and what steps they have taken to deal with this problem.

Mr. HORN. I thank the gentleman. And now the gentlewoman from Illinois, the vice chairman of the Subcommittee on Government Management, Information, and Technology, Mrs. Biggert, 5 minutes.

Mrs. BIGGERT. Thank you, Mr. Chairman. Last year I understand that the chairman, Mr. Horn, did meet with the staff in Illinois, the Year 2000 Task Force, to talk about the year 2000 compliance. And out of this meeting came assurances that the Illinois utilities will be prepared for the year 2000, and particularly the systems that depend on power, such as water and sewer and things that we think of applying to municipalities, and they will continue to function effectively.

Is this true of other States? Are they far along in planning for these, dealing with utilities and things that cross really municipal lines but really are the functions that will go across the State?

Mr. KOSKINEN. As I noted, we are in the process with our working groups of reaching out and asking organizations to provide information on progress at the State and local level to us. That is where the National Association of Counties survey came from. As a general matter, I think the vast majority of States are doing a very good job. They are well organized and prepared to deal with the program. There are a few that are starting slower and have had a lower priority, but I think that is changing.

Our concern, even in the States doing very well, is at the local level. As you know, there are thousands of counties and cities out there that States do not directly manage those and, in fact, oftentimes do not have regular communication with them. So the challenge I have given to the States, as well as to Federal agencies, is to do whatever we can to reach out to make sure that every mayor, every city manager, and every county executive has this problem as a priority. If they have it off on the side, if they say somebody else is taking care of it; or, as we increasingly hear, "We will fix it when it breaks." I think that there is great risk in those communities to their emergency response system, their local hospitals, their local power plants, their local telephone companies.

Mrs. BIGGERT. What are you doing, then, to increase that awareness; are there meetings?

Mr. KOSKINEN. We have had meetings. We are working with the associations of counties, of cities, of States. We are providing information to them. We are encouraging them to provide information to them. The National League of Cities and the National Association of Counties have an organization, Public Technology, Inc. [PTI], which has been providing information to local governments.

Ultimately it is the responsibility of the local communities and the local governments are responsible for fixing their own systems, but our goal is to make sure nobody can say, "Gee, I didn't know about it." They may have to explain why they didn't do anything about it, but we are making sure that we are doing everything we can to make sure it is on their radar screen. It is up to them to make sure it is their priority.

Mrs. BIGGERT. It is their responsibility, but do you have any contingency plans in case the State systems should fail?

Mr. KOSKINEN. Yes. Our concern, as I noted, is that I think we will end up with no major national problems, but without work done locally, we could have a whole series of local problems, of local power outages or other local challenges. And it will all happen at once, as we go into the year 2000.

So FEMA is now engaging in starting a series of regional meetings with State and local emergency managers and their year 2000 coordinators to look at that problem, because I think that will be the real challenge for the emergency response system. We can handle a localized hurricaine or a tornado or whatever it might be. The question is how do the State systems and the Federal systems respond to what may be not necessarily guaranteed, but what may be a wide number of, local outages or problems.

If you have 20 such problems in a State and you have 50 States, you could have 1,000 communities all across the country saying, "Gee, we should have done more and now we have a problem, what help can you give us?" And we need to have a system capable of responding.

Mrs. BIGGERT. Just one other question, then. As far as the Department of Defense, you said that they were probably not moving as fast as some of the other agencies. Can we be really assured that they will meet those goals that have been set?

Mr. KOSKINEN. Yes. The Defense Department, obviously, is the largest Federal department. It has, in many ways, the most challenging systems because it has a lot of embedded chips or integrated circuits built into all their weapons systems. If you look at the structure in response to this problem over the last 12 months, you will see major changes in the way the Department has organized with it.

In August, the Secretary made it clear that this was on his agenda; that every commander in chief had to have it on their agenda. This issue was moved out of being an issue or CIO issue and into an operational force readiness issue. And, as I said, a week ago Saturday we spent the entire day reviewing the progress of every service and every function. And I think that while not every Department of Defense system will make the governmentwide compliance goal, I think the Department will have close to 90 percent of its systems done by March 31, which is an amazing accomplishment in light of where they were 9 months ago.

Mrs. BIGGERT. Thank you. Thank you, Mr. Chairman.

Mr. HORN. You have still got 30 seconds or so.

Mrs. BIGGERT. Well, in the words of Mr. Ose, I yield back my time.

Mr. HORN. We will go right to the top of the ladder. Sheila Jackson Lee is with the Subcommittee on Technology of the Committee on Science, 5 minutes for questioning.

Ms. JACKSON LEE. Mr. Chairman, thank you very much. I appreciate the opportunity for this hearing. Let me say to the public, if you wanted to know who that singular member was, it was my good friend, Connie Morella, last night standing up. And I am sure Chairman Horn was nearby on the Y2K issue, a very important issue.

In fact, let me say to Mr. Koskinen that I am being asked these questions in my district, so people are really concerned about the Y2K.

Not hearing all your presentation, and I apologize for being in other meetings and also apologize for having to leave, but would you take a stab at a question that has been posed on various news magazine shows and various sort of expose news magazine, television programs of people running to the hills and preparing?

Since the government has the responsibility of setting the tone and giving comfort to our citizens that we are aware of this issue, that we are moving expeditiously to ensure that civilization as they know it remains, can you speak to limiting hysteria about the issue that we are dealing with?

I know the questions were asked earlier, but I do want to have you just state for me succinctly, in looking at Congressman Horn's

assessment of the government efforts. I think I heard you say March 31st, but can you say to me why you think that is going to happen with what they have in place? With respect to the public and its general concern about us not being prepared, do you have a response to that?

Mr. KOSKINEN. Yes. And there is a longer response in my formal statement. But I think the bottom line is, what we are saying is in a context in which we have an obligation to provide real information to the public, and I think that is important. At this point, there is no indication that there will be any major national problem resulting from the year 2000 and, therefore, there is no indication that people need to disrupt their lives in preparation for it.

We will continue to provide the public information. I am confident—and Congressman Horn and I continue to discuss this—that the Federal Government is not only making great progress, but the vast majority of systems will meet the March 31 deadline and all systems will meet the January 1, 2000, deadline. So the Federal Government will not be the source of any difficulties that the public or the economy confront as we move into the year 2000.

On the other hand, there are areas we are concerned about. We are concerned about issues internationally. We are concerned about ensuring, to the extent we can, that State and local governments and smaller businesses all pay attention to this problem. And ultimately our commitment to the public is that they should know everything about this problem that I know; and we are doing everything we can to share information with them. Because I think what the public needs and what is an obligation in the private sector, as well as the public sector, is to provide information. The public needs to know about the state of preparedness.

The Federal Government is now acknowledged as the most transparent organization in the world on this issue. There is no one that provides as much information about its year 2000 progress, and as much discussion about it, as the Federal Government. And a lot of that is the result of an ongoing, constructive dialog between these committees and the executive branch. But we need to have that happen more often, because I think people are uneasy when they have no information about what the facts are, and they don't know what is going to happen.

So our goal over the next 6 months is to provide that information to the public. But at this stage in time, I can state confidently there is no evidence that there are going to be major dislocations. But people need to be engaged in a dialog with their county executives, with their mayors, with their city managers to ensure they are paying attention to this problem.

Ms. JACKSON-LEE. On that, might I followup very briefly?

Last evening the President acknowledged that all Social Security checks would be on time. This computerized problem probably will impact most decidedly those who are least advantaged, primarily the beneficiaries, if you will, of government programs. And when I say "government programs," AFDC, and you mentioned local governments, but Veterans, et cetera.

We mentioned Social Security. Where are we on those other kinds of issues, and would you also comment—and forgive me if it is in your speech as to whether or not—in your remarks, there are

internal task forces, I imagine, in each of the departments and the agencies that correlate with your work.

Mr. KOSKINEN. Yes, there are. Benefit programs run by the Federal Government are basically—to all intents and purposes, are none, not only Social Security, but Veterans Affairs and those benefits. Our challenge is that most Federal benefit programs are actually administered by State and local governments; food stamps, unemployment insurance, Medicaid are all State-run programs.

As I noted, we are concerned about this because it won't do us any good if 45 out of 50 States do a wonderful job. In those five States, the answer cannot be that beneficiaries do not receive benefits. So in the next OMB quarterly report, we have asked the Federal agencies to report the status of each State in each of the major Federal programs in terms of their progress, and we will monitor that progress as we go forward, because we need to ensure that those programs operate.

Because you are exactly right, the people most in need will oftentimes be Social Security beneficiaries, veterans beneficiaries and local people benefiting from programs like food stamps; and we have to ensure that jointly, working with the States, those programs operate.

Mr. HORN. Thank you very much.

Ms. JACKSON-LEE. Thank you.

Mr. HORN. We now have, first, the Government Management, Information, and Technology Subcommittee and then we are going to yield to the Technology Subcommittee. And eventually, we will cover everybody here.

Mr. Ose, the gentleman from California.

Mr. OSE. Thank you, Mr. Chairman.

First, may I pass a compliment, noting the subject matter that we are on, I walked in the room this morning at 11:14 and promptly at 11:15 this committee meeting started. So I think that is a great standard to adhere to. And I want to compliment you, Mr. Koskinen, I have a couple questions.

Is the Fed prepared?

Mr. KOSKINEN. Yes.

Mr. OSE. Treasury?

Mr. KOSKINEN. The Fed and the Treasury not only began work on their own systems, but have been major leaders not only domestically but internationally in trying to ensure that the financial systems around the world and the banks around the world operate. The Fed is a leader with the world's central banks; the Fed acutally chairs the joint Year 2000 Council which the banks set up.

The Fed has already been testing its interfaces with several thousand banks to make sure they work. And the Fed is one of the most active participants on the President's council. So I think, while we have issues and a lot of work going on in the other areas, the financial institutions area is in the best shape of any business area in the United States.

Mr. OSE. So when the check-clearing process hopefully doesn't stop, if it does stop, we know where to come?

Mr. KOSKINEN. That's right. I think at this juncture, that won't be the problem, at least from the Federal Government. I can't guarantee that every company's financial management and payroll sys-

tem will function, but the clearinghouses will function, and the Federal checks will be issued.

Mr. OSE. All right. I want to followup on my colleagues' comment or question earlier, am I right, the question about insurance. Any of the interface partners, the contractors that we deal with here, many of them cannot provide service when asked to bid, because they cannot obtain insurance on any actuarially sound basis, because there is no way of quantifying the exposure.

With respect to Mrs. Morella's question about the liability exposure, is there any way we, as the Federal Government, can set a standard for quantifying that exposure that would then allow insurance companies to set a policy for potential service providers in this area?

Mr. KOSKINEN. Well, it is the kind of a transition challenge in the legal issue. There is the issue in terms of how do we ensure that people can continue to work on systems. And there is a warranty and a patent and copyright problem; if the manufacturer doesn't exist or can't help you, can you work on this system, without violating copyright and patent laws? So those areas fit into my concern about what do we do to make sure the systems operate.

At this juncture, while there has been a lot of talk over the last 6 to 9 months about the insurability or noninsurability with people doing the work, it does not appear to have been a major impediment—certainly, from the Federal Government, where we monitor it carefully—to getting the work done.

It doesn't mean that there aren't companies out there that are having difficulty; there was a recent article about some service providers who have been negotiating in that area. So I think it is worth considering. But at this juncture, and even in our working groups, we have not found significant parts of the economy or the government that have said, we cannot get people to work on the problem because they cannot get insurance.

Mr. OSE. Mr. Chairman, if you will indulge me, I don't quite know if this is the context, but in the course of our deliberations, I think this is one of the critical issues that we are going to deal with is finding a way to open the door for providers to come and provide assistance, not only to the Federal Government, in our world here, but also to private industry.

With that, I yield the rest of my time.

Mr. HORN. You have made a very good point, and I thank you for making it. Now, long-suffering Mr. Gutknecht has 5 minutes and then Ms. Norton, Mr. Miller, and that will round out the 5-minutes.

Mr. GUTKNECHT. Thank you, Mr. Chairman. I couldn't help observe as I came into the room that about—almost 4 years ago we had our first hearing on this matter, at least in the technology committee. And at that hearing, I think we had three experts, maybe half a dozen staff, maybe two people who wondered in off the street. But there was almost no interest in this matter. And it is interesting how it has now finally, I think, dawned on the American people, this is a serious issue.

And I remember that first hearing and almost no one showed up. And, in fact, I sort of wondered why I was there when I looked at

the audience. But I do congratulate the Chairs. And I congratulate you, I think we have made significant progress.

More for the benefit of some of the other Members here, I would encourage other Members—all Members should consider doing what my staff and I did about a month and a half ago, back in our district, in fact, I hope we can do another one. That is, have a town hall meeting just about this subject.

And we invited some people from the financial institutions, a couple of large banks. We invited people from State and local government. We invited people from the utilities. We were fortunate enough to get the top person from Northwest Airlines to come in and speak. And it was a very, very interesting hearing. And the only regret that I had is, we didn't publicize it quite enough. So we should have had a little better public attention, but it did get pretty good press.

I think what was great about that, really is twofold, first of all, it opened up my eyes—and I will get to a question. The problem in some respects is even bigger than some of us had thought before the meeting.

And you raised the issue of embedded chips, and I want to come back to that.

But it was also very impressive to me how much is being done in the private sector. I sort of kept a little running total of the companies and, as I say, these were—well, we had a couple of major utilities and a major airline, and obviously it is an important issue to them. But I think of the private concerns that testified that day at this town hall meeting that we had, they were committing somewhere north of $100 million to this effort. So they take it extremely seriously, and I think that was the good news.

But the bad news—I want to come back to this—one of the utilities had testified, I think, if I remember correctly, they had discovered that they have somewhere in the area of 312,000 embedded chips somewhere in their whole system. And you touched on that. How serious do you believe that problem is?

They are confident that they have enough backup systems, or even if one should cause a problem somewhere, that it will not cause a major disruption. From your perspective, do you have any idea how big the embedded chip problem is for the Federal Government and are things being done about it?

Mr. KOSKINEN. Well, fortunately, from sampling the Federal Government, the embedded chip problem is primarily an operational issue, and other than the Defense Department and running a few power plants, the government is primarily engaged in information and data exchange and, the financial exchange software side of the issue. But it is a major issue. Depending on who you ask, there are 40 to 50 billion chips out there, loose or tied down, in the world.

Last week, the North American Electric Reliability Council issued its second assessment of the electrical power industry, and they are obviously, as noted, focused on this. They had a lot of concerns in their first assessment, released last fall, about the scope of the embedded chip problem. The report last week revealed that fortunately it turns out the number the chips that actually have the problem in power production or distribution is relatively small, and most of them would not shut down the power plant; they

would create problems in bookkeeping and recordkeeping and other issues. And the NERC is confident that information is now available and is being shared within the industry.

So that in the power industry, while there are a large number of chips out there—in terms of thousands per company and probably billions in the industry generally—companies are beginning to address the problem effectively. And at this point, the industry does not view it as being an insurmountable obstacle or a major threat to them, although it is going to take a lot of work.

Mr. GUTKNECHT. Let me just come back to one last point before my time expires here.

You have stated you will be in crisis management in 1999?

Mr. KOSKINEN. Right.

Mr. GUTKNECHT. Judging by your general demeanor, I find that hard to believe, or I should say, I am not certain anyone will really know, and I think thats good. I appreciate the fact that you are approaching this with a very calm demeanor.

Have you developed a crisis management strategy and, if so, how will you implement that? I mean, I am not really clear on what you mean by that.

Mr. KOSKINEN. Yes, I have been—I said we would go through and the council would go through a proselytizing, organizing phase into a monitoring and assessment phase, which is where we are now, and into a contingency planning, crisis management phase. We need to be prepared as we move through this year, and certainly as we move into January 1st to be prepared for whatever happens, domestically and internationally.

Our strategy across the board is to buildupon existing infrastructures and organizations and experiences. So we are forming a coordinating center for the Federal response to this issue, whatever it might be, which will build on the existing work of FEMA domestically, the State Department and the Treasury and the Defense Department internationally, along with the intelligence community, and that would be built into the Federal level. We are working with State and local governments. Tomorrow, with the Senior Advisors Group, will begin discussing with them the status of industry-wide plans, industry by industry, for their own emergency responses.

All of that will be integrated, so we will know if somebody has a water treatment problem or a power plant problem where the resources are in the private sector, to deal with that issue. There will be data bases available and inventories of the resources done, and with a little luck, we will have a very effective structure that won't have much of a challenge.

But what we have to be prepared for in terms of dealing with those crises and what the public needs to have confidence in is, in the fact that we are prepared for whatever will happen.

Mr. GUTKNECHT. Thank you.

Mr. HORN. I thank the gentleman, and now call on the delegate from the District of Columbia, Ms. Norton.

Ms. NORTON. Mr. Chairman, I want to—despite the fact that I have been delayed in getting here, I certainly want to commend and thank you for starting this session off right with a Y2K Federal Government hearing.

I just want to say to my colleague, John Koskinen—who has always been unflappable ever since we were in law school together, so I am not surprised he remains unflappable in the wake of this problem—that under his leadership, I am absolutely confident it is being solved.

I do want to thank the Federal Government, as well, for its assistance to the District of Columbia, which is going to be receiving some assistance as it readies itself for the Y2K problem. It is particularly important because the District government itself is being rebuilt and the District doesn't want to build into the Y2K problem, but just the opposite.

The question on crisis management, I think, is the one that is really in the—that you have just heard is Sputnik is in the back of everybody's mind that, yeah, all the big fellows do their jobs, but then somebody else doesn't, and there is some ripple effect and we all end up, God knows where.

I have two questions, and one is, I don't quite understand how anybody who does her job can control people who are not doing theirs when it comes to this problem. I just do not understand how that occurs. And I take it you could only safeguard yourself in case those who ripple down the line haven't done theirs. I would just like to get a few words on that. I apologize for being tardy; I might have missed something in that regard.

And, second, I would like to know how the government, whether the government has any posture it wants to take with respect to how ordinary citizens should respond to the independent operator analysts who are out there, some predicting the end of the world; and unfortunately, Y2K corresponds with the millennium, so there is a bunch of fools running around as well, and whether there is any—and any thought has been given to some kind of sane, reliable voice that people could turn to who aren't in this hearing, who haven't heard all the facts, so that as the time approaches, you won't have people hunkered down in their basements or—and please tell me now if you should have that—or gathering their food for the next year.

In other words, have you taken into account that a crisis mentality may be building up unless somebody hears from somebody they can trust?

Mr. KOSKINEN. All right. Well, the first question. Clearly that has been a challenge for us from the start. We are working with and trying to raise the level of awareness, activity, and compliance within organizations internationally, as well as domestically, over whom we have no authority at all. In fact, most of the people I spend my time with don't have to listen to me at all, and our goal and challenge has been to set up cooperative working relationships with them internationally and domestically.

And the good news is, thus far, certainly in the United States, we have had wonderful cooperation and response from every critical sector in the country and the major trade organizations. You are exactly right, this problem reveals the growing interconnectiveness of everything. That is why we started out saying even if we could get all the Federal systems done, it doesn't necessarily come close to solving the problem.

The reason I am spending all this time in all these other areas is because it is, in fact, an increasingly seamless web. And no one is an island unto themselves, either as an individual or a country or a city. And so we all have a great stake in everybody else's ability to deal with this problem. And the crisis management issue and the contingency planning we are asking all Federal agencies to engage in and encourage everybody in is to first take a look at doing the best they can to fix their problems, and second to have a backup program. If your systems don't all work, what will you do to keep your business operating, your government agency functioning; and what is your backup system if others you depend upon have systems that don't work.

In the Washington, DC area, in the last few days a lot of people obviously had to exercise backup plans when power that they relied upon was not available. With regard to public panic and public response, I think over time we will continue to provide the public with information and advice.

The Red Cross now has a very good Website that basically says that if you are worried about the year 2000 transition you should think of preparing as you would normally be prepared in the wintertime for a long weekend or a winter storm, and have a couple of days and water and food. But our view is that, at this juncture, there is no indication that you should disrupt your life.

And one of the things we need to do is to ensure the public is confident about our ability to deal with the problem. As you said, if we thought you ought to be hunkering down, we would be the first people to tell you, because I think the Federal Government has an obligation to give the people its best advice.

So on our hotline, as we move forward, we will continue to update the information we have and to provide advice to the public on what we think is an appropriate response. At this juncture our advice to the public is not to panic, not to go to New Mexico and buy a lot, and, in fact, primarily to be informed consumers of information, to pay attention, call our hotline, look at our Website. There will be plenty of time as the spring unfolds for all of us jointly to review that information and respond accordingly.

And we will be providing the public with updated information about what we think are the appropriate responses.

Mr. HORN. I thank the gentlewoman.

And now I yield to the gentleman from California, Mr. Miller, who has been long-suffering, waiting to get his questions in. And we finally made it, Gary.

Mr. MILLER. Well, thank you, Mr. Chairman.

It is a good feeling to be a new member and a freshman on a committee. And it is especially refreshing when you ask all the questions last, and all the good ones have been asked, and you are left with the other ones. But I look back at this and I have to praise the technology companies over the past years for getting this message out and creating the panic. You did a great job in driving the stock prices up. It really did; I invested in some of those companies.

And then the press further took those concerns and expanded upon them because they sell newspapers. And then I have listened to the questions presented by the knowledgeable and experienced

members on this committee, and they create more questions. I hate to fall into the category of those crazies we refer to out there, who look at panic and comply with that and become a part of it.

But there are some questions I guess I have never thought of until I listened to the questions asked today and the questions answered. One was the Y2K problem, many have said is going to be the end of the world as we know it; and the press did a good job of playing that up very well.

But I look at what we have done. Welfare reform is a good example. When the Federal Government enacted welfare reform, they turned it over to the States; and the States' and our job at this point is we turned it over to many counties. And counties also are responsible for Medicaid distribution and others.

And I guess I am concerned on the flow of technology to the States and substates who are fiscally impacted currently and counties, and most of our counties are fiscally impacted, especially California, and how the flow of technology gets to those counties, because now the counties are distributing the welfare funds that we provide to the States and the Medicare checks that are—Medicaid checks that are being given to them.

How do we ensure that there is an adequate flow not only to the States, but to the counties? Because by the time the flow of information gets to the States, they are dealing with their issues. How do we ensure that information also flows to the counties, who are actually providing most of the services that are being delivered today?

Mr. KOSKINEN. That is and has been one of our biggest challenges. I spent last summer at the National Association of Counties executive meetings, because in many ways the hardest people to get a hold of in this country are counties. They don't have a regular line of communication directly with the Federal Government, and in fact, the States told me when I started working with them last spring, counties don't want to hear anything from the Federal Government and they don't want to hear too much from the States. So there aren't regular, as you say, lines of communication.

We hope in response to your earlier question that we have done everything we can think of, but we are going to continue to work on it to get the information to the counties about the importance of the problem and ensure that they have access to technical information. With regard to State-run Federal programs, we are now going State by State to get assurances from the States as to the status of their preparedness; and to the extent they rely upon counties, information they have on county preparedness and what work they have been doing with counties.

And California has done a very good job. California held statewide meetings of county executives in major cities last year to start dealing with this problem. And, in fact, they and several other States have done that, Texas and others, we encouraged States to have that as a benchmark to follow.

There are some States where there is very little communication going on with their counties. And as I noted, I am concerned about that.

Again, I don't think we can mandate compliance across the board, but we can be very focused on at least the administration

of Federal programs. There are 160 Federal programs that are run by States and localities, and we need to continue to focus on them. And I think, as we go through the spring, that is going to be a growing problem for us, which is why I am delighted when there are regional and local hearings and town meetings. Because while we need to keep paying attention to how the Federal Government is doing, and it was an appropriate place to begin the dialog 3 or 4 years ago, it is increasingly clear to me that the problem is going to be at the State and local level if we are going to have a problem.

Mr. MILLER. Mr. Ose touched on an issue that has become a concern, and that is, we are asking people to share technology. The minute you do that there is liability risk associated with that sharing of technology. And I guess this question can be for the chairman, although, I think, more for him to think of in the future: What are we doing to cap the liability risk to encourage sharing of technology? I mean, I am sure in many cases organizations or groups will have the technology available, but they understand that clearly by them sharing that with others, they are at risk if there is a problem that occurs through that sharing of technology.

Are we doing anything in that fashion?

Mr. KOSKINEN. Yes. In my earlier discussions with the major industries, including telecommunications and securities, they were concerned about this issue. And, as I noted, last October the President signed into law legislation passed by Congress that protects not only companies, but trade associations who voluntarily disclose technical or other information about how they deal with this problem. It does not deal with the issue of those who are selling that service, and whether they can get insurance, but we have now removed the legal obstacles to information sharing. The interesting problem is—we are working with about 170 trade associations—many lawyers are still advising their clients not to say anything on the grounds that it will get them into trouble.

Mr. MILLER. That is where the problem is?

Mr. KOSKINEN. Yes. So in our working relationships with industry groups we are trying to figure out exactly how to break that barrier down, because you are exactly right, the exchange of that information is critical not only for large companies to compare test results, but it is critical information available to smaller and medium-sized organizations in the public and private sector, who can then go to that information and say—I haven't got a lot of time left, but I am told by those people that this is where I ought to spend my time and money and that is what I am going to do, and if they are wrong, at least I am better off than I would be otherwise.

Mr. MILLER. A closing question about maritime. And this is a question I hate to ask because maybe it is a little farfetched. Listening to the rumor, watching the press and the panic that could be created, we talked about printing available cash, but what impact might that have on our banks that have cash reserve requirements they have to meet, minimum requirements of standards? If this thing is blown out of perspective, that might impact that.

Are we doing anything to alleviate that impact?

Mr. KOSKINEN. Yes. We have—one of the reasons to have cash available is to ensure the banks don't run into difficulties. But again it goes into the balancing act I talked about and we have all

worried about for the last year. This is a serious problem, people have to pay attention, and we have to solve it. But on the other hand, if 200 million Americans decide to do anything very different economically than they normally do, that has the potential of being a self-fulfilling prophecy of a major problem, even if all the systems run fine.

So all of us have to try to deal with that problem. I am trying to make sure people address that problem, and understand the seriousness of it. But on the other hand, I do not want people to gratuitously decide, "Well, I think what I am going to do is not necessarily buy a lot in New Mexico, I will just take some money out of the markets, some money out of the bank, and go out and buy some extra supplies."

Mr. MILLER. We are going to address the reserve problems if that does occur?

Mr. KOSKINEN. If there is a reserve problem, the Fed is focused on it.

Mr. HORN. I thank the gentleman.

I see Mrs. Maloney, former ranking member of this Subcommittee on Government Management, Information, and Technology.

Would you have any questions to pose to our witnesses?

Mrs. MALONEY. Of course, Mr. Chairman, I congratulate you on your chairmanship, and I see you are on the case. We just got organized yesterday and you are already holding hearings.

And I just wondered—I thought it was very important that the President mentioned very, very strongly the Y2K problem and the attention that he and the Vice President and the administration are giving the problem in making sure that we are ready for the 21st century.

And I just want to know, in a brief oversight or review, do you think we are going to be ready? Do we have reason to be concerned? Could you just respond?

Really, I am sure you heard the President's speech last night, and I am sure you heard him talk about year 2000. I would just like to know in a general sense, where do we stand in the Federal Government?

I know you say some of the smaller governments are having some problems. What about internationally? Would you like to just give us a broad, brief overview of, do you think we are going to be ready? Are we going to meet the President's challenge of being ready and making sure that everything is working?

Mr. KOSKINEN. That is more than a 5-minute answer. My testimony is designed to deal with those issues. As a general matter, I think the Federal Government will be ready; I am confident of that. I think that the vast majority of States are doing a good job. I am concerned about local communities that may not be focused on the problem, but a lot of them have done that.

I am concerned about the risks of overreaction by the public, and internationally, I am concerned about the countries that have not yet paid enough attention to this problem and have the potential to create difficulties for the American economy and the American public.

Mrs. MALONEY. Well, since you seem to think that domestically we are all right, could you talk about the international problems

that you expect would possibly be the most problematic to the United States?

Mr. KOSKINEN. The most problematic to us and the largest challenges, I think, are in maritime shipping; and I think that not because I know there is a problem, but because I don't know what the information is, because there is no organized attack on that problem in that area yet.

I think that international financial transactions are generally in good shape. It will not be a problem for us. We are concerned about ensuring that in a lot of countries there are power supplies, particularly that those provided by Russian-made nuclear plants are safe and can operate as we go forward.

I think we will have, in some countries, difficulty getting telephone or other services. So I think, while it may not affect the American public generally, we will have an obligation to advise travelers about what they can expect in some countries and to work with American businesses operating abroad. At a minimum, we have to worry about how to run embassies and consulates in areas that may have difficulty with their infrastructure.

Mrs. MALONEY. Well, the chairman has had numerous——

Mr. HORN. That is panel 2, you know, on the international situation.

Mrs. MALONEY. Well, since he is here and he mentioned shipping, if I could ask him a brief question on that.

Mr. HORN. Sure.

Mrs. MALONEY. And I know, Mr. Chairman, you have had many, many hearings, and I congratulate you for being on the case.

But you express some concern on international shipping and that 95 percent of all goods that enter the United States are transported by ship. And specifically what are your concerns and why hasn't there been enough focus on this area, given the fact that 95 percent of all goods come by ship; and what can we do to change that so that the shipping or maritime industry will not be disrupted during this date change?

Mr. KOSKINEN. The U.S. Coast Guard has done an excellent job on their statistics for me, and they have been working very actively with American shipping interests in American ports. As I noted, there has been no organized global effort in this area. We are trying to solve that by, in fact, starting that effort in March, in London, with all the major international port and shipping associations dealing with this problem.

Certainly, when you look at oil or any other thing we rely on that comes from abroad you have to figure out, how do you get it out of the ground or out of the production mode to the port? How do you get it through the port and onto the ships? How do you get it across the oceans and into U.S. ports? That is a complicated supply chain, and we hope to have more attention paid to it.

The individual companies and major shippers, and certainly U.S. ones, have been paying attention to this, but again they do not control foreign port operations and often they do not control foreign production sources. We all need to see what we can do about that in the next 344 days.

Mrs. MALONEY. Well, my time is almost up. But I want to make sure the electricity is working on that day. I mean, we are going

to all need it. And the Secretary of Energy, Bill Richardson, publicly raised concerns earlier this month about electric utilities falling behind the Y2K repairs. A recent industry poll indicates that a number of utilities will not meet their June 30th deadline for compliance systems. And Secretary Richardson indicated that he may name specific firms if sufficient progress is not achieved.

Should other Cabinet secretaries follow this approach for vital industry sectors and businesses that are not on track for the Y2K, compliant with public health and safety, and does the Y2K Council have any plans to release the names of companies that are likely to miss Y2K deadlines?

Mr. KOSKINEN. We do not have that information. In fact, the act that was passed allows us to collect industry association information and industry information by protecting individual companies from having anybody reach that data, so that companies will be candid about it. But one of the reasons the North American Electric Reliability Council has 96 or 98 percent participation is that they have listed everybody who participated in their survey, which drove a lot of people to participate. We are going to encourage other industry groups to do that. This way the public will know which companies are actually providing the information and participating in the surveys.

With electric power, I think it is important to note that what the Secretary is concerned about is a small percentage of the power companies. The industry has a June 30 goal to have everything done; it is not a question of those companies not meeting the January 1, 2000 goal. And I think it is appropriate for all of us, as I say, to know as the Secretary said, there are no show stoppers and there will not be national issues. But it is also appropriate for us to be concerned about our local power companies. And we in Washington are concerned about, how will Pepco and Virginia Power deal with it, and we won't find that out from the national assessment.

We need to find that out, and those companies need to be forthcoming across the countries locally. We are going to try to do what we can to encourage that.

Mrs. MALONEY. I thank you for your testimony and for your public service. I can see why the President called you back into public service to work on this critical problem for the country. And I appreciate your willingness to serve and for being here today. Thank you.

Mr. KOSKINEN. Thank you.

Mr. HORN. In rounding this out, I am going to yield myself 5 minutes, which I have not taken. And let me just ask three fast questions.

During our staff research, we found that the police departments have not been too proactive on assessing the Y2K status of the 911 systems.

Do you have any information? Have any of your staff taken a look at that problem?

Mr. KOSKINEN. Yes. In the Emergency Services Working Group we are reaching out to—there is a group of people who run 911 systems, there is an association, and our Emergency Services Working Group is reaching out to get an assessment from them of that prob-

lem. FEMA and the Justice Department are working with State and local emergency managers to get people to understand they need to look at it.

The 911 systems are at risk. They are generally increasingly sophisticated computer operations that have problems, and we are concerned about that.

Mr. HORN. In terms of your plans with reference to Federal agencies, are you assured in your mind that all of them will meet the January 1, 2000, deadline?

Mr. KOSKINEN. I am.

Mr. HORN. You are?

Mr. KOSKINEN. Yes.

Mr. HORN. What makes you so optimistic?

Mr. KOSKINEN. I don't view it as optimism. I have actually spent since May——

Mr. HORN. I know you are a happy personality.

Mr. KOSKINEN. I am a very happy person. I should start frowning more when I say we have big problems. I have been meeting with all of the OMB tier 1 agencies and their senior managers on a monthly basis since May and monitoring their progress, as OMB has been doing and ensuring. I am confident at this juncture, and have been for some time, that the Secretaries of each of those agencies is personally committed to dealing with that problem.

I met yesterday at the Energy Department with Secretary Richardson and his senior staff as part of my monthly surveys, and they are making strong progress. I am confident that the information is generally accurate, because as I have said, if agencies wanted to make up the numbers, they would have figured out how to do that a couple of years ago, and they wouldn't have had either negative reports from you or OMB.

It has taken a lot of work. It is a great tribute to phenomenal efforts by Federal employees in all of those agencies. And I am, as I say, confident on the basis of the progress they are making and the reports that are coming out—and I think you are going to see in, as I noted in my testimony, the major agencies we are all concerned about by the time we get to the March 31 deadline, that substantial progress has been made over the last 6 to 9 months. And it has come with a lot of prodding and encouragement from all of us.

And as I have said in my prepared testimony, I think we all have to be prepared to acknowledge that accomplishment, just as we have been prepared to encourage them to move forward. Because a lot of employees are working around the clock, they are working weekends, they are dedicated to making sure that their agencies can perform their missions.

Mr. HORN. What legislation do you feel the administration should be recommending and Congress acting on that relates to Y2K? What is needed now to be helpful in the next phase?

Mr. KOSKINEN. We have asked the President's Council and the agencies to provide us any legislative needs they have, either for expanded authority or limited authority in particular areas. At this juncture, we do not have a major legislative request or initiative that we can see.

The emergency funding has been a significant help for us and a major issue. We are listening and trying to learn more about what the concerns are in the private sector on liability, but at this point, there is not a coordinated industry response in that area. But in terms of specific agency responsibilities, the only issue we are looking at that may require legislation is what, if anything, should we do around the January 1 weekend.

There have been issues raised about whether or not to move the holiday and whether we can allow people to move payments from the first week in January to the last week in December to take pressure off systems. If you do that and want to keep it as year 2000 income, you need a tax policy or a tax change. We have a task force, led by the Federal Reserve actually and all the agencies, looking at that. I think we will not recommend a holiday change, but we have other recommendations in terms of technically allowing companies and certainly Federal agencies to try to take pressure off their systems and that may take legislation. But other than that, I think our problem is primarily management and administration.

Mr. HORN. Well, I agree with that, with over the years, and my own feeling was, last fall, as you know, I was not keen on any legislation relating to liability at this point. I wanted everybody to get out there, provide leadership, get the job done and quit worrying about it. And I felt a lot of people had been misadvised by saying, Don't say anything, Chief; then they can't sue you.

Well, it seems to me if you don't say anything and don't provide the leadership, they will sue you.

Mr. KOSKINEN. Exactly.

Mr. HORN. So we are now, though, into another era, and the question is, should liability legislation be developed to either get a specialized court that would really know something about computing and the whole history of it, or do some other things that would limit the liability if good-faith efforts have been made.

Do you have any reaction to that?

Mr. KOSKINEN. At this point we do not have a position. As I say, at this juncture, we do not have any proposals or any view that there is a need for legislation. But we are—we are cognizant of the fact that a wide range of people are focused on it, and we are prepared to listen to what they have to say.

Mr. HORN. OK. I am going to yield back the rest of my time, so if Mr. Turner, as ranking member, has any questions—feel free—Mrs. Morella, as co-chair, has any questions, fine.

Or we can send him down and have the staff and you answer them and put it in the record at this point.

So whatever your wishes are. We have two more witnesses and two major topics to go into.

Mrs. MORELLA. Just briefly. You are going to love the legislation that I am going to ask you to look at. It is not liability, because I recognize the difficulty of coming up with something, particularly at this point, that is going to cover the liability system, but it would help to provide for the acceleration of business continuity plans, et cetera, and for more openness.

I want to ask you, have you thought about doing any PSAs, because another part of this bill would have to do with letting con-

sumers know what they should be asking, kind of reaction plans. But it just seemed to me it would just be a great opportunity to do some PSAs to alert the public, as well as the businesses, about the——

Mr. KOSKINEN. We for some months have been looking at what the appropriate Federal role should be in that area. The Advertising Council early on told us the programs they generally work with have a 5-year time horizon and, therefore, the short-term nature of the Y2K problem didn't fit within the 5 year timeframe.

The other problem with PSAs, by themselves, if they are free, they usually run late at night and at odd times. We have actually talked with public relations and advertising firms about, what it would take if you mounted a full-scale program; and in some detail, we have had proposals to spend $50 to $100 million. As I said, I am not quite sure how to explain to you or the public that I spent $100 million on an advertising program, as opposed to giving the money to people locally to solve their problems.

One of the things we hope to explore with our Senior Advisors Group and the working groups is to see what the private sector is doing in terms of both research about the problem and their media campaigns, and take a look at what the appropriate integration of a Federal response to that ought to be.

In the meantime, we are spending a lot of time with the press responding to all of the inquiries. We have yet to turn anybody down. But it is a very important point, and we are trying to figure out what is the most effective way to get information into the hands of the public. And to the extent that it—and we can find an effective role for the Federal Government and even the expenditure of some money integrated into the messages that others are providing, we will do that and be pleased to share it with you.

But at this juncture no one has been able to convince me yet that it is the right of priority for us to independently be spending phenomenal amounts of money.

Mrs. MORELLA. No, but you know, PSAs, as you say, they have to do it, the media; and I just think that you can get television and radio—it won't all be at 2:30 a.m. Besides, there are a lot of people who listen at this time and watch anyway. But I think they would use it at various other times during the day.

I think you should consider that in other ways also of communicating this. Don't be an alarmist, but don't be a Pollyanna, you know, I mean that kind of thing.

I know that—I don't want to take more time, because we have got two more panels. But I think it is always a shame that a person like you can't be there when the other two panelists are talking so you can respond, because I have already read much of that testimony. And, you know, we are talking about trade, we are talking about commerce, a suggestion from Mr. Willemssen that maybe we prioritize, your council prioritize what the United States needs, in terms of oil, in terms of food and commodities; and then have plans to make sure that we are going to receive it, the early warning system, that this is from the National Intelligence Council. Mr. Gershwin talks about Russia and China and early warning systems.

And then I also wonder about, in the United States, our own—the money we transmit for Medicare, Medicaid, for all kinds of things, student loans and all—have we, have we traced any of that money to the States and the localities to find out whether they are compliant? What I am saying is, a steady stream—the hip bone connected to the thigh bone connected to the knee bone—have we made these agencies that dole out this money find out from their recipients whether they are ready?

In other words, say you are part of our food chain of the line; do you see what I am getting at?

Mr. KOSKINEN. Yes. Let me first say to your general concern, Mr. Gershwin is an active member of the President's Council. We are working very closely with the National Intelligence Council on this matter, so I think I am very well versed on where he is. And Mr. Willemssen and I show up in a lot of places together. And actually, once a month GAO, Mr. Willemssen and Mr. Dodaro and others and I sit down and spend an hour or two reviewing where we are and their recommendations on what we are dealing with. So I think I am well advised about what their suggestions are.

And, as always, we have found that GAO's suggestions are particularly helpful. And as you will note, over time, a lot of those suggestions have been accepted and integrated into either the OMB work or our work.

Mrs. MORELLA. The recommendation is great. But I mean in terms of the action beyond the recognition. I know you are working very hard; I commend you for what you are doing. It is just, I do think they offer some good recommendations that need some action. Thank you.

Thank you, Mr. Chairman.

Thank you, Mr. Koskinen. I look forward to meeting with you.

Mr. HORN. Mr. Turner, any questions?

Mr. TURNER. Mr. Chairman, maybe just a couple.

Chairwoman Morella expressed an interest in PSAs, and I was just looking at the latest report from OMB to this committee regarding the estimated cost to the Federal Government of complying with Y2K, and I believe it says it is close to $6.5 billion.

Mr. KOSKINEN. Correct.

Mr. TURNER. Maybe $100 million, if it would be profitable and helpful, might not be that large a sum in the scheme of things.

My concern, as I shared with you earlier, is that I certainly want to be very careful about what PSAs we are airing, because it is hard, I am sure, to judge whether PSA's are going to increase public comfort or discomfort with the problem.

One of the things that I wanted to ask you about is that a year ago people were saying there just aren't enough computer programmers out there to help us comply with this problem, and we are going to have to figure out how to find some folks and get them trained. You don't hear a lot about that anymore.

What is the status of the necessary personnel to solve Y2K?

Mr. KOSKINEN. It is a problem we are all concerned about; as a potential problem, we have been monitoring it very carefully with the Federal Government. One of the first things we did when I started was to have OPM authorize the agencies to bring back an-

nuitants, retirees, who knew about these kinds of issues without forcing them to give up their retirement benefits.

What has happened, while the cost has gone up in the private sector, to some extent for services, which generally happened, I think, as we monitored—and the reason there hasn't been a national shortage is that the tools and the techniques for dealing with this problem have increased at about the same rate as the demand, so that the original assumptions—where you would have to take each line of code and change it—and people then started multiplying out how long it took and how many billion lines of code there were, it turned out there have been a lot of what are called "windowing techniques" that allow you to adjust for the problem without necessarily changing all the programmatic codes.

Also, while there is no silver bullet, there are a wide range of tools that, depending on the software programs and the operations, that have speeded up the process for either finding out where the problems are or testing against them.

There have been some anecdotal reports of shortages. GAO again did a review of the agencies and found some specific areas and pockets of concern. But as a general matter, the Federal Government has not found that it or its contractors have had trouble getting enough personnel. And even in the private sector, we have not yet seen major shortages occur.

And I think it is primarily not because people are wrong in the concern; I think it is because everybody has gotten a lot better at figuring out how to get the work done efficiently.

Mr. TURNER. Thank you.

Thank you, Mr. Chairman.

Mr. HORN. Vice Chair Biggert, any last questions?

Mrs. BIGGERT. No.

Mr. HORN. OK. We will now move to the second panel.

And we thank you very much for spending the time with us. I never—I know you will never not answer a question. You answer it eloquently. You answer it very speedily.

Mr. KOSKINEN. Thank you, Mr. Chairman, and Chairman Morella. I do appreciate your ongoing support.

Mr. HORN. If you can stay a little, we would welcome anything you want to say.

Mr. KOSKINEN. Thank you, but as you can imagine what my life is like, right now I am almost late for my next meeting.

Mr. HORN. If panel 2 would come forward, please.

We have, on panel 2, Dr. Lawrence Gershwin, National Intelligence Officer for Science and Technology of the National Intelligence Council. This is Dr. Gershwin. And then you are accompanied by Norman Green, Deputy National Intelligence Officer for Science and Technology. So can we have him take a seat also?

I am going to swear you all in, since one of you will be talking probably somewhere along the line. Dr. Michael Harrington, principal technical staff—and tell me how to pronounce it; is it the MITRE Corp., is that the best way——

Dr. HARRINGTON. Yes.

Mr. HORN [continuing]. And Mary Walsh, Year 2000 Issues Manager, Directorate of Intelligence, Central Intelligence Agency.

Come on up, get chairs here. Will the staff make sure that we have enough chairs or just grab one. And Joel Willemssen, our favorite witness here, Director of Civil Agencies Information Systems, Accounting and Information Management Division, General Accounting Office.

So have we got everybody a seat?

[Witnesses sworn.]

Mr. HORN. The clerk will note that all five witnesses have affirmed the oath.

And we are now going to begin with Dr. Lawrence Gershwin, National Intelligence Officer for Science and Technology at the National Intelligence Council. You might tell us the formation of the National Intelligence Council, just for the record.

STATEMENTS OF LAWRENCE K. GERSHWIN, Ph.D., NATIONAL INTELLIGENCE OFFICER FOR SCIENCE, ACCOMPANIED BY NORMAN GREEN, DEPUTY NATIONAL INTELLIGENCE OFFICER FOR SCIENCE AND TECHNOLOGY, NATIONAL INTELLIGENCE COUNCIL; MICHAEL HARRINGTON, Ph.D., PRINCIPAL TECHNICAL STAFF, MITRE CORP.; MARY WALSH, YEAR 2000 ISSUES MANAGER, DIRECTORATE OF INTELLIGENCE, CENTRAL INTELLIGENCE AGENCY; AND JOEL WILLEMSSEN, DIRECTOR OF CIVIL AGENCIES INFORMATION SYSTEMS, ACCOUNTING AND INFORMATION MANAGEMENT DIVISION, GENERAL ACCOUNTING OFFICE

Dr. GERSHWIN. Sure. The National Intelligence Council works for the Director of Central Intelligence as an interagency intelligence mechanism. And our purpose is to bring together the work of all of the intelligence agencies into one unified set of analyses for the purpose of serving the Director of Central Intelligence in his overall role as manager of the entire intelligence community.

And as such, I am 1 of the 12 National Intelligence Officers on the council. And our job is, of course, to work certain areas, and in my case, science and technology issues, for the Director of Central Intelligence.

Mr. Chairman, Mrs. Morella, I am pleased to be able to discuss today the understanding that the intelligence community has about foreign efforts to deal with the Y2K problem. I will give you our current assessment of where we see the problems as most likely to occur. But we are not yet in a position to make a confident assessment of the global impacts of the likely Y2K failures or the implications for U.S. interests.

The Y2K situation is very fluid, and our assessments could change significantly over the next several months as more information becomes available, as countries become more aware of and deal with Y2K issues, and as incidents of Y2K failure increase. I will highlight for you today those areas that we think have a significant chance of affecting U.S. interests.

All countries will be affected to one degree or another by Y2K-related failures, and problems in one country sector can have widespread consequences because of interdependence between sectors worldwide. The consequences of Y2K failures abroad will range from the relatively benign, such as a localized inability to process credit card purchases, to problems within systems across sectors

that will have humanitarian implications, such as power loss in midwinter.

We have few indications that countries are today undertaking contingency planning for recovery from Y2K failures. Foreign countries trail the United States in addressing Y2K problems by at least several months and, in many cases, much longer.

Y2K remediation is underfunded in most countries, and time and resource constraints will limit the ability of most countries to respond adequately by 2000. Governments in many countries have begun to plan seriously for Y2K remediation only within the last year, some only in the last few months; and some continue to significantly underestimate the costs and time requirements for remediation and, importantly, testing.

Because many countries are way behind, testing fixes will come late and unanticipated problems typically arise in the testing phase. The largest institutions, particularly those in the financial sectors, are the most advanced in Y2K remediation. Small- and medium-sized entities trail in every sector worldwide.

Most countries have failed to address aggressively the issue of embedded processors. And while recent understanding is that failures here will be less than previously estimated, it is nevertheless the case that failure to address this issue will still cause some highly dependent sectors with complex sensor and processing systems to have problems centered right around the January 1st date.

The lowest level of Y2K preparedness is evident in Eastern Europe and Russia, in Latin America, in the Middle East, and Africa and several Asian countries, including China. But global linkages in telecommunications, financial systems, air transportation, the manufacturing supply chain, oil supplies, and trade mean that Y2K problems will not be isolated to these individual countries, and no country will be immune from failures in such sectors.

Regarding Russia and Ukraine, the coincidence of widespread Y2K-related failure is likely to occur in the winter of 1999 to 2000. With continuing economic problems and food shortages, already difficult conditions for the population could have major humanitarian consequences for those countries. While the Russian Government initiated centralized guidance to ministries and agencies in May 1998, the State committee responsible for initiating overall guidance has stated that there is not enough time or money to resolve the Y2K problem. We think they are right.

Russian estimates of the cost of remediation of their government system seem considerably less than Western estimates for comparable systems in other countries or what we regard as what it will cost in Russia. Thus far, both Russia and Ukraine have exhibited a low level of Y2K awareness and remediation activity. While Russia possesses a talented pool of programmers, they seem to lack the time, organization and funding to adequately confront the Y2K problem.

Concerns include problems with computer-controlled systems and subsystems within power distribution systems and nuclear power generating stations leading to reactor shutdowns, or improper power distribution resulting in loss of heat for indeterminate periods of time in the dead of winter in Russia and Ukraine. Indica-

tions point toward a slow, reactive mode of operations on the part of, for instance, the Russian Atomic Energy Ministry.

Although Western Europe is in relatively better shape than some of the regions I have cited earlier, European awareness of and concern about the Y2K problem is uneven, and they do lag the United States in fixing their problems.

I should point out that none of the countries that we are dealing with seem to have anything like the level of government-led activity, as we heard earlier from John Koskinen. And frankly it is that level of government activity and leadership on it that I think is required worldwide in all of these countries, including some of the more advanced countries in order to make this stuff work.

European attention was focused on modifying computer systems for the European Monetary Union conversion, which was implemented successfully on January 1, but this was done, in many cases, by postponing coming to grips with Y2K problems. For example, the Netherlands has expressed concern that the EU members are not working together to solve Y2K problems and has threatened to cutoff its own power grid from the rest of Europe in order to protect domestic power distribution from external problems.

The Asian economic crisis has hampered the Y2K remediation efforts of all of the Asia-Pacific countries except Australia. While the lines of authority for China's Y2K effort have been established, its late start in addressing Y2K issues suggest Beijing will fail to solve many of its Y2K problems in the limited time remaining and will probably experience failures in key sectors such as telecommunications, electric power and banking.

We are focusing increasingly in the intelligence community, in our own study of foreign Y2K problems, on those critical sectors that directly affect U.S. interests. These include, among others, foreign military systems, trade, and oil production and distribution, all of which I will elaborate on.

First, regarding military systems, military systems and their command and control are particularly information-technology dependent, and thus potentially vulnerable to disruption if Y2K problems are not adequately addressed. We have been especially attentive to the issue of foreign strategic missile systems, and particularly those in Russia and China, to experience Y2K-related problems. United States and Russian officials have been discussing these issues for some time now, and we do not see a problem in terms of Russian or Chinese missiles automatically being launched or nuclear weapons going off because of computer problems arising from Y2K failures.

Rather, the problem that we are more focused on is whether the Russians will manage to locate and fix problems in their early warning systems that they use to monitor foreign missile launches and how their leadership is preparing to deal either with the prospect of incorrect information being provided by such systems or with system outages. The level of concern in Russia is growing on these issues as awareness of the nature of the Y2K problem grows.

Turning to world trade and oil, some of our most important trading partners have been documented by, among others, the Gartner Group, as behind the United States in fixing their Y2K problems. And China and Japan will be good examples. Significant oil export-

ers to the United States and the global market including a number of countries—Venezuela, Saudi Arabia, Mexico, Nigeria, Angola and Gabon—that are lagging in their Y2K remediation efforts.

Oil production is largely in the hands of multinational corporations in the oil-producing countries, but this sector is highly intensive in the use of information technology and complex systems using embedded processors, and is highly dependent on ports, ocean shipping and domestic infrastructures.

The oil industry is fraught with potential Y2K problems. Embedded microprocessors are found throughout the oil industry in drilling, pumping, transportation, processing and refining operations. A typical offshore platform or onshore gas plant reportedly uses 50 to 100 embedded systems, each containing up to 10,000 individual microchips.

While the industry has been actively involved in remediation, planning for remediation of a single offshore platform can reportedly involve up to 60 different vendors. We are concerned about the shipping of oil products, because ocean shipping and foreign ports have both been flagged as among the least prepared sectors.

One additional issue I want to raise is that many foreign officials and companies who are aware of Y2K problems are looking to the West, and particularly the United States, for help, and to western suppliers for technical solutions. In some cases, foreign companies or governments may blame the United States and other foreign vendors for problems in this equipment and thus seek legal redress for their failures. And worldwide litigation issues are quickly becoming a part of the Y2K international scene.

In closing, let me note that today we can list all the issues that concern us worldwide in terms of the impact of Y2K failures on infrastructures, economies, countries and regions, national security, trade and so on. But today we cannot yet provide good answers or predictions that would be meaningful on the consequences. We have cast a wide net for information on Y2K developments and are working very closely through the President's Council on Y2K Conversion, with the rest of the Federal Government. As the time for greater likelihood of failures comes nearer, awareness of and reporting of Y2K problems abroad should increase dramatically and we thus expect to have a much better handle on the type and extended failures we are likely to see around the world.

But the incredible complexity of global interconnectivity and interdependence, and the effects when some parts of the information technology baseline start to fail, is a daunting challenge to interpret and analyze. There will be many analysts in both public and private sectors here and abroad trying to make reasonable judgments about the consequences and implications. The problem is formidable, but we will do our best to support the U.S. Government in assessing these consequences. Thank you.

[The prepared statement of Dr. Gershwin follows:]

TESTIMONY OF LAWRENCE K. GERSHWIN,
NATIONAL INTELLIGENCE OFFICER
FOR SCIENCE AND TECHNOLOGY,
NATIONAL INTELLIGENCE COUNCIL

GOVERNMENT MANAGEMENT, INFORMATION AND
TECHNOLOGY SUBCOMMITTEE OF THE HOUSE GOVERNMENT
REFORM AND OVERSIGHT COMMITEE

January 20, 1999

Good morning, Mr. Chairman. I am pleased to be able to discuss with you today the understanding that the Intelligence Community has about foreign efforts to deal with the Y2K problem. I will give you our current assessment of where we see problems as most likely to occur, but we are not yet in a position to make a confident assessment of the global impacts of the likely Y2K failures, or the implications for US interests. The Y2K situation is very fluid, and our assessments could change significantly over the next several months as more information becomes available, as countries become more aware of and deal with Y2K issues, and as incidents of Y2K failure increase. I will highlight for you today those problem areas that I think have a significant chance of affecting US interests.

Fixing the Y2K problem is labor and time intensive, and challenging with respect to project management. Current Gartner Group estimates of global expenditures to fix the problem are on the order of one to two trillion dollars, which is about 3-5 percent on average of every country's annual gross domestic product. A wide range of modern information technology is potentially affected including operating systems or applications software that use dates or date-related transactions, and embedded microprocessors in such applications as energy, transportation, telecommunications, and manufacturing systems.

All countries will be affected--to one degree or another--by Y2K-related failures. Problems in one country or sector can have widespread consequences because of interdependence between sectors worldwide. The consequences of Y2K failures abroad will range from the relatively benign, such as a localized inability to process credit card purchases, to problems within systems across sectors that will have humanitarian implications such as power loss in mid-winter. We have few indications that countries are undertaking contingency planning for recovery from Y2K failures.

Foreign countries trail the United States in addressing Y2K problems by at least several months, and in many cases much longer. Y2K remediation is underfunded in most countries:

- Time and resource constraints will limit the ability of most countries to respond adequately by 2000.
- Governments in many countries have begun to plan seriously for Y2K remediation only within the last year, some only in the last few months, and some continue to significantly underestimate the cost and time requirements for remediation and, importantly, testing. Because many countries are way behind, testing of fixes will come late, and unanticipated problems typically arise in this phase.
- The largest institutions, particularly those in the financial sectors, are the most advanced in Y2K remediation. Small and medium-size entities trail in every sector worldwide.

- Most countries have failed to address aggressively the issue of embedded processors. While recent understanding is that failures here will be less than previously estimated, it is nevertheless the case that failure to address this issue will still cause some highly dependent sectors with complex sensor and processing systems to have problems, centered right on the January 1 date.
- The lowest level of Y2K preparedness is evident in Eastern Europe, Russia, Latin America, the Middle East, Africa, and several Asian countries, including China.

Global linkages in telecommunications, financial systems, air transportation, the manufacturing supply chain, oil supplies, and trade mean that Y2K problems will not be isolated to individual countries, and no country will be immune from failures in these sectors.

The coincidence of widespread Y2K-related failures in the winter of 1999-2000 in Russia and Ukraine, with continuing economic problems, food shortages, and already difficult conditions for the population could have major humanitarian consequences for these countries. While the Russian government initiated centralized guidance to ministries and agencies in May of 1998, the State Committee responsible for initiating overall guidance has stated that there is not enough time or money to resolve the Y2K problem. We think they're right. Russian estimates of the cost of remediation of their government systems seem considerably less than Western estimates for comparable systems in other countries. Thus far both Russia and the Ukraine have exhibited a low level of Y2K awareness and remediation activity. While Russia possesses a talented pool of programmers, they seem to lack the time, organization, and funding to adequately confront the Y2K problem. Concerns include problems with computer-controlled systems and subsystems within power distribution systems and nuclear power generating stations leading to reactor shutdowns, or improper power distribution resulting in loss of heat for indeterminate periods in the dead of winter in Russia. Indications point towards a slow, reactive mode of operations on the part of the Russian Atomic Energy Ministry.

Although Western Europe is in relatively better shape than some of the regions I have cited earlier, European awareness of and concern about the Y2K problem is uneven, and they do lag the United States in fixing their problems. European attention was focused on modifying computer systems for the European Monetary Union conversion, which was implemented successfully on 1 January, but this was done by, in many cases, postponing coming to grips with Y2K problems. For example, the Netherlands has expressed concern that the EU members are not working together to solve Y2K problems, and has threatened to cut off its power grid from the rest of Europe in order to protect domestic power distribution from external problems.

The Asian economic crisis has hampered the Y2K remediation efforts of all of the Asia-Pacific countries except Australia. While the lines of authority for China's Y2K effort have been established, its late start in addressing Y2K issues suggests Beijing will fail to solve many of its Y2K problems in the limited time remaining, and will probably experience failures in key sectors such as telecommunications, electric power, and banking.

We are focusing increasingly in our study of foreign Y2K problems on those critical sectors that directly affect US interests. These include, among others, foreign military systems, trade, and oil production and distribution, all of which I will elaborate on.

Military systems and their command and control are particularly information-technology dependent, and thus potentially vulnerable to disruption if Y2K problems are not adequately addressed. We have been especially attentive to the issue of foreign strategic missile systems, in particular those in Russia and China, to experience Y2K-related problems. US and Russian officials have been discussing these issues for some time now, and we do not see a problem in terms of Russian or Chinese missiles automatically being launched, or nuclear weapons going off, because of computer problems arising from Y2K failures.

The problem we are more focused on is whether the Russians will manage to locate and fix problems in their early warning systems that they use to monitor foreign missile launches, and how their leadership is preparing to deal either with the prospect of incorrect information being provided by such systems, or with system outages. The level of concern in Russia is growing as awareness of the nature of the Y2K problem grows.

Regarding world trade and oil: some of our most important trading partners have been documented by, among others, the Gartner Group, as behind the US in fixing their Y2K problems (China and Japan, for example). Significant oil exporters to the United States and the global market include a number of countries—Venezuela, Saudi Arabia, Mexico, Nigeria, Angola, and Gabon—that are lagging in their Y2K remediation efforts. Oil production is largely in the hands of multi-national corporations in the oil-producing countries, but this sector is highly intensive in the use of information technology and complex systems using embedded processors, and is highly dependent on ports, ocean shipping, and domestic infrastructures.

The industry is fraught with potential Y2K problems. Embedded microprocessors are found throughout in the oil industry in drilling, pumping, transportation, processing, and refining operations. A typical offshore platform or onshore gas plant reportedly uses 50-100 embedded systems, each containing up to 10,000 individual microchips. While the industry has been actively involved in remediation, planning for remediation of a single offshore platform can reportedly involve up to 60 different vendors. We are concerned about the shipping of oil products, because ocean shipping and foreign ports have both been flagged as among the least prepared sectors.

One additional issue I want to raise is that many foreign officials and companies who are aware of Y2K problems are looking to the West, and particularly the United States, for help, and to Western suppliers for technical solutions. In some cases, foreign companies or governments may blame the United States and other foreign vendors for problems in equipment and thus seek legal redress for their failures. Worldwide litigation issues are quickly becoming a part of the Y2K scene.

In closing, let me note that today we can list all the issues that concern us worldwide, in terms of the impact of Y2K failures on infrastructures, economies, countries and regions, national security, trade, and so on. But today we cannot yet provide good answers or predictions that would be meaningful on the consequences. We have cast a wide net for information on Y2K developments and are working very closely, through the President's Council on Year 2000 Conversion, with the rest of the federal government. As the time for greater likelihood of failures comes nearer, awareness of, and reporting on Y2K problems abroad should increase dramatically, and we thus expect to have a better handle on the type and extent of failures we are likely to see around the world.

But the incredible complexity of global interconnectivity and interdependence, and the effects when some parts of the information technology baseline start to fail, is a daunting challenge to interpret and analyze.

There will be many analysts, in public and private sectors, here and abroad, trying to make reasonable judgments about the consequences and implications. The problem is formidable, but we will do our best to support the US government in assessing these consequences.

Mr. HORN. We thank you for that very helpful statement, and we will now go to Mr. Willemssen.

Mr. WILLEMSSEN. Thank you, Mr. Chairman, Chair Morella, Ranking Member Turner, Congresswoman. Thank you for inviting us here to testify today on Y2K.

I will briefly summarize our statement on, one, where the Federal Government stands, issues confronting State and local governments, and the readiness of key infrastructure and economic sectors. And in doing so, I will focus on suggestions we have for Mr. Koskinen and OMB to improve its oversight of these areas.

First, regarding the Federal Government. While the most recent November quarterly reports show improvement in addressing Y2K, many agencies still have a long way to go. We have a number of suggestions for Mr. Koskinen and OMB to consider in this area.

First, on reporting of Y2K progress. OMB's draft guidance to agencies for the upcoming February quarterly reports asks agencies to identify and report on their core business functions that are to be addressed in their business continuity and contingency plans. We endorse this initiative. In fact, OMB could go a step further and use this information to ask agencies to report on their end-to-end testing and contingency plans for these critical functions.

For example, with the time available for end-to-end testing diminishing, OMB should consider for the government's most critical functions setting target dates and having agencies report against them for the development of end-to-end test plans, the establishment of test schedules, and the completion of those tests.

For business continuity and contingency plans, OMB could consider setting a target date such as April 30th for the completion of those plans, and a date such as September 30th for completing testing of those plans.

Another key task that could be aided by identifying the government's core business functions is setting priorities. Having this information in hand provides an opportunity to ensure that the most important areas will be addressed; namely, those affecting health and safety, national defense, adverse financial impact to the citizen and adverse economic impact. This would enable agencies and OMB to report in 1999, after March 31, on the Y2K compliance of business functions, not individual systems. And, really, that is the bottom line of what we are trying to accomplish here, is business functions being Y2K compliant, not individual systems.

Another key element of a business continuity and contingency plan is the development of a zero day, or day one strategy for the period in late December 1999 and early January 2000. The Social Security Administration, a recognized Federal leader on Y2K, has developed such a strategy. Among the features of that strategy is a moratorium on software changes for the last few months of 1999 and first few months of 2000. Because this type of action can reduce agencies' risks, we think OMB may want to consider requiring other agencies to also take this kind of initiative.

Turning next to State and local governments. They face a major risk of year 2000-induced failures to the many vital services they provide. The report we issued in November on State systems used in Federal welfare programs revealed that the majority of those

systems were not compliant. For example, States told us that only about 16 percent of Medicaid systems were compliant.

The extent of information available to the public on State and local year 2000 readiness, however, varies considerably. For example, while some State and local governments provide detailed year 2000 readiness information on their Websites, others provide very limited data. We think that States that are providing detailed data are doing their citizens a service in letting them understand what kind of progress is being made.

Accordingly, we think another initiative that Mr. Koskinen's council could undertake is developing and distributing to State and local governments a template that identifies the types of year 2000 information that the entity could disclose to the public. Disclosure of such information could reduce the public's concern and potential panic over potential disruptions caused by Y2K.

Turning last to the key infrastructure and economic sectors, we believe Mr. Koskinen and his council are to be commended on the strides they have made over the last several months in this area. However, to enhance the further availability of information on sector Y2K readiness and to further reduce likelihood of major disruptions, we offer some additional suggestions for Mr. Koskinen.

First, the Council must continue to aggressively pursue readiness information in the areas in which it is lacking, such as the health sector and local law enforcement. If the current approach of using associations to voluntarily collect information does not work, the Council may have to consider other legislative remedies such as requiring such disclosure, especially where it is important in certain infrastructure areas.

Second, to encourage the reporting of more complete information, the Council should consider requesting that all the national associations publicly disclose, at a minimum, those companies that have responded to surveys.

Third, for the next report of the Council scheduled in April, we would urge the Council to include key data to help evaluate the readiness of sectors and to identify each sector's major components and its readiness.

And last, since the international arena, as we have heard, carries some of the greatest risks and uncertainties, the Council could consider prioritizing those trade and commerce activities that are most critical to our Nation's well-being and identify alternative options to obtain needed materials, should the need arise.

That concludes a summary of my statement, and I would be pleased to address any questions that you may have.

[The prepared statement of Mr. Willemssen follows:]

United States General Accounting Office

GAO

Testimony

Before the Committee on Government Reform and the Committee on Science, House of Representatives

For Release on Delivery
Expected at
11:15 a.m.
Wednesday,
January 20, 1999

YEAR 2000 COMPUTING CRISIS

Readiness Improving, But Much Work Remains to Avoid Major Disruptions

Statement of Joel C. Willemssen
Director, Civil Agencies Information Systems
Accounting and Information Management Division

GAO/T-AIMD-99-50

Messrs. Chairmen and Members of the Committees:

Thank you for inviting us to participate in today's hearing on the Year 2000 problem. According to the report of the President's Commission on Critical Infrastructure Protection, the United States--with close to half of all computer capacity and 60 percent of Internet assets--is the world's most advanced and most dependent user of information technology.[1] Should these systems--which perform functions and services critical to our nation--suffer problems, it could create widespread disruption. Accordingly, the upcoming change of century is a sweeping and urgent challenge for public- and private-sector organizations alike.

Because of its urgent nature and the potentially devastating impact it could have on critical government operations, in February 1997 we designated the Year 2000 problem as a high-risk area for the federal government.[2] Since that time, we have issued over 70 reports and testimony statements detailing specific findings and recommendations related to the Year 2000 readiness of a wide range of federal agencies.[3] We have also issued guidance to help organizations successfully address the issue.[4]

Today I will highlight the Year 2000 risks facing the nation; discuss the federal government's progress and remaining challenges in correcting its systems; identify state and local government Year 2000 issues; and provide an overview of the available information on the readiness of key public infrastructure and economic sectors.

---

[1] Critical Foundations: Protecting America's Infrastructures (President's Commission on Critical Infrastructure Protection, October 1997).

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

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

[4] Year 2000 Computing Crisis: An Assessment Guide (GAO/AIMD-10.1.14, issued as an exposure draft in February 1997 and in final form in September 1997), which addresses the key tasks needed to complete each phase of a Year 2000 program (awareness, assessment, renovation, validation, and implementation); Year 2000 Computing Crisis: Business Continuity and Contingency Planning (GAO/AIMD-10.1.19, issued as an exposure draft in March 1998 and in final form in August 1998), which describes the tasks needed to ensure the continuity of agency operations; and Year 2000 Computing Crisis: A Testing Guide (GAO/AIMD-10.1.21, issued as an exposure draft in June 1998 and in final form in November 1998), which discusses the need to plan and conduct Year 2000 tests in a structured and disciplined fashion.

THE PUBLIC FACES RISKS OF
YEAR 2000 DISRUPTIONS

The public faces a risk that critical services provided by the government and the private sector could be severely disrupted by the Year 2000 computing problem. Financial transactions could be delayed, flights grounded, power lost, and national defense affected. Moreover, America's infrastructures are a complex array of public and private enterprises with many interdependencies at all levels. These many interdependencies among governments and within key economic sectors could cause a single failure to have adverse repercussions in other sectors. Key sectors that could be seriously affected if their systems are not Year 2000 compliant include information and telecommunications; banking and finance; health, safety, and emergency services; transportation; power and water; and manufacturing and small business.

The following are examples of some of the major disruptions the public and private sectors could experience if the Year 2000 problem is not corrected.

- With respect to aviation, there could be grounded or delayed flights, degraded safety, customer inconvenience, and increased airline costs.[5]

- Aircraft and other military equipment could be grounded because the computer systems used to schedule maintenance and track supplies may not work. Further, the Department of Defense could incur shortages of vital items needed to sustain military operations and readiness.[6]

- According to the Basle Committee on Banking Supervision--an international committee of banking supervisory authorities--failure to address the Year 2000 issue would cause banking institutions to experience operational problems or even bankruptcy.

- Medical devices and scientific laboratory equipment may experience problems beginning January 1, 2000, if their software applications or embedded chips use two-digit fields to represent the year.

Recognizing the seriousness of the Year 2000 problem, on February 4, 1998, the President

---

[5]FAA Systems: Serious Challenges Remain in Resolving Year 2000 and Computer Security Problems (GAO/T-AIMD-98-251, August 6, 1998).

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

signed an executive order that established the President's Council on Year 2000 Conversion led by an Assistant to the President and consisting of one representative from each of the executive departments and from other federal agencies as may be determined by the Chair. The Chair of the Council was tasked with the following Year 2000 roles: (1) overseeing the activities of agencies; (2) acting as chief spokesperson in national and international forums; (3) providing policy coordination of executive branch activities with state, local, and tribal governments; and (4) promoting appropriate federal roles with respect to private-sector activities.

MUCH WORK REMAINS TO ADDRESS THE FEDERAL GOVERNMENT'S YEAR 2000 PROBLEM

Addressing the Year 2000 problem 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.

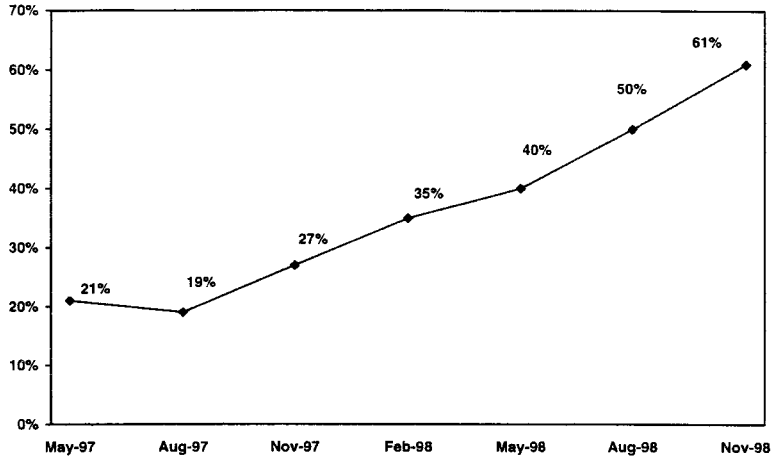
To meet this challenge and monitor individual agency efforts, the Office of Management and Budget (OMB) directed the major departments and agencies to submit quarterly reports on their progress, beginning May 15, 1997. These reports contain information on where agencies stand with respect to the assessment, renovation, validation, and implementation of mission-critical systems, as well as other management information on items such as business continuity and contingency plans and costs.

Latest Quarterly Reports Show Some Improvement, But More Work Is Needed

While the federal government's most recent reports show improvement in addressing the Year 2000 problem, 39 percent of mission-critical systems were reported as not yet compliant. As chart 1 illustrates, in May 1997, OMB reported that about 21 percent of the mission-critical systems (1,598 of 7,649) for the 24 major departments and agencies were Year 2000 compliant.[7] Eighteen months later, OMB reported that, as of mid-November 1998, 4,069 of the 6,696 mission-critical systems in their current inventories, or about 61 percent, were compliant.

[7]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.

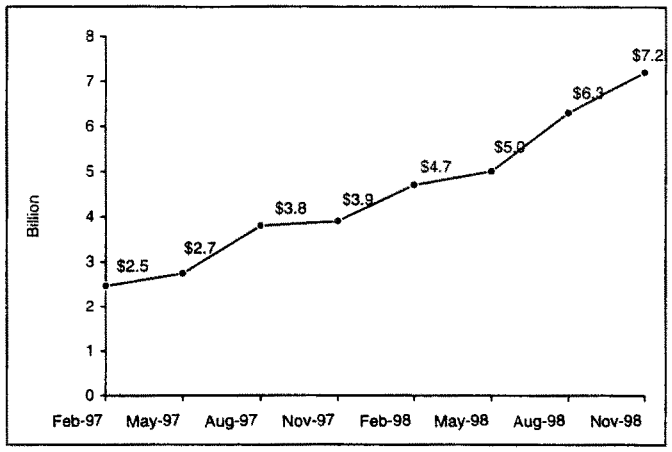
Chart 1: Mission-Critical Systems Reported Year 2000 Compliant, May 1997-November 1998



Source: OMB quarterly reports

As federal agencies have more fully realized the complexities and extent of Year 2000 activities, estimated costs have also continued to rise. As chart 2 illustrates, since February 1997, the federal government's Year 2000 cost estimate has more than tripled.

Chart 2: Federal Government's Year 2000 Estimated Costs (in billions)



Note: The August 1998 figure of $6.3 billion and the November 1998 figure of $7.2 billion are the totals of all individual submissions from the 24 major departments and agencies that were generally submitted on August 14th and November 13th, respectively. In its summaries of the agency reports, OMB reported the government's total estimated Year 2000 costs as $5.4 billion and $6.4 billion, respectively. For the August 1998 costs, OMB did not include all costs in its estimate because, for example, it was still reviewing some of the estimates provided by the agencies. For the November 1998 costs, OMB did not provide explanations in its report for the discrepancies between the agency reports and its estimates for 15 of the 18 agencies with differences.

ource: February 1997 data is from OMB's report Getting Federal Computers Ready for 2000, February 6, 1997. May 1997 to May 1998 data are from OMB's quarterly reports. The August and November 1998 data are from the quarterly reports of the 24 major federal departments and agencies.

In addition, many agencies have not met, or are at high risk of not meeting, OMB's interim target dates for completing assessment, renovation, and validation of systems to be repaired. As of mid-November 1998,

- 4 of the 24 major departments and agencies (17 percent) reported that they had not completed assessing their mission-critical systems to be repaired--over a year behind OMB's governmentwide target of June 1997,

- 16 of the 24 major departments and agencies (67 percent) reported that they had not completed renovating their mission-critical systems to be repaired--several weeks after OMB's governmentwide deadline of September 1998, and

- 6 of the 24 major departments and agencies (25 percent) reported that they had validated 50 percent or fewer of their mission-critical systems to be repaired. OMB's governmentwide target to complete validation is January 1999.

Federal agencies must also be concerned about the Year 2000 readiness of their telecommunications and embedded systems. However, according to the 24 major departments and agencies November 1998 quarterly reports, many agencies had not completed inventorying and/or assessing their telecommunications or embedded systems.

Many federal agencies that are trying to cope with this enormous task are also facing concerns about whether they have sufficient staff. As we reported in April 1998[8] and again in October 1998,[9] many agencies have expressed concerns that the personnel needed to resolve their Year 2000 problems would not be available. However, comments from these agencies are largely anecdotal, and a comprehensive, analytical assessment of the issue has not yet been made. As a result, the full extent and severity of the Year 2000 workforce issue across the government is not known. The President's Council on Year 2000 Conversion, the Office of Personnel Management (OPM), and the Chief Information Officers (CIO) Council have various initiatives underway to address Year 2000 personnel issues. However, it is not yet known whether these efforts will ensure an adequate supply of qualified personnel to solve the government's Year 2000 problem.

Among our recommendations on this issue was that OMB determine if recent OPM

---

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

[9]Year 2000 Computing Crisis: Status of Efforts to Deal With Personnel Issues (GAO/AIMD/GGD-99-14, October 22, 1998).

initiatives have satisfactorily addressed agencies' reported personnel problems and, if they have not, designate an official to work with OPM and the CIO Council to help individual agencies resolve their Year 2000 workforce concerns. The Chair of the President's Council on Year 2000 Conversion and officials representing the CIO Council, OMB, and OPM concurred with our recommendations.

Reviews Show Uneven Federal Agency Progress

While the Year 2000 readiness of the government has improved, our reviews of federal agency Year 2000 programs have found uneven progress. Some agencies are significantly behind schedule and are at high risk that they will not fix their systems in time. Other agencies have made progress, although risks continue and a great deal of work remains.

Overall, our more than 70 reports and testimony statements contained over 100 recommendations related to the Year 2000 readiness of a wide range of individual agencies. These recommendations have been almost universally embraced.

Our recommendations have centered on the following:

- **Project planning**. We have recommended better organizational planning and management oversight--including systems inventorying and analysis--in a number of programs and entities.

- **Priority-setting**. With over 2,600 mission-critical systems still needing to be made Year 2000 compliant, it is important to establish priorities. Resources need to be focused on those business processes and supporting systems that could threaten national security, the economy, the health and safety of Americans, or their financial well-being.

- **Data exchanges**. To remediate their data exchanges, agencies must (1) identify data exchanges that are not Year 2000 compliant, (2) reach agreement with exchange partners (such as states) on the date format to be used, (3) determine if data bridges and filters are needed and, if so, reach agreement on their development,[10] (4) develop and test such bridges and filters, and (5) test and implement new exchange formats.

- **Testing**. Agencies should perform thorough testing of their systems, including end-to-end testing of multiple systems supporting a major business function.

[10]A bridge is used to convert 2-digit years to 4-digit years or to convert 4-digit years to 2-digit years. A filter is used to screen and identify incoming noncompliant data to prevent it from corrupting data in the receiving system.

- **Business continuity and contingency planning**. Given the interdependencies among agencies, their business partners, and the public infrastructure, 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.

The following are examples of the results of some of our recent reviews.

- In September 1998 we reported[11] that the Health Care Financing Administration (HCFA) had taken several steps to respond to recommendations in our May 1997 report in which we identified serious problems in HCFA's oversight of its Medicare contractors' Year 2000 remediation efforts, as well as problems with its own Year 2000 activities.[12] At that time, however, HCFA and its contractors were severely behind schedule in repairing, testing, and implementing the mission-critical systems supporting Medicare. As a result, in September, we concluded that it was highly unlikely that all of the Medicare systems would be compliant in time to ensure the delivery of uninterrupted benefits and services into the year 2000. To improve the prospects for success, we made several recommendations to HCFA, including the need to rank the remaining Year 2000 work on the basis of an integrated project schedule. We further recommended that HCFA (1) identify the critical path for its Year 2000 program to ensure that all critical tasks are prioritized and completed in time to prevent unnecessary delays, (2) define the scope of an end-to-end test of the Medicare claims process and develop plans and a schedule for conducting such a test, (3) develop a risk management process, and (4) accelerate the development of business continuity and contingency plans for the Medicare program. HCFA has agreed to implement these recommendations.

- In August 1998 we reported[13] that the Department of Veterans Affairs had made progress in addressing the Year 2000 recommendations in our May 1997 report.[14] However, concerns remained, including that (1) the Veterans Benefits Administration

---

[11]Medicare Computer Systems: Year 2000 Challenges Put Benefits and Services in Jeopardy (GAO/AIMD-98-284, September 28, 1998).

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

[13]Year 2000 Computing Crisis: Progress Made in Compliance of VA Systems, But Concerns Remain (GAO/AIMD-98-237, August 21, 1998).

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

had made limited progress in renovating two key mission-critical systems--one that processes claims benefits and updates benefits information, and one that contains veterans' names, addresses, service histories, and claims folder locations; and (2) the Veterans Health Administration did not know the full extent of its Year 2000 problem because it had not yet completed its assessment of, for example, locally developed software or customized versions of national applications used by its medical facilities. We made additional recommendations to the Department of Veterans Affairs, including that it (1) reassess its Year 2000 mission-critical efforts for the two key mission-critical systems where limited progress had been made as well as other information technology projects to ensure that Year 2000 efforts have adequate resources to achieve compliance in time, and (2) ensure the rapid development of business continuity and contingency plans for each medical facility.

Our work has shown that the Department of Defense and the military services face significant problems.[15] For example, our June 1998 report on the Navy found that while positive actions have been taken, remediation progress had been slow and the Navy was behind schedule in completing the early phases of its Year 2000 program.[16] Further, the Navy had not been effectively overseeing and managing its Year 2000 efforts and lacked complete and reliable information on its systems and on the status and cost of its remediation activities. We recommended improvements to the Department of Defense and the military services' Year 2000 programs related to critical issues such as data exchanges, testing, and contingency planning; they have concurred with these recommendations.

n addition to our agency-specific reports, in April 1998 we highlighted governmentwide ulnerabilities and made recommendations to the President's Council on Year 2000 Conversion to address them.[17]

Verification Strategy

OMB's assessment of the current status of federal Year 2000 progress was predominantly

---

[15]Defense Computers: Year 2000 Computer Problems Put Navy Operations At Risk (GAO/AIMD-98-150, June 30, 1998), Defense Computers: Army Needs to Greatly Strengthen Its Year 2000 Program (GAO/AIMD-98-53, May 29, 1998), GAO/AIMD-98-72, April 30, 1998, and Defense Computers: Air Force Needs to Strengthen Year 2000 Oversight (GAO/AIMD-98-35, January 16, 1998).

[16]GAO/AIMD-98-150, June 30, 1998.

[17]GAO/AIMD-98-85, April 30, 1998.

based on agency reports that had not been consistently reviewed or verified. Without independent reviews, OMB and the President's Council on Year 2000 Conversion had little assurance that they were receiving accurate information. In fact, we have found cases in which agencies' systems compliance status as reported to OMB has been inaccurate. For example, in June 1998, 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.[18] 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 for development.[19] (The department removed these systems from compliant status in its August 1998 quarterly report.)

To address this issue, we previously recommended that the Council require agencies to develop an independent verification strategy. According to OMB, all agencies are now required to independently verify their validation process and senior management at all large agencies are now relying on independent verification to provide a double-check that their mission-critical systems will, in fact, be ready for the year 2000.

One tool that some agencies are using to ensure the compliance of their mission-critical systems is a certification process. For example, in August 1998, a Deputy Secretary of Defense memorandum required that the Chief of Staff of the Army, Chief of Naval Operations, Chief of Staff of the Air Force, Commandant of the Marine Corps, and the Directors of the Defense Agencies certify that they have tested the Year 2000 capabilities of their respective components and national security systems. Such a certification, signed by the agency head, would reemphasize that the agency head is accountable for ensuring that the organization's mission-critical systems are Year 2000 compliant and could also provide a higher degree of confidence and valuable reassurance that a system reported as compliant has been comprehensively remediated and tested.

End-To-End Testing

To ensure that their 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. The purpose of end-to-end testing is to verify that a defined set of interrelated

---

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

[19] 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).

systems, which collectively support an organizational core business area or function, will 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 continually with their data exchange partners to plan and execute effective end-to-end tests (our Year 2000 testing guide sets forth a structured approach to testing, including end-to-end testing).[20] We recommended that, for the highest priority functions, the Council designate lead agencies responsible for ensuring that end-to-end operational testing of processes and supporting systems is performed.

Some of this type of testing has been performed in the government. However, 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.

Business Continuity and Contingency Planning

Business continuity and contingency plans are essential. 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 on 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.

Accordingly, we recommended that the Council require agencies to develop contingency plans for all critical core business processes. Since early 1998, OMB has clarified its contingency plan instructions and, along with the CIO Council, has adopted our business continuity and contingency planning guide.[21] In the case of the 24 major departments and agencies, we reported in March 1998[22] that--according to their February 1998 quarterly

[20]GAO/AIMD-10.1.21, November 1998.

[21]GAO/AIMD-10.1.19, August 1998.

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

reports--several agencies planned to develop contingency plans only if they fell behind schedule in completing their Year 2000 fixes. As we testified in June 1998,[23] only limited progress was reported in agencies' May 1998 quarterly reports which indicated that only four agencies had drafted contingency plans for their core business processes. According to their latest quarterly reports in November 1998, many agencies reported that they had completed or are drafting Year 2000 contingency plans for the continuity of their core business processes while others were in the early stages of such planning.

A key aspect of business continuity and contingency planning is testing the plan to evaluate whether individual contingency plans are capable of providing the level of support to the agency's core business processes and whether the plan can be implemented within a specified period of time. In instances in which a full-scale test may not be feasible, the agency may consider end-to-end testing of key plan components. Moreover, an independent review of the plan can validate the soundness of the proposed contingency strategy. To provide assurance that agencies' business continuity and contingency plans will work if they are needed, OMB may want to consider requiring agencies to test their business continuity strategy and set a target date, such as September 30, 1999, for the completion of this validation.

As noted in our business continuity and contingency guide,[24] another key element of a business continuity and contingency plan is the development of a zero day or day one risk reduction strategy, and procedures for the period between late December 1999 and early January 2000. For example, the Social Security Administration--a recognized federal leader in addressing the Year 2000 issue--has developed such as strategy. Among the features of this strategy is a moratorium on software changes, except for those mandated by law. SSA plans to minimize changes to its systems that have been certified as Year 2000 compliant by not allowing discretionary changes to be made. The moratorium will be in effect for commercial-off-the-shelf and mainframe products between July 1, 1999 and March 31, 2000 and for programmatic applications between September 1, 1999 and March 31, 2000. Such a Year 2000 change management policy will significantly reduce the chance that errors will be introduced into systems that have already been found to be compliant. Because this policy can reduce agencies' risks, OMB may want to consider directing agencies to implement similar policies.

Other aspects of SSA's day one strategy are the implementation of (1) an integrated control center, whose purposes include the internal dissemination of critical data and

---

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

[24] GAO/AIMD-10.1.19, August 1998.

problem management, and (2) a timeline that details the hours in which certain events will occur (such as when workloads will be placed in the queue and backup generators will be started) during the late December and early January rollover period. OMB may wish to consider requiring other agencies to develop similar plans.

SSA is also planning to address the personnel issue with respect to the rollover. For example, it plans to obtain a commitment from key staff to be available during the rollover period and establish a Year 2000 leave policy. Such a strategy, developed well in advance of the turn of the century, would help agencies manage the risks associated with the actual rollover and better position agencies to address disruptions if they occur. Therefore, OMB may wish to consider requiring agencies to develop and implement similar plans for the change of century rollover.

Reporting of Year 2000 Progress

To improve oversight of Year 2000 readiness, we previously recommended changes to OMB's quarterly reporting process. Specifically, we recommended (1) requiring additional agencies that play a significant role in the life of the nation to also report regularly to OMB; (2) requiring agencies to report on the status of their efforts to replace systems, not just on those being renovated; and (3) specifying the particular steps that must be taken to complete each phase of a Year 2000 program (i.e., assessment, renovation, validation, and implementation).

OMB has acted on these recommendations. Specifically, on March 9 and April 21, 1998, OMB issued a memorandum to an additional 31 and 10 agencies, respectively, requiring that they provide information on their Year 2000 progress and again in about a year's time (beginning with the August 1998 report, OMB required nine of these agencies to report quarterly). In addition, in its April 28, 1998, quarterly reporting guidance, OMB requested that agencies provide information on the oversight mechanism(s) used to ensure that replacement systems are on schedule; it also specified that agencies should ensure that their reporting on the completion of phases be consistent with the CIO Council's best practices guide and our enterprise readiness guide.[25] Moreover, in June 1998, OMB required that agencies that were not making adequate progress or about which OMB had concerns, report monthly on their progress in remediating mission-critical systems.

While these initiatives have enhanced the government's understanding of its Year 2000 remediation status, OMB has an opportunity to further improve its reporting approach. OMB 's draft guidance for the next quarterly reports is a good first step towards

[25]GAO/AIMD-10.1.14, September 1997.

improving this approach. OMB's draft guidance calls on federal agencies to identify and report on the core business functions that are to be addressed in their business continuity and contingency plans. We endorse this initiative because it could help identify the government's critical functions.

OMB could go a step further and require that agencies, based on their core business functions, report on the status of their end-to-end testing and business continuity and contingency plans.

- End-to-end testing. The boundaries on end-to-end tests are not fixed or predetermined, but rather vary depending on a given business area's system dependencies (internal and external) and criticality to the mission of the organization. Therefore, in planning end-to-end tests, a critical step is to understand and analyze the organization's core business functions. In addition, such critical business functions often involve multiple mission-critical systems that cut across organizational boundaries. With the time available for end-to-end testing diminishing, we believe that OMB should consider, for the government's most critical functions, setting target dates, and having agencies report against them, for the development of end-to-end tes plans, the establishment of test schedules, and the completion of the tests.

- Business Continuity and Contingency Planning. The identification of core business functions is a necessary feature of a business continuity and contingency plan. If agencies are required to identify these functions in the February 1999 quarterly report, OMB could consider setting a target date, such as April 30, 1999, for the completion of business continuity and contingency plans, and require agencies to report on their progress against this milestone. This would encourage agencies to expeditiously develop and finalize their plans and would provide the Council and OMB with more complete information on agencies' status on this critical issue.

Another key task that could be aided by the identification of the government's core business functions is setting priorities. While individual agencies have been identifying mission-critical systems, this has not always been done on the basis of a determination of the agency's most critical operations. Governmentwide priorities need to be based on such criteria as the potential for adverse health and safety effects, adverse financial effect on American citizens, detrimental effects on national security, and adverse economic consequences. Further, 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. Other entities have recognized the need to set priorities. For example, Canada established 48 national priorities covering areas such as national defense, food production, safety, and income security. In April, 1998, we recommended that the Council establish governmentwide priorities and ensure that agencies set agencywide priorities. However, governmentwide priorities have not yet been

established. Identification of the government's core business functions provides an opportunity to do this.

STATE AND LOCAL GOVERNMENTS
FACE SIGNIFICANT YEAR 2000 RISKS

State and local governments also face a major risk of Year 2000-induced failures to the many vital services that they provide. For example,

- food stamps and other types of payments may not be made or could be made for an incorrect amount;
- date-dependent signal timing patterns could be incorrectly implemented at highway intersections, and safety severely compromised, if traffic signal systems run by state and local governments do not process four-digit years correctly; and
- prisoner release or parole eligibility determinations may be adversely affected by the Year 2000 problem.

A recent survey of state Year 2000 efforts indicated that much remains to be completed. The states reported to the National Association of State Information Resource Executives that, as of January 15, 1999,[26] they had thousands of mission-critical systems.[27] With respect to the remediation of these systems, (1) 9 states reported that they had completed between 1 and 24 percent of the activities required to return a modified system or renovated process to production, (2) 12 states reported completing between 25 and 49 percent, (3) 19 states reported completing between 50 and 74 percent, and (4) 6 states reported completing more than 75 percent of their mission-critical systems.[28] On a more positive note, almost all states reported that they are actively engaged in internal and external contingency planing. However, of the 48 states that established target dates for the completion of these plans, 16 (33 percent) reported the deadline as September 1999 or later.

---

[26]Individual states submit periodic updates to the National Association of State Information Resource Executives. For the January 15th report, the states submitted their data between December 7, 1998 and January 14, 1999.

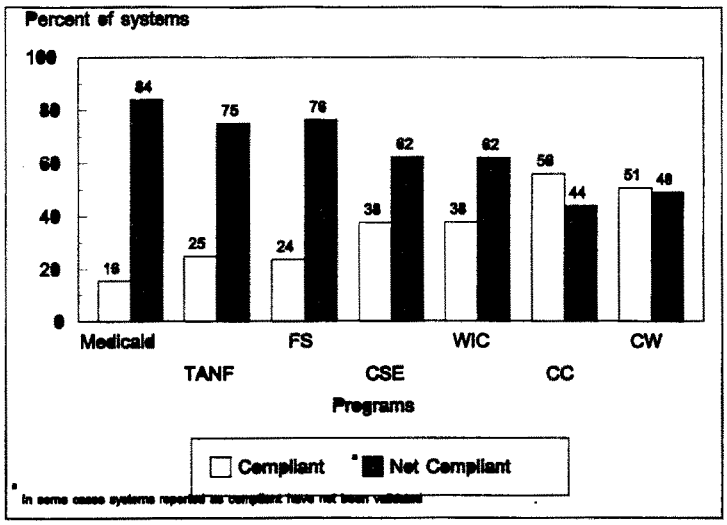
[27]The National Association of State Information Resource Executives defined mission-critical systems as those that the state has identified as priorities for prompt remediation.

[28]Four states did not respond to this question.

Our recent survey of the state systems used in federal welfare programs revealed that the majority of state welfare systems were not yet Year 2000 compliant (see chart 3).[29] Failure to complete Year 2000 conversion could result in billions of dollars in benefits payments not being delivered on time or in correct amounts. Other highlights of the survey results included that states reported that (1) assessment had been completed for about 80 percent of the welfare systems and (2) renovation had been completed on about one third of the welfare systems.

[29] Year 2000 Computing Crisis: Readiness of State Automated Systems to Support Federal Welfare Programs (GAO/AIMD-99-28, November 6, 1998). The survey was conducted in July and August 1998 and included the following welfare programs: Medicaid; Temporary Assistance for Needy Families (TANF); Women, Infants, and Children (WIC); food stamps (FS); child support enforcement (CSE); child care (CC); and child welfare (CW). Forty nine states, the District of Columbia, and three territories responded to our survey.

Chart 3: Reported Status of State Welfare Systems, as of July/August 1998



State audit organizations have identified other significant Year 2000 concerns. For example, (1) California's State Auditor reported[30] that state agencies were prematurely declaring their critical projects complete when they had not been thoroughly tested, that not all state agencies had completed the necessary steps to ensure that data exchanges will work seamlessly, and that managers of most state agencies had not developed business continuity plans, (2) Texas' Office of the State Auditor reported[31] that many state entities had not finished their embedded systems inventories and, therefore, it was not likely that they would complete their embedded systems repairs before the Year 2000, and (3) Vermont's Office of Auditor of Accounts reported[32] that the state faces the risk that critical portions of its Year 2000 compliance efforts could fail. State audit offices have also made recommendations, including the need for increased oversight, Year 2000 project plans, contingency plans, and personnel recruitment and retention strategies.

Recent reports on local governments have also highlighted significant Year 2000 concerns at this level. For example,

- A November 1998 survey commissioned by the National Association of Counties of a sample of 500 counties found that (1) 50 percent of the counties had a countywide Year 2000 plan, (2) 36 percent had completed assessment, (3) 16 percent had repaired or replaced their systems, (4) 41 percent had completed an inventory of county equipment that contain embedded systems, (5) 28 percent planned to conduct countywide testing, and (6) 73 percent had no contingency plans.

- Our testimony[33] on the District of Columbia reported that while the pace of the District's Year 2000 effort had picked up considerably, the District is still far behind in addressing the problem and at risk that critical processes could fail. Among the vital activities that the District should undertake include promptly identifying its most important operations and determining which systems supporting these operations can be fixed before the Year 2000 deadline.

---

[30] Year 2000 Computer Problem: Progress May Be Overly Optimistic and Certain Implications Have Not Been Addressed (August 27, 1998).

[31] A Review of Oversight for the State's Embedded Systems Year 2000 Repair Efforts (SAO Report No. 98-056, August 10, 1998).

[32] State Auditor's Report On Vermont's Year 2000 Preparedness For The Period Ending April 1, 1998 (May 5, 1998).

[33] Year 2000 Computing Crisis: The District of Columbia Faces Tremendous Challenges in Ensuring Vital Services Are Not Disrupted (GAO/T-AIMD-99-4, October 2, 1998).

- Among the Pennsylvania's Legislative Budget and Finance Committee's recent findings regarding its local government entities were that (1) many have not attempted to identify if they have a Year 2000 problem, (2) they appear largely unaware of potential embedded system problems, and (3) less than half of the entities that contract with service vendors have received verbal or written assurance that their vendors' systems will be Year 2000 compliant.[34]

- The Office of the New York State Comptroller's Division of Municipal Affairs reported that while 100 percent of New York's counties had made plans to deal with the Year 2000 problem, 26 percent of the cities, 54 percent of the towns, 48 percent of the villages, and 61 percent of the fire districts had not made plans to address the Year 2000 problem.[35]

The Chair of the President's Council on Year 2000 Conversion has expressed concerns about the Year 2000 readiness of state and local governments and has developed initiatives to address them. For example, the Council established working groups on state and local governments and tribal governments. The Chair of the Council also participates in monthly multi-state conference calls. In addition, OMB's draft guidance for the next quarterly reports requires federal agencies to report on the status of states that administer federal programs. This is an important initiative because states are key to the federal government's implementation of certain critical programs (such as food stamps and Medicaid). Accordingly, we also believe that OMB may want to consider establishing Year 2000 target dates (such as when renovation, validation, and implementation should be completed) for states to meet. In addition, OMB should consider ensuring that agencies have developed business continuity and contingency plans for state-administered programs that would be implemented if a state does not meet certain milestones.

The extent of information available to the public on state and locality Year 2000 readiness varies considerably. For example, while some states and local governments provide detailed Year 2000 readiness information on their web sites, others provide only limited data. States that are providing detailed readiness information are assisting their citizens in understanding the progress being made to address the Year 2000 problem. Accordingly, another initiative that the Council could consider is developing and distributing to state and local governments a template that identifies the types of Year 2000 information that the entity could disclose to the public. For example, the template could contain the percentage of systems that the state or local government has assessed,

---

[34] The Year 2000 Problem in Local Governments and School Districts (September 1998).

[35] 1998 Municipal Technology Survey Results (September 1998).

renovated, and validated in key areas such as utilities, transportation, health and human services, safety and emergency services, revenue, education, and administrative systems (such as elections systems). In areas in which the state or local government may perform a regulatory function, such as drinking water or electric power, the government could provide readiness data on those regulated entities. Public disclosure of such information could reduce the public's concern over potential disruptions caused by Year 2000-induced failures.

YEAR 2000 READINESS INFORMATION AVAILABLE IN SOME SECTORS, BUT KEY INFORMATION STILL MISSING OR INCOMPLETE

Beyond the risks faced by the federal, state, and local governments, the Year 2000 also poses a serious challenge to the public infrastructure, key economic sectors, and to other countries. To address these concerns, in April 1998 we recommended that the Council use a sector-based approach and establish the effective public-private partnerships necessary to address this issue.[36] The Council subsequently established over 25 sector-based working groups and has been initiating outreach activities since it became operational last spring. In addition, the Chair of the Council recently announced that he was forming a Senior Advisors Group composed of representatives from private-sector firms across key economic sectors. Members of this group are expected to offer perspectives on cross-cutting issues, information sharing, and appropriate federal responses to potential Year 2000 failures. The first meeting of this group is scheduled for this month.

Our April 1998 report also recommended that the President's Council on Year 2000 Conversion develop a comprehensive picture of the nation's Year 2000 readiness, to include identifying and assessing risks to the nation's key economic sectors--including risks posed by international links. In October 1998 the Chair directed the Council's sector working groups to begin assessing their sectors. The Chair also provided a recommended guide of core questions that the Council asked to be included in surveys by the associations performing the assessments. These questions included the percentage of work that has been completed in the assessment, renovation, validation, and implementation phases. The Chair plans to issue quarterly public reports summarizing these assessments. The first such report was issued on January 7, 1999.

The January 7, 1999, report summarizes information collected to date by the working

[36]GAO/AIMD-98-85, April 30, 1998.

groups and various trade associations.[37] The Council acknowledged that readiness data in certain industries were not yet available and, therefore, were not included in the report. Nevertheless, based on the information available at the time, it concluded that

- virtually all of the industry areas reported high awareness of the Year 2000 and its potential consequences,
- participants in several areas, particularly financial institutions, are mounting aggressive efforts to combat the problem,
- it is increasingly confident that there will not be large scale disruptions in the banking, power, and telecommunications areas and, if disruptions do occur, they are likely to be localized,
- large organizations often have a better handle on the Year 2000 problem than do smaller ones, and some small and medium-sized businesses and governments continue to believe that the Year 2000 problem will not affect them or are delaying action until failures occur, and
- international failures are likely since, despite recent increased efforts, a number of countries have done little to remediate critical systems.

The Council's report is a good step toward obtaining a picture of the nation's Year 2000 readiness. However, the picture remains substantially incomplete because assessments were not available in many key areas, such as 911 centers, fire services, and the maritime industry. Also, some surveys did not have a high response rate, calling into question whether they accurately portray the readiness of the sector. In addition, in some cases, such as drinking water and health care, the report provides a general assessment of the sector but does not contain detailed data as to the status of the sector (e.g., the average percentage of organization's systems that are Year 2000 compliant or the percentage of organizations that are in the assessment, renovation, or validation phases).

The Council must remain vigilant and closely monitor and update the information in the sectors where information is available and obtain information for those where it is not. Particular attention should be paid to the public infrastructure, including critical areas such as power, water, and telecommunications since most, if not all, major enterprises rely on these essential elements for daily functioning. Other key economic sectors include health, safety, and emergency services; banking and finance; transportation; and

[37] First Quarterly Summary of Assessment Information (The President's Council on Year 2000 Conversion, January 7, 1999).

manufacturing and small business. In addition, with the advent of electronic communication and international commerce, the United States is also critically dependent on international Year 2000 readiness.

Power

The electric power industry is complex and highly automated. It is made up of an interconnected network of generation plants, transmission lines, and distribution facilities. There are three independent interconnections that provide electricity to every household and company in North America.

On January 11, 1999, the North American Electric Reliability Council (NERC) issued its second report on the Year 2000 status of electric power systems.[38] NERC found that, as of November 30, 1998, on average, the electric industry is close to, but slightly lagging in meeting the industry's target date of June 30, 1999, for being "Year 2000 ready."[39] In addition, NERC reported that reporting organizations, on average, had completed 96 percent of the inventory phase, 82 percent of the assessment phase, and 44 percent of the remediation/testing phase.

Related to the power sector are the oil and gas industries. An August 1998 survey of these industries by the President's Council on Year 2000 Conversion's oil and gas working group, in conjunction with the American Petroleum Institute, the Interstate Natural Gas Association of America, the American Gas Association, and other industry groups found that, for their business systems and associated software, (1) 45 percent of respondents[40] were in the planning, inventory, or assessment phases, (2) 36 percent were

[38] Preparing the Electric Power Systems of North America for Transition to the Year 2000 (NERC, January 11, 1999). This report was prepared in response to a May 1998 request by the Department of Energy. According to NERC, about 98 percent of the electricity supply and delivery organizations in North America participated in this assessment (194 of 198 bulk electric entities and 2,821 of 2,888 distribution entities).

[39] NERC defined Year 2000 ready as meaning that a system or component has been determined to be "suitable for continued use into the Year 2000." NERC noted that "this is not necessarily the same as Y2K Compliant, which implies fully correct date manipulations."

[40] The respondents to this survey represented 45 percent of U.S. oil and natural gas production, 78 percent of U.S. refining capacity, 70 percent of U.S. crude oil and refined product pipeline deliveries, 81 percent of natural gas interstate pipeline deliveries, 43 percent of U.S. branded retail outlets, and 50 percent of the total natural gas volume of investor-owned local distribution companies.

in the remediation phase, and (3) 19 percent were in the validation phase. In regard to embedded systems, (1) 60 percent of respondents were in the planning, inventory, or assessment phases, (2) 26 percent were in the remediation phase, and (3) 14 percent were in the validation phase.

Water

The water sector includes drinking water and wastewater utilities. These utilities are owned by local governments and private companies and range in size from small, serving communities of less than 10,000, to large, serving populations of over 1 million. Automation in these utilities varies greatly as well, from plants with high levels of automation to smaller plants with little, if any, computerized equipment.

A September 1998 report on a survey by the American Water Works Association, the Association of Metropolitan Water Agencies, and the National Association of Water Companies[41] stated that, of the 600 responding public water utilities, half had completed their assessments of internal systems. These organizations expect to complete a more extensive report on the readiness of water system operators by March 1999. With respect to wastewater systems, in December 1998 the Association of Metropolitan Sewage Agencies reported that 95 percent of respondents[42] had begun to implement solutions for the Year 2000 problem, while 26 percent were complete or nearly complete.

Telecommunications

In testimony in June, we reported that the Year 2000 readiness of the telecommunications sector is one of the most crucial concerns to our nation because telecommunications are critical to the operation of nearly every public- and private-sector organization.[43] For example, the information and telecommunications sector (1) enables the electronic transfer of funds, the distribution of electrical power, and the control of gas and oil pipeline systems; (2) is essential to the service economy, manufacturing, and efficient delivery of raw materials and finished goods; and (3) is basic to responsive emergency

---

[41]These organizations represent approximately 4,000 public water systems, which provide services to about 80 percent of the United States population.

[42]The Association of Metropolitan Sewage Agencies originally surveyed its 206 members in June 1998 and conducted a follow-up survey in October 1998. Seventy-six agencies responded to the June survey and 43 responded to the October follow-up.

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

services. Reliable telecommunications services are made possible by a complex web of highly interconnected networks supported by national and local carriers and service providers, equipment manufacturers and suppliers, and customers.

According to the President's Council on Year 2000 Conversion, information from the telecommunications industry indicates that the major companies have active Year 2000 programs and have made substantial progress toward updating their systems but that less information is available regarding the readiness of smaller organizations. With respect to specific segments of the telecommunications sector, (1) preliminary information from the Network Reliability and Interoperability Council found that, based on a polling of companies that represent 94 percent of the access lines in the United States, the average target completion date was June 30, 1999, (2) current data are not available for the cable segment but responses to a survey by the Cable Services Bureau are expected in early 1999, (3) the Wireless Telecommunications Bureau expects to complete a comprehensive assessment of this segment in the first quarter of 1999, and (4) the Mass Media Bureau is conducting a survey of a cross-section of broadcasters that is expected to be completed in early 1999.

Health

The health sector includes health care providers (such as hospitals and emergency health care services), insurers (such as Medicare and Medicaid), and biomedical equipment. Readiness information on the health care sector has been limited. However, the Council health care working group plans to gather Year 2000 readiness information of this sector throughout 1999, especially among smaller health care organizations. In addition, with the support of the Association of State and Territorial Health Officials, the Centers for Disease Control and Prevention sent a Year 2000 readiness assessment survey to 57 state and territorial health officials. The results of this survey are expected by the end of January 1999. In addition, the Department of Health and Human Services' Office of Inspector General plans to survey the Year 2000 readiness of a sample of Medicare providers.

We also have previously reported that the Health Care Financing Administration and its contractors were severely behind schedule in repairing, testing, and implementing the mission-critical systems supporting Medicare.[44] In addition, our July/August 1998 survey of state Medicaid systems found that 16 percent were Year 2000 compliant.[45]

---

[44]Medicare Computer Systems: Year 2000 Challenges Put Benefits and Services in Jeopardy (GAO/AIMD-98-284, September 28, 1998).

[45]Year 2000 Computing Crisis: Readiness of State Automated Systems to Support Federal Welfare Programs (GAO/AIMD-99-28, November 6, 1998).

Regarding biomedical equipment, we reported that the Department of Health and Human Services' Food and Drug Administration (FDA)--which provides information from the biomedical equipment manufacturers to the public through an Internet World Wide Web site--had no assurance that manufacturers had adequately addressed the Year 2000 problem for noncompliant equipment because it did not require manufacturers to submit test results certifying compliance.[46] Moreover, FDA's database lacked detailed information on the make and model of compliant equipment and, as of July 30, 1998, only about 12 percent of biomedical equipment manufacturers had responded to FDA's inquiries. To address these issues, we recommended that the Departments of Health and Human Services and Veterans Affairs (1) work jointly to develop immediately a single data clearinghouse that provides compliance information to all users of biomedical equipment and (2) determine what actions, if any, should be taken regarding biomedical equipment manufacturers that have not provided compliance information.

In response to our recommendation, FDA, in conjunction with the Department of Veterans Affairs, established a biomedical equipment clearinghouse. The Department of Health and Human Services reported that, as of October 28, 1998, approximately two-thirds of the biomedical equipment manufacturers that make products containing electronic components have provided information to the clearinghouse.

Safety and Emergency Services

This sector involves organizations that respond to disasters as well as those that have a daily impact on public safety, such as police, fire, and emergency medical services. The Federal Emergency Management Agency conducted a survey of state emergency management directors in October/November 1998 and received responses from 46 states, the District of Columbia, and 4 territories. According to the Federal Emergency Management Agency, all state-level agencies have resolved, or planned to resolve, the vast number of Year 2000-related issues involving critical emergency preparedness facilities, systems, and services. Concerns were raised, however, about the limited amount of resources to assess, fix, test, and validate state-level systems. In addition, the state emergency management directors were not generally aware of the status of emergency preparedness and Year 2000 progress at the local level. A survey by the International Association of Emergency Managers, which has a membership of 1,700 individuals representing local emergency management organizations, found that, of the 172 respondents, 159 were actively working on the Year 2000 problem and 59 reported that their systems were "fully prepared."

---

[46]Year 2000 Computing Crisis: Compliance Status of Many Biomedical Equipment Items Still Unknown (GAO/AIMD-98-240, September 18, 1998).

Information on the Year 2000 status of other parts of this sector, such the readiness of fire services, 911 centers, emergency medical services, and local law enforcement has not yet been collected although some assessments are ongoing or planned for early 1999.

Banking and Finance

A large portion of the institutions that make up the banking and finance sector are overseen by one or more federal regulatory agencies. In September 1998 we testified on the efforts of five federal financial regulatory agencies[47] to ensure that the institutions that they oversee are ready to handle the Year 2000 problem.[48] We concluded that the regulators have made significant progress in assessing the readiness of member institutions and raising awareness on important issues such as contingency planning and testing. Regulator examinations of bank, thrift, and credit union Year 2000 efforts found that the vast majority were doing a satisfactory job of addressing the problem. Nevertheless, the regulators faced the challenge of ensuring that they are ready to take swift action to address those institutions that falter in the later stages of correction and to address disruptions caused by international and public infrastructure failures.

With respect to the securities industry, a September 1998 Securities and Exchange Commission survey of the national securities exchanges, the National Association of Securities Dealers, the Securities Industry Association, and the registered or exempt clearing agencies found that (1) the exchanges and the National Association of Securities Dealers had completed remediation and testing on 95 percent of mission-critical systems and have finished implementation on 73 percent of these systems and (2) the clearing agencies have completed renovation and testing on 87 percent of critical systems and implementation of 86 percent of these systems.

Transportation

The transportation sector includes air traffic, railroads, the maritime industry, highways, and transit providers. We have previously expressed concern about the Federal Aviation

---

[47]The National Credit Union Administration, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the Federal Reserve System, and the Office of the Comptroller of the Currency.

[48]Year 2000 Computing Crisis: Federal Depository Institution Regulators Are Making Progress, But Challenges Remain (GAO/T-AIMD-98-305, September 17, 1998).

Administration's Year 2000 efforts. Specifically, we reported in August 1998,[49] that FAA had made progress in managing its Year 2000 problem and had completed critical steps in defining which systems needed to be corrected and how to accomplish this. However, with less than 17 months to go, FAA still had to correct, test, and implement many of its mission-critical systems. A November 1998 survey by the National Air Carrier Association, Inc. of its seven carriers that specialize in low-cost scheduled and charter passenger and cargo transportation had 5 respondents. The survey found that some of the small carriers had only 55 percent of their assessment completed, while larger carriers had made more progress. The results of surveys of larger commercial carriers and airports are expected in the first quarter of 1999.

According to the President's Council on Year 2000 Conversion, neither the railroad industry nor the maritime industry had complete, consolidated Year 2000 readiness assessment data although such information is expected in early 1999. A survey by the American Association of Motor Vehicle Administrators, which represents motor vehicle and traffic law enforcement administrators in the United States and Canada, received 44 responses from 31 states in an August 1998 survey. Thirty-four percent of respondents stated that they were Year 2000 compliant while 59 percent stated that they were assessing the issue or had at least one Year 2000 project planned or underway. With regard to transit providers, of the 162 respondents (a response rate of nearly 50 percent) to a American Public Transit Association May 1998 survey of transit systems, (1) 20 percent reported that they were Year 2000 compliant, (2) 79 percent reported that their systems would be Year 2000 compliant by the year 2000, and (3) 21 percent reported that they were not sure whether they would be compliant by the year 2000.

Manufacturing and Small Business

The manufacturing and small business sector includes the entities that produce or sell a myriad of products such as electronics, heavy equipment, food, textiles, and automobiles. The President's Council on Year 2000 Conversion consumer affairs working group is assessing the Year 2000 compliance of consumer products and financial services. In addition, the Federal Trade Commission, which chairs this working group, has set up a web site and the Council has established a toll-free telephone number through which consumers can obtain Year 2000 information.

The Department of Agriculture, the chair of the Council's food supply working group, contracted with the Gartner Group to obtain a Year 2000 assessment of the nation's food supply. The Gartner Group's analysis of the four largest companies within specific food

[49] FAA Systems: Serious Challenges Remain in Resolving Year 2000 and Computer Security Problems (GAO/T-AIMD-98-251, August 6, 1998).

industries (e.g., beef, refined sugar, fertilizer) found that the awareness and progress of most of these companies was commendable and that remediation efforts ranged from still completing inventories and assessments to well underway. However, Gartner Group's research has shown that the level of preparedness of large companies is higher than that of smaller companies. Therefore, they cautioned that in food industries in which the large companies control only a small percentage of the market (such as the fish industry), an industry-wide failure to remediate could have widespread impact.

The President's Council on Year 2000 Conversion reported that the status of Year 2000 efforts in the nation's millions of small and medium-sized businesses is a concern. The National Federation of Independent Business reported in December 1998 on the results of its October/November survey of a sample of small businesses. According to this report, only 38 percent of respondents had taken or were taking action. In addition, according to the report, about one-third of small businesses that are aware of the Year 2000 problem and are vulnerable to it plan no preventive measures.

International

In addition to the risks associated with the nation's key economic sectors, one of the largest, and largely unknown, risks relates to the global nature of the problem. International concerns were underscored by a September 1998 report by the Organization for Economic Co-operation and Development.[50] This report stated that (1) while awareness is increasing, the amount of remediation still required is daunting, (2) significant negative economic impact is likely in the short term, although much uncertainty exists about the extent of Year 2000-induced disruptions, (3) governments face a major public management challenge requiring acceleration of their own preparations and stronger leadership, and (4) stronger international cooperation is essential, especially in conjunction with cross-border testing.

Another example of potential international problems is illustrated by a Gartner Group survey of 15,000 companies in 87 countries which found that many countries are in the early stages of Year 2000 readiness. As of September 1998, the Gartner Group found that

[50]The Organization for Economic Co-operation and Development surveyed its member countries and reviewed existing studies and media reports on the Year 2000 problem and issued a report on its findings, The Year 2000 Problem: Impacts and Actions (September 1998). The organization's 29 member countries are Australia, Austria, Belgium, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States.

the United States, Australia, Belgium, Canada, England, Holland, Ireland, Sweden, and Switzerland were farthest ahead. Behind these leaders were countries such as Japan, Germany, India, and Brazil. Countries furthest behind included Russia, China, and the Philippines.[51]

The United States has attempted to promote international dialog on the Year 2000 problem. In June 1998 the United Nations General Assembly adopted a resolution on the global implications of the Year 2000 issue. The resolution recognized that effective operation of governments, companies, and other organizations was threatened by the Year 2000 issue and coordinated efforts were required to address it. The resolution went on to request that all member countries attach a high priority to raising the level of awareness and to consider appointing a nationwide coordinator to tackle the problem. The Chair of the President's Council also has met with the United Nations and other international bodies, and helped organize a significant December 1998 National Y2K Coordinators' meeting attended by over 120 countries, hosted by the United Nations' Working Group on Informatics. This meeting should help encourage the establishment of regional coordinating mechanisms and foster greater international dialog on the Year 2000 issue.

Additional Actions That Could Be Considered
By the President's Council on Key Sectors

The President's Council on Year 2000 Conversion is to be commended on the strides that it has made to obtain Year 2000 readiness data that is critical to the nation's well-being as well as its other initiatives, such as the establishment of the Senior Advisors Group. To further reduce the likelihood of major disruptions, the Council may wish to consider other actions.

- The Council must continue to aggressively pursue readiness information in the areas in which it is lacking, such as the railroad industry, health sector, and local law enforcement. If the current approach of using associations to voluntarily collect information does not yield the necessary information, the Council may wish to consider whether legislative remedies (such as requiring disclosure of Year 2000 readiness data) should be proposed.

- To encourage the reporting of more complete information, the Council should consider requesting that the national associations publicly disclose, at a minimum, those companies that have responded to surveys.

[51] Year 2000 Global State of Readiness and Risks to the General Business Community, testimony presented by the Gartner Group before the Special Committee on the Year 2000 Technology Problem, October 7, 1998.

- In its January 1999 meeting, the Chair provided Council members with items to consider when preparing the working groups' input into the April 1999 assessment report. These items included the key facts to obtain from survey information and information on the group conducting the assessment, and number surveyed/number that responded. This type of data should help the Chair and the Council evaluate the readiness of the sectors. Indeed, we would urge the Council to include this same information in the April assessment report to the public. In addition, to ensure that the Council's working groups have adequately covered the nation's sectors, another goal for the next quarterly assessment report could be for the working groups to identify each sector's major components and report summary readiness information, including significant trends, by major component to the Chair for inclusion in the report to the public.

- Since the international arena carries some of the greatest Year 2000 risks and uncertainties, the Council could prioritize trade and commerce activities that are critical to the nation's well-being (e.g., oil, food, pharmaceuticals) and, working with the private sector (perhaps using the Senior Advisors Group), identify options to obtain these materials through alternative avenues in the event that Year 2000-induced failures in the importing country or in the transportation sector prevent these items from reaching the United States.

- - - - -

In summary, national, federal, state, and local efforts must increase substantially to ensure that major service disruptions do not occur. Strong leadership and partnerships are essential if government programs are to meet the needs of the public at the turn of the century.

Messrs. Chairmen, this concludes my statement. I would be happy to respond to any questions that you or other members of the Committees may have at this time.

GAO REPORTS AND TESTIMONY ADDRESSING THE YEAR 2000 CRISIS

Status Information: FAA's Year 2000 Business Continuity and Contingency Planning Efforts Are Ongoing (GAO/AIMD-99-40R, December 4, 1998)

Year 2000 Computing Crisis: A Testing Guide (GAO/AIMD-10.1.21, November 1998)

Year 2000 Computing Crisis: Readiness of State Automated Systems to Support Federal Welfare Programs (GAO/AIMD-99-28, November 6, 1998)

Year 2000 Computing Crisis: Status of Efforts to Deal With Personnel Issues (GAO/AIMD/GGD-99-14, October 22, 1998)

Year 2000 Computing Crisis: Updated Status of Department of Education's Information Systems (GAO/T-AIMD-99-8, October 8, 1998)

Year 2000 Computing Crisis: The District of Columbia Faces Tremendous Challenges in Ensuring That Vital Services Are Not Disrupted (GAO/T-AIMD-99-4, October 2, 1998)

Medicare Computer Systems: Year 2000 Challenges Put Benefits and Services in Jeopardy (GAO/AIMD-98-284, September 28, 1998)

Year 2000 Computing Crisis: Leadership Needed to Collect and Disseminate Critical Biomedical Equipment Information (GAO/T-AIMD-98-310, September 24, 1998)

Year 2000 Computing Crisis: Compliance Status of Many Biomedical Equipment Items Still Unknown (GAO/AIMD-98-240, September 18, 1998)

Year 2000 Computing Crisis: Significant Risks Remain to Department of Education's Student Financial Aid Systems (GAO/T-AIMD-98-302, September 17, 1998)

Year 2000 Computing Crisis: Progress Made at Department of Labor, But Key Systems at Risk (GAO/T-AIMD-98-303, September 17, 1998)

Year 2000 Computing Crisis: Federal Depository Institution Regulators Are Making Progress, But Challenges Remain (GAO/T-AIMD-98-305, September 17, 1998)

Year 2000 Computing Crisis: Federal Reserve Is Acting To Ensure Financial Institutions Are Fixing Systems But Challenges Remain (GAO/AIMD-98-248, September 17, 1998)

Responses to Questions on FAA's Computer Security and Year 2000 Program (GAO/AIMD-98-301R, September 14, 1998)

Year 2000 Computing Crisis: Severity of Problem Calls for Strong Leadership and Effective Partnerships (GAO/T-AIMD-98-278, September 3, 1998)

Year 2000 Computing Crisis: Strong Leadership and Effective Partnerships Needed to Reduce Likelihood of Adverse Impact (GAO/T-AIMD-98-277, September 2, 1998)

Year 2000 Computing Crisis: Strong Leadership and Effective Partnerships Needed to Mitigate Risks (GAO/T-AIMD-98-276, September 1, 1998)

Year 2000 Computing Crisis: State Department Needs To Make Fundamental Improvements To Its Year 2000 Program (GAO/AIMD-98-162, August 28, 1998)

Year 2000 Computing: EFT 99 Is Not Expected to Affect Year 2000 Remediation Efforts (GAO/AIMD-98-272R, August 28, 1998)

Year 2000 Computing Crisis: Progress Made in Compliance of VA Systems, But Concerns Remain (GAO/AIMD-98-237, August 21, 1998)

Year 2000 Computing Crisis: Avoiding Major Disruptions Will Require Strong Leadership and Effective Partnerships (GAO/T-AIMD-98-267, August 19, 1998)

Year 2000 Computing Crisis: Strong Leadership and Partnerships Needed to Address Risk of Major Disruptions (GAO/T-AIMD-98-266, August 17, 1998)

Year 2000 Computing Crisis: Strong Leadership and Partnerships Needed to Mitigate Risk of Major Disruptions (GAO/T-AIMD-98-262, August 13, 1998)

FAA Systems: Serious Challenges Remain in Resolving Year 2000 and Computer Security Problems (GAO/T-AIMD-98-251, August 6, 1998)

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

Internal Revenue Service: Impact of the IRS Restructuring and Reform Act on Year 2000 Efforts (GAO/GGD-98-158R, August 4, 1998)

Social Security Administration: Subcommittee Questions Concerning Information Technology Challenges Facing the Commissioner (GAO/AIMD-98-235R, July 10, 1998)

Year 2000 Computing Crisis: Actions Needed on Electronic Data Exchanges (GAO/AIMD-98-124, July 1, 1998)

Defense Computers: Year 2000 Computer Problems Put Navy Operations At Risk (GAO/AIMD-98-150, June 30, 1998)

Year 2000 Computing Crisis: Testing and Other Challenges Confronting Federal Agencies (GAO/T-AIMD-98-218, June 22, 1998)

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)

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)

(511723)

Mr. HORN. Thank you very much. I yield 5 minutes to the co-chairman of the Task Force, Mrs. Morella, chairman of the Subcommittee on Technology.

Mrs. MORELLA. Thank you, Mr. Chairman. I want to commend both of you for your excellent, succinct and candid testimony. I must say to GAO, Mr. Willemssen, you have certainly done a tremendous number of reports that all deal with Y2K. I remember, I think it was 3 years ago, under the issues at risk, at-risk issues, Y2K was mentioned then with computer security on it, which continues to be mentioned.

Mr. Gershwin, I certainly again value the statement you made about other countries and what they haven't done, what they have done, and the leadership that we must show.

I asked Mr. Koskinen kind of the question in sort of a rough-hewn verbiage to try to find out what is being done under his direction to coordinate the concerns that both of you have expressed. And you have expressed a series of recommendations throughout. You have expressed the problems with some ways that maybe we can look at it.

Would you tell us, these two committees, subcommittees, how you work with Mr. Koskinen; what more needs to be done to push forward that kind of action that we need? Either of you can answer first.

Mr. WILLEMSSEN. I will start first. As John mentioned up front, when he was here earlier, we do meet with him on a monthly basis and we share issues that we have, and he does likewise.

In addition, as issues come up on individual agencies where we are doing reviews, we will give him a heads-up as soon as we have the available data, to let him know of our concerns and that we will be reporting on those.

Similarly, with some of the suggestions we have offered here today, we have let him know of those suggestions, and also OMB, and I think it is accurate to say they, in general, agree with those suggestions. They also added we might be a little ahead of them; that they were considering these types of actions anyway. But we do have general concurrence.

So we have found the working relationship to be working pretty well. Not to say that we haven't always wanted a little more aggressive action in some of these areas. But if you look back at some of the major recommendations we made to Mr. Koskinen as soon as he took the job, most of those recommendations now have been implemented, although some of them not as quickly as we would have liked.

Mrs. MORELLA. Would you like to comment, Mr. Gershwin?

Dr. GERSHWIN. Yes. I am the intelligence community's representative on the President's Council on the Y2K Conversion, so I regularly attend the meetings. But much more than that, we are heavily involved, my deputy Norm Green and I, in the international working group that is part of the Council. We have been actively involved with State Department, who chairs that working group, and in providing briefings to people in State Department about our information on the foreign Y2K efforts. We will be doing the same thing with the Department of Energy, because I have been meeting with those folks.

We are very actively engaged with the Defense Department's work in the President's Council. In fact, Norm Green and one of the DOD people chairs a subgroup that has to do with international issues. So I think we are extraordinarily involved in the work of the President's Council, as well as doing our own independent analysis of this. But it is essentially all being provided to not only John Koskinen but other members of the Council.

Mrs. MORELLA. Too bad we cannot clone both of you in terms of what you know needs to be done.

My concern is that these governments have so many other problems, like the Asian financial crisis, that Y2K is still, regardless of your international group, still at the bottom of the list; and in terms of putting money into it and the expertise that they don't have.

Mr. Willemssen, I am interested in, too, is the suggestions are made, they are listened to, affirmative response in terms of we agree with what you are saying. Do you, the next month when you meet, followup and say, these are some recommendations that it would have been far better had you done something with it; or would you tell us what you have done? What kinds of accountability is there other than these are some suggestions?

Mr. WILLEMSSEN. We do followup with them. I will give you one example. The recommendations that we had made early in 1998 was for John Koskinen to take a sector-based approach and conduct detailed assessments of those sectors. He eventually did that. I wish he would have done it 6 months earlier. And he knew that we were pushing him to do that, and I am glad that he has done it.

The type of rich detailed data that we need on many of those sectors still isn't there. And I think when the next quarterly report comes out from John in April, if we still continue to see the dearth of rich detailed data, then we have to start looking at other alternatives to get that information.

Mrs. MORELLA. It is a tremendous frustration, from my point of view, in terms of so many things need to be done. I am convinced we are not going to be ready, and yet I am not one who panics. I tell everybody, "Don't worry, critical-mission systems will be taken care of." I am not really even sure of that. And I am really worried about, what did you call it, "business connections," when I talk about making sure about how one group links with one another. Oh, "business continuity points." Whatever, you know exactly what I mean. The kind of connection I think we need to do more evaluating and working on that.

So I look forward to continuing to work with both of you and with your very capable staffs to make sure that it is incorporated soon.

Thank you, Mr. Chairman.

Mr. HORN. Thank you. Now Mr. Turner, the ranking member, 5 minutes for questioning.

Mr. TURNER. Dr. Gershwin, one of the concerns you addressed was the lack of preparation in Russia by the Russian Atomic Energy Ministry. If I were to ask you what are the greatest threats or problems that could occur, what national security problems

would be on your top list of concerns? What kind of things would you list for us?

Dr. GERSHWIN. As far as Russia is concerned?

Mr. TURNER. Russia and, in general, national security concerns.

Dr. GERSHWIN. OK. National security in a broad sense is more than military issues, obviously, and we are really quite concerned now, as we see it, about world trade issues, which are essentially U.S. and global economic security.

The potential for there to be enough disruption of the global economy that, as we have seen in the last 6 months, the United States is certainly tied into the global economy in a serious way. So I would probably put that as the top issue I would raise as far as the international implications.

Another one, which I think is really quite important, is the fact that these disruptions, particularly in places like Russia and China, will be taking place in the middle of winter. And we have had a little taste of that in our area here in the last few days.

Mrs. MORELLA. My area, as a matter of fact.

Dr. GERSHWIN. Particularly in Montgomery County. But Russia is likely to experience some serious power outages. Their nuclear reactors, some of their nuclear reactors may shut down.

One of the issues on their nuclear reactors is simply the vital role that Russian nuclear reactors play in the overall power distribution in that country and the difficulty they might have in getting them back up again, leading to serious power outages, which would hurt an already hurting economy.

In addition, a worry that we have, and that we are working on rather hard to get more information on, is the potential for nuclear reactors in places like Russia to have safety problems in their shutdowns. If the nuclear reactors experience failures, if the back-up diesel generators experience failures, there could be electrical problems that interfere with the safety mechanisms in those nuclear reactors.

While we don't want to raise the specter at this point of huge problems in terms of safety of nuclear reactors worldwide, the fact is that in Russia itself that is a concern to us, and we are going to be studying that in a lot more detail over the next few months. So I would certainly raise that, then, as an important national security concern because of nuclear power problems.

Taking that a little further, I think just the electric power grids in many of these key countries are susceptible to some sort of failures, because I don't think most of these countries we are talking about, such as China and Russia, have done nearly the work done in North America. All of these countries are extremely dependent, frankly, on their electric power for many, many things.

So, again, in terms of major domestic disruptions in those countries, leading to all kinds of economic difficulties, possible needs for United States and western humanitarian assistance to those countries in the middle of winter, I see some of those as the critical national security issues.

Mr. TURNER. I have seen a lot of efforts being made by our domestic utility companies to comply and be ready for Y2K, and I am sure many efforts are being made with regard to nuclear power plants within our own country. Have we made any efforts to offer

international assistance, or would that be an appropriate response to what appears to be a very serious potential problem?

I assume you are talking about that it is not beyond the realm of possibility that there could be another Chernobyl as a result of Y2K in Russia or some other country where they have not prepared their nuclear reactors.

Dr. GERSHWIN. That would be the issue obviously we ought to be worried about, although at this point I think it would be premature to raise that flag, but I think it is something that we are watching.

The Department of Energy is certainly in a position to discuss nuclear power issues with other countries. You would really have to ask them where they stand in terms of those kinds of discussions. But I think there is a fair amount of information shared from one country to another; various mechanisms to discuss nuclear power problems.

One of the issues is simply that countries like Russia do not easily welcome advice from the West on their Y2K problems. There has been some discussion, but they have been very slow to react in many areas, and that would be one of them.

Mr. TURNER. Thank you, Mr. Chairman.

Mr. HORN. Thank you. Vice Chairman Biggert, 5 minutes.

Mrs. BIGGERT. Thank you, Mr. Chairman.

Dr. Gershwin, you mentioned that there are many of these countries in the infancy stage of awareness. What is kind of the cutoff date? If they haven't done anything, is there a time that it really is too late, and then what do we do?

Dr. GERSHWIN. As John Koskinen told me sometime back, when we start to go through these, there are countries that are 24 months behind the United States, 36 months behind. It is never too late to do something. And part of the purpose of the U.N. meeting in December was to make it clear to countries that, as behind as they are, they can do an awful lot in 1999 to help themselves out. They may not, and in fact they won't be as well prepared as the United States, but they can do a heck of a lot better and avert a lot of the problems by doing some serious contingency planning and the like.

So it is really hard to put a firm cutoff date; but, frankly, if a country is 24 months behind the United States, and the United States will be prepared without a lot of time to spare, then I would say a lot of the countries, particularly in the developing world, are going to have failures that they have not prepared for and are going to have to deal with the consequences afterward.

The best bet, I think, for these countries is to identify where their problems are most likely to occur and start making plans for how to work around those problems.

Mrs. BIGGERT. Have you seen evidence of these countries identifying these problems since December and since that meeting?

Dr. GERSHWIN. It is probably a little too quick to be able to tell. Some of them just appointed national coordinators for this to get ready for the meeting in December, and a lot of their plans are only going to start rolling in over the next 2 or 3 months. And, frankly, one of the problems we have in trying to assess this is the lack of information, certainly publicly available from abroad, compared to

what is going on in this country, makes it difficult for us to gather a lot of key information about sectors and countries and so on.

In the intelligence community we have other ways to get information, other than what people declare, but the fact is that openly available information would be extremely helpful to us. A lot of countries are simply not providing that at this point because I don't think they themselves even know.

Mrs. BIGGERT. Well then, can you say there really is no problem that there might be an automatic missile launch from China and Russia?

Dr. GERSHWIN. Fortunately, countries like China and Russia are countries that we have for years, for decades, we have studied very carefully their missile systems. I used to do that for a living, before I got into the Y2K business here. And so we know enough about the Russian strategic weapons, the Chinese strategic weapons to be quite confident that those systems should not experience the kinds of failures that would lead to anything automatically launched.

The worry we do have, and as I expressed in my testimony, and particularly for the Russian early warning system, that the Russian early warning system needs some serious scrutiny by the Russians so that they understand the potential failures they could have there, and that they don't misinterpret the information. But in terms of automatic anything, we don't think automatic launches of missiles are conceivable.

Mrs. BIGGERT. I think that Mr. Koskinen stated that the international financial transaction markets were in good shape, and we certainly have been working on that at a domestic level, for example, in Illinois. But what about the Asian financial markets; could this cause a problem there? And then how would that affect other international transactions?

Dr. GERSHWIN. Well, the issue from countries in the Asian area is, since they have been heavily preoccupied with the financial problems over the last many months, it tends to detract from their attention on the Y2K problem. And one thing we have learned about the Y2K problem is, you have to be consistent and energetic in working the problems and then good things will happen.

So, frankly, we are not yet in a position to evaluate on a kind of a regional basis just how well Asian financial solutions will take place. But certainly the countries that have been experiencing problems, it is a real flag that would go up. I indicated in my testimony that we think at least some of the Chinese financial institutions could have some problems. I would certainly worry as well about Japan, just because of the enormous difficulty they have had in the last many months.

Any country experiencing global financial disruptions is going to focus so heavily on that that it could detract from their Y2K fixes.

Mrs. BIGGERT. Have there been any international lawsuits filed over this issue?

Dr. GERSHWIN. Yes, there have, and I don't know if any of my colleagues have any specifics on that. I know there have been already some international litigation being filed. Anybody know? No.

Mrs. BIGGERT. Do you know what the type or nature of the litigation is?

Dr. GERSHWIN. I think it has to do with western information technology companies that have been involved in these countries, and whether they have essentially provided technology and services which warrant Y2K compliance and, hence, are undermining the economies and technologies and companies and so on.

But we do have some specifics on that, not a lot, but it has been building. We could certainly get that for you.

Mrs. BIGGERT. Could you supply that for the record?

Dr. GERSHWIN. Certainly.

Mrs. BIGGERT. Thank you.

Mr. HORN. Without objection it will be put in the record at this point.

[The information referred to follows:]

International Litigation Related to Y2K

Litigation related to the Y2K problem is of major concern to all businesses, particularly banks, throughout the world. Press reports indicate that cases could run the full spectrum of business relationships, pitting companies against their suppliers, companies against their computer software vendors, companies against their legal or accounting firms, and companies against their insurers and banks. Most of the small number of lawsuits filed to date are class-action complaints against software manufacturers who allegedly misrepresented the invulnerability of their products to the Y2K problem.

The Gartner Group, a business and information technology consulting firm in Stamford, Connecticut, has estimated that punitive and compensatory damage awards related to Y2K could reach as much as $1 trillion – a figure which exceeds Gartner's estimate of the total cost of only fixing software problems ($300 billion to $600 billion over a few years surrounding 2000). Gartner readily concedes that the estimate of $1 trillion is sheer guesswork based on the assumption that every dollar in actual damage will generate some multiple in punitive and compensatory damages.

With regard to international litigation, the following are selected comments/examples gleaned from press reports.

- The Edmonton, Alberta, Canada government will hit up computer-industry giants to recoup at least some of its growing costs for exterminating the 2000 computer bug. The Provincial Treasurer said "We're going to be saying, 'This is your equipment, you supplied it to us, you didn't tell us there was a problem.'"
- The UK's high street banks are refusing to sign up to Pledge 2000 -- an initiative to promote Y2K friendly companies – fearing legal action if their computer systems fail come the Millennium.
- A computer analyst in Scotland, who was forced to leave a large insurance company in 1995 due to illness, is suing that company for depriving him of cashing in on the millennium bug chaos. He is suing for money he has lost since 1995 and for potential future earnings.
- A small computer company in Ottawa has learned that its insurance company is no longer willing to cover his business because of the so-called Y2K risks.

Mrs. BIGGERT. Then a question for Mr. Willemssen. Do you agree with Mr. Koskinen that the traffic control system will be totally compliant well in advance of the year 2000?

Mr. WILLEMSSEN. No, I wouldn't agree with that statement, especially well in advance. FAA's air traffic control system still has a lot of risks.

FAA, its Administrator, Administrator Garvey, the Program Manager Ray Long, have done a tremendous job over the last year. Unfortunately, FAA got a very late start on this issue, and they are heavily automated. In some cases that automation is fairly archaic, and it will take a tremendous effort, continued tremendous effort for them to be fully compliant and to test those systems from an end-to-end perspective and have a full understanding of their data exchanges and data flows with other partners, such as airports, airlines, National Weather Service, Department of Defense.

So am I optimistic that they will complete all of that well in advance? No.

Mrs. BIGGERT. They have also put in new computer systems in some of the regions, too, and there has been some downside to that; there have been some failures. You suggested having a moratorium on software changes and other things. How is that going to affect?

Mr. WILLEMSSEN. You have just pointed out another reason for why it is so difficult for FAA. They have multiple locations throughout the country. We are not talking about one system in one place. That increases the complexity that much more. And to the extent they continue installing new systems or modifying existing systems, every time you open up the software, you increase the risk of additional Y2K-related problems. And, therefore, that is something that FAA is going to have to look at as they near the end of 1999.

Once they have certified, for example, a system is compliant, if they go in and modify the software, well, essentially, that is not really compliant anymore, if you have made a lot of adaptive changes or made major modifications to the software. So that is something for them to consider.

Mrs. BIGGERT. Thank you. Thank you, Mr. Chairman.

Mr. HORN. Thank you. Good questions.

Let me just ask a few wind-up questions, although if my colleagues have other questions, fine.

But, No. 1, on the reactors—and the vice chairman comes from a State where much of their electric power is from nuclear reactors in Illinois—what do we know about the types of reactors that we have around the world and the extent to which there can be a malfunction there of some sort that would affect the power grid and power coming out of those reactors?

And if you had to look from the Moon down at the United States and then at Russia and then at France, because the competition on reactors over 30 years has been the United States reactors or the French reactors, what would you be able to tell us as to where is the highest risk that a power grid can go out just because of something that is built into any of those reactors?

Dr. GERSHWIN. I think Russia is the No. 1 problem.

Mr. HORN. How many Chernobyl-type reactors do they still have, or did they change that?

Dr. GERSHWIN. No, they still have roughly the same number they had before because they really have not modernized their reactors.

Mr. HORN. That is about 11 or so?

Dr. GERSHWIN. No, I think there are more than that.

Mr. GREEN. In the mid-fifties.

[The information referred to follows:]

The Number of active Chernobyl-type reactors in Russia, Lithuania, and Ukraine that pose a potential moderate to high risk of radioactive release is 14. There are some 20 reactors of other types in Russia and East Europe that also present a potential moderate to high risk.

Dr. GERSHWIN. There are a number not only in Russia but actually in some of the other countries, in Eastern Europe, Lithuania, places like that.

Those particular reactors are worrisome to us. We have studied in the intelligence community, with the support of the Department of Energy, what we call the most dangerous reactors in the world, apart from just Y2K issues. Russia and its former allies just lead that list.

Those are dangerous in the sense of we didn't think their safety enhancements were very good. These are the very same reactors that have not really received enough Y2K attention in terms of Y2K remediation. And they are, obviously, extremely connected to the electric power grids in Russia and some of the other countries, which can work both ways: failures in electric power grid, causing reactor problems; failures in the reactors, causing overall reduction in the electric power available to run the country.

So when you look at all that, I think the Russian reactor problem and those of some of the other nearby countries is serious, a serious problem.

I should just mention in France, and it is an area obviously we are interested in as well, French reactors are pretty much all of the same design. If there were a Y2K problem in French reactors, it might affect a large number of reactors in France, and that could cause France to have some serious problems.

This is something we will be looking into. I am not raising the issue right now that we are worried about France, but just the nature of nuclear reactors is such that we ought to look particularly carefully at nuclear reactors around the world. And we will be doing that.

In fact, we have a study under way at Pacific Northwest Laboratories in the State of Washington under the Department of Energy guidance, which I asked them to do, to look specifically at reactors and the implications of reactor failures in terms of what could happen in those countries, both from a safety point of view and an energy point of view. So we will be looking very closely at that particular subject area.

Mr. HORN. Is there a problem with the embedded chips within these reactors, or to what degree do they operate on sort of an automatic flow-through; that that power can be shut off under certain circumstances or permitted to go into the distribution system or what?

Dr. GERSHWIN. There are certainly embedded processors in a lot of those systems. We don't necessarily have the exact designs of all those things, so in some cases we have to estimate it. But they are

very complex indeed, in many cases largely because of the safety mechanism and how those are implemented. So nuclear reactors are certainly an area where the embedded processor problem could become significant.

Mr. HORN. If you looked at American reactors the same way you look at Russian reactors—and you know we have had a blackout in the central States, we had a blackout in New York, we had a recent blackout in San Francisco—anything we can learn from what is going on elsewhere? Are we in that danger?

Dr. GERSHWIN. Well, of course, we in the intelligence community don't really study the United States as such, so I can't really say about that.

Mr. HORN. Well, I always felt you should. And when I was in strategic intelligence, we looked at a lot of stuff to see what other people could find. And all you did was go to the Government Printing Office and there was the plans usually for everything.

Dr. GERSHWIN. I know there has been quite a bit of scrutiny already of U.S. nuclear reactors. In fact, when I was at Pacific Northwest Labs last month, one of their experts, who was a nuclear reactor designer, had in fact been visiting some U.S. reactors and had learned how they are dealing with the Y2K problem. And the message he gave me was you have to really know an awful lot about these reactors to identify places where there could be a Y2K problem, and then it is quite fixable.

He was quite optimistic that the U.S. reactors would do well in this Y2K remediation. But he, as a result of that, became more concerned about foreign reactors because he knows how complicated it is to take a look at these things and figure out what to do.

Mr. HORN. Moving to refining and to these huge tankers, to what extent do they pose a problem in terms of embedded chips, microprocessors?

Dr. GERSHWIN. They are very heavily dependent on embedded processors and processor systems for many, many key functions, because they do a lot of monitoring, status monitoring, looking at recent maintenance to make sure that things are being maintained on a proper schedule. So there is quite a bit of date sensitivity in the oil industry and the shipping associated with it.

So that throughout the oil industry, from extraction, refining, shipping and so on, there are just many, many places where Y2K problems can emerge. So that it is a very complicated business, in fact, to take a look at this. And our concern is because of that complexity, the potential for failure is significant. And we know enough about this to know that there is quite a bit of concern being raised about some of the foreign oil companies, particularly located in some of these foreign countries, as to how well they are going to do. It is an area of high interest, obviously now by the President's Council, by a number of folks.

Mr. HORN. To our knowledge at this point, would there be any chance of an environmental spill as a result of something going wrong?

Dr. GERSHWIN. I would just hazard a guess that, yes, that could possibly happen. We haven't specifically looked at that, but that would certainly be within the realm, I would think. Somebody else

might disagree, but I will just give you my top-of-the-head impression.

Mr. HORN. Who will look at that question? Is it EPA, is it the Department of the Interior? Who is going to take a look at the environmental——

Dr. GERSHWIN. I think the Department of Energy and the Environmental Protection Agency would seem like naturals for that issue.

Mr. HORN. We are going to have them in in a couple of weeks. We are going at the laggards that were pretty far behind and trying to find out what the problem is, as well as some of the success stories which we ought to be sharing with the others.

Do any of my colleagues have any other points here they would like to make?

Mrs. MORELLA. This has been excellent testimony. With regard to the prioritizing, what should happen after that is done? You suggest prioritizing in terms of oil, trade, food, pharmaceuticals. I guess you would add nuclear reactors to that.

Dr. GERSHWIN. Yes, and military systems generally.

Mrs. MORELLA. Military systems. What actions would you suggest following prioritizing?

Dr. GERSHWIN. Well, our role, at least in the intelligence community, is to try to assess the likelihood of failures in some of these key infrastructure areas and then assess the implications for the United States, which should, hopefully, lead to ideas for actions the United States could take to reduce the impact on the United States.

If you look at sort of the oil industry example, as we get closer to understanding this, we should be able to have a better sense of a scope of the magnitude of the potential failures. And that should help lead to an assessment of whether that will have a small effect on the United States' interest or a big effect.

Mrs. MORELLA. Have we done anything in terms of prioritizing, or is that just a suggestion?

Dr. GERSHWIN. We are just moving in that direction now. We have a lot of work to do. We are still gathering data, and we have not done a lot of assessment yet, frankly.

Mrs. MORELLA. Right. One of our problems is that we don't have the opportunity to have a continuing resolution when it comes to January 1, 2000. So I do hope you move. It is a great idea. I do hope you get the Council to move very fast on that.

Dr. GERSHWIN. I think we are doing—there is a lot of energy being put into this at this point, by not only the President's Council but by the U.S. intelligence community.

Mrs. MORELLA. Mr. Willemssen, do you have any other comments you want to make?

Mr. WILLEMSSEN. No, other than glad to hear the comments Dr. Gershwin made that there is an increasing focus in this area. We need data in order to make some decisions and understand where our risks are so that we can take appropriate actions.

Mrs. MORELLA. I hope you will both keep us posted, and I look forward to working with you. Thank you. Thank you, Mr. Chairman.

Mr. HORN. Thank you.

Mr. Willemssen, I have just one short question. Months ago I suggested to Mr. Koskinen that he ought to have some people on a weekly report to keep the heat on them. Do you know if they are doing that at all at this point, and are the laggards being separated out from the people that do know what they are doing?

Mr. WILLEMSSEN. Those in the bottom two tiers are reporting monthly to OMB and Mr. Koskinen. One thing you may want to consider is, obviously, the March 31 date is fairly important. It may be something useful for OMB and Mr. Koskinen to report shortly after that date so that we know where indeed we stand as a Federal Government.

And then we have to start shifting the focus away from compliance of individual systems and thinking more about compliance of key business functions and whether they are going to operate as intended; multiple systems, again working together, often across agency boundaries, often involving our State and local governments. That is where a lot of the attention is going to have to be paid in the latter part of 1999.

Mr. HORN. Well, those are helpful suggestions. I share Mrs. Morella's praise for both of you and your testimony and your colleagues that have helped with that.

Today's compelling testimony, I think, further provides evidence that the Federal, State and local governments are striving to identify and solve their problems, but as Mr. Willemssen suggests, there are a lot of ways to go about that, and we can't just make it an afterthought as we concentrate solely on the Federal Government because we have found numerous connections between agencies and the State and county governments, for that matter, that have administered many of these programs for 40 or 50 years. Still, we in Congress are deeply concerned that much work remains. And as the President said last evening, Y2K must not become the first crisis of the 21st century.

In the very near future we will hold hearings to review the status of Y2K efforts at the Departments of Defense and the Postal Service. We have not been involved with the Postal Service, but our understanding is that a report of the Inspector General there seems to require us taking a look at it in conjunction with the Subcommittee on the Postal Service of Government Reform. In addition, we will be delving into the muddy area of Y2K litigation.

As a government and as a Nation we must continue to be industrious and vigilant in these efforts so that we can zap this so-called computer bug that some people still don't believe in. Some think it is a hoax. Some think it is a way to sell books. We have heard every excuse you can think of, but most of us know that, in most situations, we have got a problem, and we ought to deal with it in some managerial, efficient and effective way.

Let me now thank the staff that prepared this hearing, starting with J. Russell George, the staff director and chief counsel of the Government Management, Information, and Technology Subcommittee; Matt Ryan, who we are glad to have back with us, sitting right behind me, a senior policy adviser for the subcommittee; Bonny Heald, who is out there somewhere, and our director of communications and professional staff member, who has been very helpful; Matthew Ebert, our clerk, who puts most of this work to-

gether; and Mason Alinger, the staff assistant for the subcommittee; and then Paul Wicker and Kacey Baker, our interns. We appreciate their help.

And for the Subcommittee on Technology, Richard Russell, the very able staff director of that committee; and Ben Wu, the professional staff member; and Joe Sullivan, is it? Am I reading that right? I have a problem with some people's penmanship, even though I am a former college professor and can read almost anything, who is the clerk on the Technology Subcommittee.

And then for the minority, Faith Weiss is the professional staff member. And Earley Green, staff assistant.

And then our overworked—and we should have taken a recess if we had known we were going to go this long—court reporters, Pam Garland and Cindy Sebo. Thank you both.

With that, this hearing is adjourned.

[Whereupon, at 1:55 p.m., the hearing of the joint subcommittees was adjourned.]

○