

**OVERSIGHT OF THE YEAR 2000 TECHNOLOGY
PROBLEM: LESSONS TO BE LEARNED FROM
STATE AND LOCAL EXPERIENCES**

HEARINGS

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION, AND TECHNOLOGY

OF THE

COMMITTEE ON
GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

FIRST SESSION

—————
JULY 7, 8, AND 9, 1999
—————

Serial No. 106-47

Printed for the use of the Committee on Government Reform



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

—————
U.S. GOVERNMENT PRINTING OFFICE

60-939 CC

WASHINGTON : 1999

COMMITTEE ON GOVERNMENT REFORM

DAN BURTON, Indiana, *Chairman*

BENJAMIN A. GILMAN, New York	HENRY A. WAXMAN, California
CONSTANCE A. MORELLA, Maryland	TOM LANTOS, California
CHRISTOPHER SHAYS, Connecticut	ROBERT E. WISE, JR., West Virginia
ILEANA ROS-LEHTINEN, Florida	MAJOR R. OWENS, New York
JOHN M. McHUGH, New York	EDOLPHUS TOWNS, New York
STEPHEN HORN, California	PAUL E. KANJORSKI, Pennsylvania
JOHN L. MICA, Florida	PATSY T. MINK, Hawaii
THOMAS M. DAVIS, Virginia	CAROLYN B. MALONEY, New York
DAVID M. McINTOSH, Indiana	ELEANOR HOLMES NORTON, Washington, DC
MARK E. SOUDER, Indiana	CHAKA FATTAH, Pennsylvania
JOE SCARBOROUGH, Florida	ELIJAH E. CUMMINGS, Maryland
STEVEN C. LATOURETTE, Ohio	DENNIS J. KUCINICH, Ohio
MARSHALL "MARK" SANFORD, South Carolina	ROD R. BLAGOJEVICH, Illinois
BOB BARR, Georgia	DANNY K. DAVIS, Illinois
DAN MILLER, Florida	JOHN F. TIERNEY, Massachusetts
ASA HUTCHINSON, Arkansas	JIM TURNER, Texas
LEE TERRY, Nebraska	THOMAS H. ALLEN, Maine
JUDY BIGGERT, Illinois	HAROLD E. FORD, JR., Tennessee
GREG WALDEN, Oregon	JANICE D. SCHAKOWSKY, Illinois
DOUG OSE, California	
PAUL RYAN, Wisconsin	BERNARD SANDERS, Vermont (Independent)
HELEN CHENOWETH, Idaho	
DAVID VITTER, Louisiana	

KEVIN BINGER, *Staff Director*

DANIEL R. MOLL, *Deputy Staff Director*

DAVID A. KASS, *Deputy Counsel and Parliamentarian*

CARLA J. MARTIN, *Chief Clerk*

PHIL SCHILIRO, *Minority Staff Director*

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

STEPHEN HORN, California, *Chairman*

JUDY BIGGERT, Illinois	JIM TURNER, Texas
THOMAS M. DAVIS, Virginia	PAUL E. KANJORSKI, Pennsylvania
GREG WALDEN, Oregon	MAJOR R. OWENS, New York
DOUG OSE, California	PATSY T. MINK, Hawaii
PAUL RYAN, Wisconsin	CAROLYN B. MALONEY, New York

EX OFFICIO

DAN BURTON, Indiana

HENRY A. WAXMAN, California

J. RUSSELL GEORGE, *Staff Director and Chief Counsel*

MATT RYAN, *Senior Policy Director*

GRANT NEWMAN, *Clerk*

CONTENTS

	Page
Hearing held on:	
July 7, 1999	1
July 8, 1999	125
July 9, 1999	317
Statement of:	
Ho, Alan D., Y2K corporate manager, Commonwealth Edison; Dale Jensen, director, Y2K customer communications, Ameritech; Craig Whyte, director, regional community relations, NICOR Gas; Philip Pagano, executive director, METRA; Gary Mielak, vice president and chief technical officer, Edward Hospital	210
Kettlewell, Larry, information resource manager for Federal and State affairs, Kansas Department of Administration	52
Lobeck, Al, news director, WIBW Radio, Kansas Broadcasters	110
McKenzie, Shawn, Southwestern Bell	80
Moser, Joy, Adjutant General's Department, Public Affairs Office	64
Park, Bud, year 2000 project office manager, Western Resources	75
Roosen, Jim, Y2K program manager, Detroit Edison; Raymond Lozano, manager of Statewide community relations, Michigan Consolidated Gas, accompanied by Tom Motsinger, director, information and technology management; James Johnson, vice president of computing and information technology, Wayne State University; Don Potter, Southeast Michigan Health and Hospital Council; and Dan McDougall, director, southeast Michigan information center, United Way	448
Rubeck, Anne, director, communication technology, Kansas Hospital Association	98
Splichal, Edwin, chairman, Y2K task force Kansas Bankers Association ...	102
Sullivan, Morey, information resource manager, Kansas Department of Administration	48
Surdu, George, director, technical services organization, Ford Motor Co.; Don Costantino, director, corporate year 2000 program, General Motors Corp.; Roger Buck, DaimlerChrysler Corp.; and John Parker, vice president, information services, Northwest Airlines, Inc.	413
Swift, Clint, director of bank technology, Bank Administration Institute; Delores Croft, seniors policy advisor, Illinois Attorney General's Office; Leonard Harris, president, Chatham Food Center; Ron Clark, treasurer, Illinois Ayers Oil Co.; Monty Johnson, communications coordinator, CITGO Gas; Mike Skarr, president and CEO, Naperville area Chamber of Commerce; and Ed Paulson, author of Year 2000 Crisis Survival in 10 Minutes, professional engineer, financial expert	258
White, Jeff, director, budget research and information technology, city of Topeka	58
Willemsen, Joel, Director, Civil Agencies Information Systems, General Accounting Office	9
Willemsen, Joel C., Director, Civil Agencies Information Systems, General Accounting Office; George Boersma, director, management and budget, State of Michigan; Captain Ed Buikema, deputy State director of emergency management, Michigan State Police; Arun Gulati, deputy director, Department of Information Processing, Wayne County, MI; and Kathleen Leavey, deputy director, Detroit Water and Sewerage Department	324

	Page
Statement of—Continued	
Willemsen, Joel C., Director, Civil Agencies Information Systems, General Accounting Office; Mary Reynolds, chief technology officer, Illinois Governor's Office; Don Carlsen, director of information systems, Department for the city of Naperville; Tom Mefferd, coordinator, DuPage County Office of Emergency Management; and Robert Martin, manager of water operations, DuPage Water Commission	135
Letters, statements, etc., submitted for the record by:	
Biggert, Hon. Judy, a Representative in Congress from the State of Illinois, prepared statement of	133
Boersma, George, director, management and budget, State of Michigan, prepared statement of	366
Buck, Roger, DaimlerChrysler Corp., prepared statement of	429
Buikema, Captain Ed, deputy State director of emergency management, Michigan State Police, prepared statement of	373
Carlsen, Don, director of information systems, Department for the city of Naperville, prepared statement of	181
Clark, Ron, treasurer, Illinois Ayers Oil Co., prepared statement of	277
Costantino, Don, director, corporate year 2000 program, General Motors Corp., prepared statement of	421
Gulati, Arun, deputy director, Department of Information Processing, Wayne County, MI, prepared statement of	379
Harris, Leonard, president, Chatham Food Center, prepared statement of	266
Ho, Alan D., Y2K corporate manager, Commonwealth Edison, prepared statement of	212
Horn, Hon. Stephen, a Representative in Congress from the State of California, prepared statements of	6, 129, 321
Jensen, Dale, director, Y2K customer communications, Ameritech, prepared statement of	233
Johnson, James, vice president of computing and information technology, Wayne State University:	
Letter dated August 9, 1999	506
Prepared statement of	473
Johnson, Monty, communications coordinator, CITGO Gas, prepared statement of	287
Kettlewell, Larry, information resource manager for Federal and State affairs, Kansas Department of Administration, prepared statement of ...	54
Leavey, Kathleen, deputy director, Detroit Water and Sewerage Department, prepared statement of	386
Lobeck, Al, news director, WIBW Radio, Kansas Broadcaster, prepared statement of	112
Lozano, Raymond, manager of Statewide community relations, Michigan Consolidated Gas, prepared statement of	464
Martin, Robert, manager of water operations, DuPage Water Commission, prepared statement of	198
McDougall, Dan, director, southeast Michigan information center, United Way, prepared statement of	498
McKenzie, Shawn, Southwestern Bell, prepared statement of	82
Mefferd, Tom, coordinator, DuPage County Office of Emergency Management, prepared statement of	186
Mielak, Gary, vice president and chief technical officer, Edward Hospital, prepared statement of	241
Moser, Joy, Adjutant General's Department, Public Affairs Office, prepared statement of	66
Pagano, Philip, executive director, METRA, prepared statement of	249
Park, Bud, year 2000 project office manager, Western Resources, prepared statement of	77
Parker, John, vice president, information services, Northwest Airlines, Inc., prepared statement of	434
Paulson, Ed, author of Year 2000 Crisis Survival in 10 Minutes, professional engineer, financial expert, prepared statement of	303
Potter, Don, Southeast Michigan Health and Hospital Council, prepared statement of	482
Reynolds, Mary, chief technology officer, Illinois Governor's Office, prepared statement of	177

	Page
Letters, statements, etc., submitted for the record by—Continued	
Roosen, Jim, Y2K program manager, Detroit Edison, prepared statement of	452
Rubeck, Anne, director, communication technology, Kansas Hospital Association, prepared statement of	100
Ryan, Jim, Attorney General, Illinois, prepared statement of	273
Skarr, Mike, president and CEO, Naperville area Chamber of Commerce, information concerning local resources	298
Splichal, Edwin, chairman, Y2K task force Kansas Bankers Association, prepared statement of	104
Sullivan, Morey, information resource manager, Kansas Department of Administration, prepared statement of	50
Surdu, George, director, technical services organization, Ford Motor Co., prepared statement of	416
Swift, Clint, director of bank technology, Bank Administration Institute, prepared statement of	261
White, Jeff, director, budget research and information technology, city of Topeka, prepared statement of	61
Willemsen, Joel, Director, Civil Agencies Information Systems, General Accounting Office, prepared statements of	11, 137, 326

**OVERSIGHT OF THE YEAR 2000 TECHNOLOGY
PROBLEM: LESSONS TO BE LEARNED FROM
STATE AND LOCAL EXPERIENCES**

WEDNESDAY, JULY 7, 1999

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION, AND TECHNOLOGY,
COMMITTEE ON GOVERNMENT REFORM,
Topeka, KS.

The subcommittee met, pursuant to notice, at 1 p.m., at the Kansas State Capitol, 300 SW 10th Street, Old Supreme Court Room, Topeka, KS, Hon. Jim Ryun presiding.

Present: Representatives Horn and Ryun.

Staff present: Subcommittee on Government Management, Information, and Technology: J. Russell George, staff director and chief counsel; Matt Ryan, senior policy director; and Grant Newman, clerk. Representative Ryun's Office: Michele Butler, chief of staff; Mark Kelly, legislative director; and Jay Rinehart, press secretary.

Mr. RYUN. Thank you all very much for coming today. I think your presence indicates that there is a great deal of interest in the subject. Today will be a time when we can discuss and determine some of those potential problems, as well as some of the solutions that have been arrived at.

Let me do a couple of business things. First of all, and this is not a business thing, I want to introduce some people who are here today. I want to begin with my wife Anne who is in the corner. Say hello to everyone.

[Applause.]

Mr. RYAN. I would like to introduce you to my staff that are here today as well, Michele Butler who has worked tirelessly on this. Michele is over here, she's my chief of staff in Kansas. We also have Mark Kelly up in front, Mark Kelly is my legislative director. Jay Rineheart is here, he is working with the press, he is my press person, they are all here to help you. If there are any questions, feel free to talk with them.

I also want to introduce to you a good friend of mine and colleague who has been very instrumental in helping bring greater identification to the Y2K issue. In Washington we often turn to Chairman Horn and say, "How are we doing?" And so today you will have that opportunity. He is chairman of the House Subcommittee on Government Management, Information, and Technology. He is also the chairman of the House of Representatives Task Force for the Year 2000. He has designated the year 2000

problem as his top priority, as I think it should be. He is an expert in Congress on this problem and in fact this morning, if some of you had the privilege of listening to WIBW with Jim Case, we went over some of the issues and some of what was happening. He will be here today to answer some of your questions, along with the panelists. And as we begin, I would like to turn to Chairman Horn and have you welcome him as well. Thank you very much.

[Applause.]

Mr. HORN. Thank you very much, Jim. Jim does a terrific job in Washington, he sits on three committees, which is one more than I sit on, so he has got a lot of things going for Kansas. And this is an international problem as well as a national problem. We are delighted to be in Topeka, it's a wonderful city. I have been here about five times before because I have some good friends living here starting with my junior year in college.

This hearing of the House Subcommittee on Government Management, Information, and Technology is not only going to be in Kansas on this particular trip, we are going to Illinois tomorrow and Detroit, MI the next day. We did this last year and went to Louisiana and Texas and New York, you name it. We haven't missed too many cities in some kind of a hearing. We are an investigative committee and under the rules of the House and the Committee on Governmental Affairs in the Senate, as they call it. We do swear in all witnesses. So Mr. Ryun who is acting chair will swear in each panel as it comes that they will tell the whole truth and nothing but the truth to this particular investigation.

The year 2000 computer problem affects just about every aspect of Federal, State, and local government operations. Furthermore, it affects private sector organizations and could impact the lives of most of us. From Social Security to utilities to local emergency management, these are all important issues. The so-called year 2000 computer bug or the millennium bug, whatever you want to call it, has certainly been a large management and technological challenge, but it is mostly a management challenge. There is no silver bullet to solve it. Everybody knew that in the 1960's when they said, wait a minute, we have got this huge computer that would fill this whole chamber; your personal computer today has more capacity than those computers in a chamber this large. They said, hey, why don't we just put in '67 instead of 1967, and we went to the two digit year to save space in the memory. Of course they knew that when the year 2000 came, it would be 00 and the computer wouldn't know if it was 1900 or 2000. And many started working on this years ago, the Federal Government has been lagging except for the Social Security Administration which started on its own with no Presidential prodding, be it Republican or Democrat, and they started in 1989 and they are 100 percent compliant. And the only other one that we have looked at recently on programming areas is the weather service. And I know that must be good news to Kansas with your tremendous agricultural resources and farmers getting up at 4 a.m., and 5 a.m., wanting to know what the weather is going to be. So they are in good shape. And then we have the various report cards. We have noted that the critical mission systems in particular agencies are coming along, but it doesn't mean that some of the problematic areas of that agency

have all of the pieces together. And in our future reporting to the Nation on this, both the Senate committee and our own committee will stress that point, it doesn't do much good to have a lot of the agency's computing operations corrected, but it's a program that deals with the people and has to put out checks, has to do analysis in order to do something else, and so we are going to look at that over the next few months and we will be in various parts of the country to do that.

Back in April 1996 this subcommittee was the first to bring the question up in Congress. The Senate finally got around to it in early 1998 and we urged the President to do a number of things, one is to get a person in charge, which really wasn't happening. And No. 2 is to use the bully pulpit, as Theodore Roosevelt said, and talk to the people about this so that they don't panic, because we know from every witness that we have ever had that the longer delay occurs, the more costly labor and human resources would be to get the problem solved.

Current estimates show that the Federal Government will spend nearly \$9 billion by the end of this fiscal year to remedy the executive branch computers. The legislative branch is on its own and so is the Supreme Court. But that's a drop in the bucket compared to the extensive executive branch. And we will probably get to \$10 billion. But our estimates early on in 1996 was that it would be \$30 billion, so in that sense, if that sticks, we are doing one-third of what all of the experts said, and we will do it right by January 1, 2000.

Recently, the President's Office of Management and Budget identified 43 essential Federal programs, I mentioned Social Security and I mentioned the weather, well there are two more we are looking at very closely, and that's Medicare which affects at least 43 million people, and the Air Traffic Control system. I told the Administrator of the FAA that I will be taking my every other week flight from Dulles International Airport to Los Angeles International Airport on January 1st just to see what happens. She will go from Washington to La Guardia, which is 45 minutes to my 5 hours. And I told her not to mess around with the controllers before we both board the plane. So with those 43 programs, 10 of which are federally funded State run programs, and we will hear a lot of good testimony today on that, Medicaid, food stamps, unemployment insurance, child support enforcement, several of these State run programs are not scheduled to be ready for the year 2000 until December, leaving little, if any, time to fix unforeseen problems.

The data exchanges, which is a major thing we are looking at, and the interdependencies between computers in the field and computers in the Federal Government and State government and your local government, they exist at all levels and throughout the private sector. And a single failure in the chain of the information could have severe repercussions if they don't get all of those interrelations straightened out. For example, let me briefly illustrate how the U.S.' Social Security program uses computers. The Social Security Administration maintains data containing pertinent Social Security payment information for eligible citizens. When the payments are made, Social Security sends the payment data every

month to the Department of the Treasury's Financial Management Service. This service then cuts the Federal check which is then electronically deposited directly into the person's bank account at a local financial institution. Three organizations move and manipulate data to make these payments happen; each uses its own network of computers. If a payment is mailed to an individual's home, the U.S. Postal Service then plays a key role in the delivery of that check.

The bottom line is that if any one of these entities fails, from the Federal Government to the local bank or the Postal Service, a deserving individual will not receive a payment in time. And there are 435 Members from the States, 5 Members from the territories and 100 U.S. Senators who all know that they would have lines outside their district office. And Representative Ryun is right across the street in the Mercantile building, very accessible, and we don't want to see that happen. So we all have a vested interest in making sure it doesn't happen. But it takes thousands of people to get this job done.

If you multiply the clients, the millions of people who receive those benefits, you know the magnitude of it, one check a month and 43 million people are affected by that. The other is Social Security, 50 million people, they also have disability checks that go out.

But for computers to work we need power, energy. One of the most essential questions we are asking in the year 2000 challenge is, "Will the lights stay on?" We will have representatives from the power industry talking to us about that in this area. Without electricity our modern society would be relegated back to the proverbial "Stone Age."

From a personal standpoint I realize that when confronted with a personal emergency, I can call "911" for assistance and feel confident that the phone will be answered promptly and that a competent authority will respond rapidly. Year 2000 computer problems present other potentially serious threats at local levels, from the potential interruption of a citizen's call for police assistance to delays in a State's ability to request emergency or disaster assistance from the Federal Government.

Congressman Ryun is unquestionably the greatest American miler of all time. He raced as fast as he could toward a measurable and foreseeable goal—1 mile and a finish line. Our Nation's race to solve the year 2000 problem requires the same preparation, determination, and stamina as that of Congressman Ryun. And this is what we have tried to note to the administration, it doesn't matter whether they are Democrats or Republicans, frankly the President has not had the tools until this last year to really deal with this matter effectively.

And we know, as I said earlier, there are 177 days to go to January 1st and the clock is ticking and can't be moved and the testimony we receive today here in Topeka will help our understanding of the full extent of the year 2000 computer problem.

I would like to mention a few procedural things in this hearing before I turn it over to Congressman Ryun to preside. We are going to be passing cards out, for those of you who have questions, please write out the question. That will enable us to get more questions that we can ask either Mr. Ryun or myself. So some of our staff

will be going along on both sides, just put your hand up, they will give you a card and then if there are five cards with the same question, the staff will get it down to one question and that way we can meet most of your needs. And then we have to run for a plane to Chicago. Mr. Ryun stays here with his constituents.

The testimony we think will be very welcome and helpful here. So that's the cards. And then after Mr. Ryun swears in the witnesses, or if he wants me to swear them in, the witnesses who are already panel one before us, and when he introduces them, the transcript they have sent us, the presentation is excellent that each one of them has written, that immediately goes in the hearing record when their name is introduced. And then we will have them speak from the heart for 5 minutes and boil that down in oral testimony. We have all read your presentations, that's what's going in the hearing record. But in order for everybody to get into a dialog, especially panel one, with both of us, that's the best way to do it we've found from a lot of experience in that.

We then will go into recess to our next hearing in Illinois from here. So I'm delighted now to turn it over to Mr. Ryun to preside and chair the meeting and we will follow his direction from now on out.

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

DAN BURTON, INDIANA
 CHAIRMAN
 BENJAMIN A. GRUBIN, NEW YORK
 CONSTANCE A. MORELLA, MARYLAND
 CHRISTOPHER SHAYS, CONNECTICUT
 WEA ROSALETTINER, FLORIDA
 JIMM MORGAN, NEW YORK
 STEPHEN HORN, CALIFORNIA
 JOHN L. MICA, FLORIDA
 THOMAS M. DAVIS II, VIRGINIA
 DAVID H. MONTGOMERY, INDIANA
 MARK E. SOUDER, INDIANA
 JOE SCHROEDER, FLORIDA
 STEVEN C. LACOUTURETT, OHIO
 MARSHALL JAMES SANDFORD, SOUTH CAROLINA
 BOB BARR, GEORGIA
 DAN MILLER, FLORIDA
 ISA HUTCHINSON, ARKANSAS
 LEE TERRY, NEBRASKA
 JOEY BIGGERT, ILLINOIS
 OREG WALDEN, OREGON
 DOUG COSE, CALIFORNIA
 PAUL RYAN, WISCONSIN
 JOHNY DOOLITTLE, CALIFORNIA
 HELEN CHENOWETH, IDAHO

ONE HUNDRED SIXTH CONGRESS

Congress of the United States
House of Representatives

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

MAJORITY 1202 225-5674
 MAJORITY 1201 225-5051
 TTY 202 225-4952

FRANK A. WAXMAN, CALIFORNIA
 RANKING MEMBER
 TOM LANTOS, CALIFORNIA
 ROBERT E. WISE, JR., WEST VIRGINIA
 VALERIE O'DWYER, NEW YORK
 LOU PATRICK TONGE, NEW YORK
 PAUL E. SANDORS, PENNSYLVANIA
 SARY A. COSGROVE, CALIFORNIA
 PATRY T. MUIR, HAWAII
 CAROLYN B. MALONEY, NEW YORK
 ELIZABETH HOLMES NORRTON
 DISTRICT OF COLUMBIA
 CHAKA FATTAH, PENNSYLVANIA
 ELIJAH E. CANNON, MARYLAND
 DENNIS J. KUCINICH, OHIO
 ROGER BLANDFORD, ILLINOIS
 DANNY K. DAVIS, ILLINOIS
 JOHNNY TERNEY, MASSACHUSETTS
 JIM TURNER, TEXAS
 THOMASIN ALLEN, IOWA
 HAROLD E. FORD, JR., TENNESSEE

BERNARD SANDERS, VERMONT,
 INDEPENDENT

“Oversight of the Year 2000 Problem: Lessons to Be Learned from State and Local Experiences”
Opening Statement of Chairman Stephen Horn (R-CA)
Subcommittee on Government Management, Information, and Technology
July 7, 1999
Topeka, Kansas

This hearing of the House Subcommittee on Government Management, Information, and Technology, will come to order. I would like to welcome and thank Congressman Jim Ryun for being such a gracious host as the subcommittee meets in the city of Topeka.

The Year 2000 computer problem affects just about every aspect of Federal, State, and local government operations. Furthermore, it affects private sector organizations and could impact the lives of most individuals. From Social Security to utilities to local emergency management, the Year 2000 computer bug has certainly been a large management and technological challenge for all of us. No single organization, city, State or even country can solve the Year 2000 problem alone.

The problem, of course, dates back to the mid-1960s when programmers, seeking to conserve limited computer storage capacity, began designating the year in two digits rather than four. The year 1967, for example, simply appeared as ‘67.’ Regardless, now we all must deal with it.

More than three years ago, our subcommittee held the first Congressional hearing on the Year 2000 problem. Since that time, we have held almost 30 hearings and issued 8 “report cards” to monitor the status of the Federal Government’s Year 2000 computer solutions.

Current estimates show that the Federal Government will spend nearly 9 billion dollars to fix its computer systems. I have often said that figure will easily reach 10 billion dollars.

Recently, the President’s Office of Management and Budget identified 43 essential Federal programs such as Social Security, Medicare, and the nation’s Air Traffic Control system. Each day, these programs provide critical services to millions of Americans. Of these 43 programs, 10 are Federally funded, State run programs including Medicaid, Food Stamps, Unemployment Insurance, and Child Support Enforcement. Several of these State run programs are not scheduled to be ready for the Year 2000 until December, leaving little, if any, time to fix unforeseen problems.

Data exchanges and interdependencies exist at all levels of government and throughout the private sector. A single failure in the chain of information could have severe repercussions.

For example, let me briefly illustrate how the United States' Social Security program uses computers. The Social Security Administration maintains data containing pertinent Social Security payment information for eligible citizens. When payments are made, the Social Security Administration sends payment data to the Department of the Treasury's Financial Management Service. This Service then "cuts the Federal check," which is then electronically deposited directly into a person's bank account at a local financial institution. Three organizations move and manipulate data to make these payments; each uses its own network of computers. If a payment is mailed to an individual's home, the United States Postal Service then plays a key role.

The bottom line is: If any one of these entities fails, from the Federal Government to the local bank or Postal Service, a deserving individual will not receive the payment. Now multiply this situation by the millions of people that receive Social Security benefits and you can appreciate the magnitude of just one aspect of the Year 2000 issue. Fortunately, the Social Security Administration has been working on this problem for 10 years and is in good shape.

But, for computers to work, we need power. One of the most essential questions concerning the Year 2000 challenge is, "will the lights stay on?" Without electricity, our modern society would be relegated back to the proverbial "Stone Age."

From a personal standpoint, I realize that when confronted with a personal emergency, I can call "911" for assistance and feel confident that the phone will be answered promptly and that a competent authority will respond rapidly. Year 2000 computer problems present other potentially serious threats at local levels, from the potential interruption of a citizen's call for fire or police assistance to delays in a State's ability to request emergency or disaster assistance from the Federal Government.

Congressman Ryun is unquestionably the greatest American miler of all time. He raced as fast as he could towards a measurable, foreseeable goal...one mile and a finish line. Our nation's race to solve the Year 2000 problem requires the same preparation, determination, and stamina as that of Congressman Ryun's.

One thing is for sure, there are only about 177 days until January 1, 2000, and the clock is ticking. Accordingly, the testimony we receive today will help our understanding of the full extent of the Year 2000 computer problem.

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

Mr. RYUN. Mr. Chairman, thank you very much. Again, I want to welcome everyone. I want to say thank you to the panelists for coming. I don't think any of us fully know what will happen at the end of the year and the purpose in today's forum is to provide information to all of you that are listening.

What I have done is organized two panels. The first panel is going to give the government's perspective on the status and compliance of the government with the Y2K challenge. Let me introduce who's on the panel. First of all, Joel Willemsen, who is the Director of Civil Agencies Information Systems at the General Accounting Office. It's the Federal Government office that oversees the effectiveness of government programs and its agencies. The GAO's chief source of concern for Y2K problems is the readiness of State and local governments. Joel is the GAO's Director for Civil Agencies Information Systems, he has testified before Congress many times about the status of the Y2K preparations. I know you look forward to hearing from him and I look forward to hearing your testimony Joel.

Next we have Morey Sullivan, information resource manager for the Kansas Department of Administration. Governor Graves has been active in pursuing Y2K compliance since 1996. The department of Administration Division of Information Systems and Communications is the designated organization for coordinating and reporting on the State's year 2000 efforts. Mr. Sullivan is the information manager for the State, he will be educating us on the State's activity and the level of preparedness for this next year.

Seated next to him in the middle is Larry Kettlewell, the year 2000 Federal and local interface manager of the Kansas Department of Administration. Larry advises the State's chief information technology officer on the status of Federal and State interfaces. And he also serves as project manager for the State and local interface testing program. He will be discussing how the State of Kansas deals with the Federal Government on this issue.

Next to him is Jeff White. Jeff is director of budget research and information technology for the city of Topeka. The city started addressing this particular issue back in January 1998, focusing primarily on water, sewers, and public safety issues. Jeff has been working hard on the city's compliance since the beginning of the year and we will look forward to his testimony as well.

The last panelist is Joy Moser. She is public affairs officer for the State Adjutant General's Office. The Kansas Division of Emergency Management has provided timely information to help people with managing Y2K. The Adjutant General has sent out several different mailings, one of which is the Year 2000 Survival Test, another is the Executive Survival Guide for the Year 2000 and the Year 2000 Workbook Book. She will be our final panelist and we look forward to your testimony and remarks.

Mr. Chairman, would you like to swear everyone in?

Mr. HORN. Certainly. Would you stand and raise your right hands, please.

[Witnesses sworn.]

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

Mr. RYUN. We will begin with the first panelist.

**STATEMENT OF JOEL WILLEMSSEN, DIRECTOR, CIVIL AGEN-
CIES INFORMATION SYSTEMS, GENERAL ACCOUNTING OF-
FICE**

Mr. WILLEMSSEN. Thank you, Congressman Ryun, Mr. Chairman, thank you for inviting the GAO to testify today. As requested, I will briefly summarize our statement on the Y2K readiness of Federal Government, State, and local governments and key economic sectors.

Regarding the Federal Government, the most recent reports indicate continued progress in fixing, testing, and implementing mission-critical systems. Nevertheless, numerous critical systems must still be made compliant and must undergo independent verification and validation. Our own reviews of selected agencies have shown an uneven progress and remaining risk in addressing Y2K. And that points again to the criticality of business continuity and contingency planning.

As we look beyond individual systems and individual agencies, the Federal Government's future actions will also need to be increasingly focused on making sure that its high priority programs are compliant. In line with this, OMB has identified 43 high impact programs such as Medicare and Social Security. As you know, Mr. Chairman, we are currently reviewing those programs for you. At this point it's very clear that much additional work is needed on almost all of these programs to make sure that they are ready in time by the turn of the century.

Available information on the Y2K readiness of State and local governments also indicates that additional work remains. For example, according to recent information on States reported to the National Association of State Information Resource Executives about 18 States have completed implementing less than 75 percent of their mission-critical systems. State audit organizations have also identified significant Y2K concerns in areas such as testing, embedded systems and contingency planning.

Recent reports have also highlighted Y2K issues at the local government level. For example, a March 1999 National League of Cities poll of over 400 representatives found that almost 70 stated that they would finish 75 percent or less of their systems by January 1, 2000.

Another area of risk is represented by the Federal Human Services programs which are administered by the States such as Medicaid, food stamps, unemployment insurance, and child support enforcement. Of the 43 high impact programs identified by OMB, 10 of those are the State administered programs.

OMB reported data on the systems supporting these programs show that numerous States are not planning to be ready until close to the end of the year. Specifically, a large number of State systems are not due to be compliant until the last quarter of 1999. This is based on data that has not yet been independently verified.

If we look at the risks beyond those faced by the Federal Government and the State and local governments, Y2K also poses a serious challenge to the public infrastructure, key economic structures and to other countries. We have made a number of recommendations to John Koskinen who is the chairman of the President's Y2K Conversion Council. And the Council has made strides in obtaining

needed readiness information in these areas. Nevertheless, there is a good deal of variance among these critical sectors, and, accordingly, there is going to be over the next 6 months a need for continuing emphasis to make sure that the information on the readiness of these sectors is provided to the citizens of the country so that we can have a better understanding of where our risks are and the public can therefore be best positioned with that information.

That concludes the summary of my statement. After the panel is through, I will be pleased to address any questions you may have. [The prepared statement of Mr. Willemsen follows:]

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Government Management,
Information and Technology, Committee on Government
Reform, House of Representatives

For Release on Delivery
Expected at
1 p.m. CDT
Wednesday,
July 7, 1999

YEAR 2000
COMPUTING
CHALLENGE

Readiness Improving
But Much Work
Remains to Avoid
Disruption of Critical
Services

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



Mr. Chairman and Members of the Subcommittee:

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 a high-risk area for the federal government.² Since that time, we have issued over 120 reports and testimony statements detailing specific findings and numerous 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 challenges that remain in correcting its systems; identify state and local government Year 2000 issues; and provide an overview of available information on the readiness of key public infrastructure and economic sectors.

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

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

³A list of these publications is included as an attachment to this statement. These publications can be obtained through GAO's World Wide Web page at www.gao.gov/y2kr.htm.

⁴Year 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 RISK OF
YEAR 2000 DISRUPTIONS

The public faces the 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
- 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 signed an executive order that established the President's Council on Year 2000 Conversion, chaired 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.

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

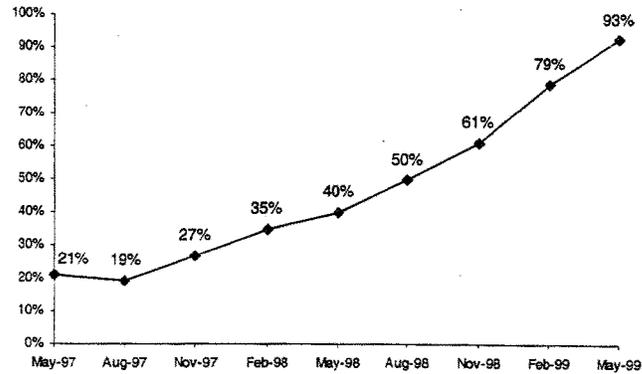
⁶Defense Computers: Year 2000 Computer Problems Threaten DOD Operations (GAO/AIMD-98-72, April 30, 1998).

IMPROVEMENTS MADE BUT
MUCH WORK REMAINS

Addressing the Year 2000 problem is 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 costs and business continuity and contingency plans.

The federal government's most recent reports show improvement in addressing the Year 2000 problem. While much work remains, the federal government has significantly increased its percentage of mission-critical systems that are reported to be Year 2000 compliant, as chart 1 illustrates. In particular, while the federal government did not meet its goal of having all mission-critical systems compliant by March 1999, as of mid-May 1999, 93 percent of these systems were reported compliant.

Chart 1: Mission-Critical Systems Reported Year 2000 Compliant, May 1997-May 1999

Source: May 1997 – May 1999 data are from the OMB quarterly reports.

While this reported progress is notable, OMB reported that 10 agencies have mission-critical systems that were not yet compliant.⁷ In addition, as we testified in April, some of the systems that were not yet compliant support vital government functions.⁸ For example, some of the systems that were not compliant were among the 26 mission-critical systems that the Federal Aviation Administration (FAA) has identified as posing the greatest risk to the National Airspace System—the network of equipment, facilities, and information that supports U.S. aviation operations.

Additionally, not all systems have undergone an independent verification and validation process. For example, in April 1999 the Department of Commerce awarded a contract for independent verification and validation reviews of approximately 40 mission-critical systems that support that Department's most critical business processes. These reviews

⁷The 10 agencies were the Departments of Agriculture, Commerce, Defense, Energy, Health and Human Services, Justice, Transportation, Treasury; the National Aeronautics and Space Administration; and the U.S. Agency for International Development.

⁸Year 2000 Computing Challenge: Federal Government Making Progress But Critical Issues Must Still Be Addressed to Minimize Disruptions (GAO/T-AIMD-99-144, April 14, 1999).

are to continue through the summer of 1999. In some cases, independent verification and validation of compliant systems have found serious problems. For example, as we testified this past February,⁹ none of 54 external mission-critical systems of the Health Care Financing Administration reported by the Department of Health and Human Services (HHS) as compliant as of December 31, 1998, was Year 2000 ready, based on serious qualifications identified by the independent verification and validation contractor.

Reviews Show Uneven Federal Agency Progress

While the overall 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. For example:

- In March we testified that FAA had made tremendous progress over the prior year.¹⁰ However, much remained to be done to complete validating and implementing FAA's mission-critical systems. Specifically, the challenges that FAA faced included (1) ensuring that systems validation efforts were adequate, (2) implementing multiple systems at numerous facilities, (3) completing data exchange efforts, and (4) completing end-to-end testing. Because of the risks associated with FAA's Year 2000 program, we have advocated that the agency develop business continuity and contingency plans.¹¹ FAA agreed and has activities underway, which we are currently reviewing.
- In May we testified¹² that the Department of Education had made progress toward addressing the significant risks we had identified in September 1998¹³ related to systems testing, exchanging data with internal and external partners, and developing business continuity and contingency plans. Nevertheless, work remained ongoing in these areas. For example, Education had scheduled a series of tests with its data exchange partners, such as schools, through the early part of the fall.

⁹Year 2000 Computing Crisis: Readiness Status of the Department of Health and Human Services (GAO/T-AIMD-99-92, February 26, 1999).

¹⁰Year 2000 Computing Crisis: FAA Is Making Progress But Important Challenges Remain (GAO/T-AIMD/RCED-99-118, March 15, 1999).

¹¹FAA Computer Systems: Limited Progress on Year 2000 Issue Increases Risk Dramatically (GAO/AIMD-98-45, January 30, 1998); GAO/T-AIMD-98-251, August 6, 1998; and GAO/T-AIMD/RCED-99-118, March 15, 1999.

¹²Year 2000 Computing Challenge: Education Taking Needed Actions But Work Remains (GAO/T-AIMD-99-180, May 12, 1999).

¹³Year 2000 Computing Crisis: Significant Risks Remain to Department of Education's Student Financial Aid Systems (GAO/T-AIMD-98-302, September 17, 1998).

- Our work has shown that the Department of Defense and the military services face significant problems.¹⁴ In March we testified that, despite considerable progress made in the preceding 3 months, Defense was still well behind schedule.¹⁵ We found that DOD faced two significant challenges: (1) completing remediation and testing of its mission-critical systems and (2) having a reasonable level of assurance that key processes will continue to work on a day-to-day basis and key operational missions necessary for national defense can be successfully accomplished. We concluded that such assurance could only be provided if Defense took steps to improve its visibility over the status of key business processes.

End-To-End Testing Must Be Completed

While it is important to achieve compliance for individual mission-critical systems, realizing such compliance alone does not ensure that business functions will continue to operate through the change of century—the ultimate goal of Year 2000 efforts. The purpose of end-to-end testing is to verify that a defined set of interrelated systems, which collectively support an organizational core business area or function, 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—are 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.)¹⁶

In January we testified that 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 the tests.¹⁷ On March 31, OMB and the Chair of the President's Council on Year 2000 Conversion announced that one of the key priorities that federal agencies will be pursuing during the rest of 1999 will be cooperative end-to-end testing to demonstrate the Year 2000 readiness of federal programs with states and other partners.

¹⁴Defense 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).

¹⁵Year 2000 Computing Crisis: Defense Has Made Progress, But Additional Management Controls Are Needed (GAO/T-AIMD-99-101, March 2, 1999).

¹⁶GAO/AIMD-10.1.21, November 1998.

¹⁷Year 2000 Computing Crisis: Readiness Improving, But Much Work Remains to Avoid Major Disruptions (GAO/T-AIMD-99-50, January 20, 1999).

Agencies have also acted to address end-to-end testing. For example, our March FAA testimony¹⁸ found that the agency had addressed our prior concerns about the lack of detail in its draft end-to-end test program plan and had developed a detailed end-to-end testing strategy and plans.¹⁹ At the Department of Defense, last month we reported²⁰ that the department had underway or planned hundreds of related Year 2000 end-to-end test and evaluation activities and that, thus far, it was taking steps to ensure that these related end-to-end tests were effectively coordinated. However, we concluded that Defense was far from successfully finishing its various Year 2000 end-to-end test activities and that it must complete efforts to establish end-to-end management controls, such as establishing an independent quality assurance program.

Business Continuity and Contingency Plans Are Needed

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, in April 1998 we recommended that the Council require agencies to develop contingency plans for all critical core business processes.²¹

OMB has clarified its contingency plan instructions and, along with the Chief Information Officers Council, has adopted our business continuity and contingency planning guide.²² In particular, on January 26, 1999, OMB called on federal agencies to identify and report on the high-level core business functions that are to be addressed in their business continuity and contingency plans, as well as to provide key milestones for development and testing of such plans in their February 1999 quarterly reports. In addition, on May 13 OMB required agencies to submit high-level versions of these plans by June 15. According to an OMB official, OMB has received almost all of the agency plans. This official stated that OMB planned to review the plans, discuss them with the agencies, determine whether there were any common themes, and report on the plans' status in its next quarterly report.

¹⁸GAO/T-AIMD/RCED-99-118, March 15, 1999.

¹⁹GAO/T-AIMD-98-251, August 6, 1998.

²⁰Defense Computers: Management Controls Are Critical To Effective Year 2000 Testing (GAO/AIMD-99-172, June 30, 1999).

²¹Year 2000 Computing Crisis: Potential for Widespread Disruption Calls for Strong Leadership and Partnerships (GAO/AIMD-98-85, April 30, 1998).

²²GAO/AIMD-10.1.19, August 1998.

To provide assurance that agencies' business continuity and contingency plans will work if needed, on January 20 we suggested that 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.²³ Our review of the 24 major departments and agencies' May 1999 quarterly reports found 14 cases in which agencies did not identify test dates for their business continuity and contingency plans or reported test dates subsequent to September 30, 1999.

On March 31, OMB and the Chair of the President's Council announced that completing and testing business continuity and contingency plans as insurance against disruptions to federal service delivery and operations from Year 2000-related failures will be one of the key priorities that federal agencies will be pursuing through the rest of 1999. Accordingly, OMB should implement our suggestion and establish a target date for the validation of these business continuity and contingency plans.

Recent OMB Action Could Help Ensure
Business Continuity of High-Impact Programs

While individual agencies have been identifying and remediating mission-critical systems, the government's future actions need to be focused on its high-priority programs and ensuring the continuity of these programs, including the continuity of federal programs that are administered by states. Accordingly, governmentwide priorities need to be based on such criteria as the potential for adverse health and safety effects, adverse financial effects on American citizens, detrimental effects on national security, and adverse economic consequences. In April 1998 we recommended that the President's Council on Year 2000 Conversion establish governmentwide priorities and ensure that agencies set agencywide priorities.²⁴

On March 26, OMB implemented our recommendation by issuing a memorandum to federal agencies designating lead agencies for the government's 42 high-impact programs (e.g., food stamps, Medicare, and federal electric power generation and delivery). (OMB later added a 43rd high-impact program.) Appendix I lists these programs and their lead agencies. For each program, the lead agency was charged with identifying to OMB the partners integral to program delivery; taking a leadership role in convening those partners; assuring that each partner has an adequate Year 2000 plan and, if not, helping each partner without one; and developing a plan to ensure that the program will operate effectively. According to OMB, such a plan might include testing data exchanges across partners, developing complementary business continuity and contingency plans, sharing key information on readiness with other partners and the public, and taking other steps necessary to ensure that the program will work. OMB directed the lead agencies to provide a schedule and milestones of key activities in the plan by April 15. OMB also asked agencies to provide monthly progress reports. As you know, we are currently reviewing agencies' progress in ensuring the readiness of their high-impact programs for

²³GAO/T-AIMD-99-50, January 20, 1999.

²⁴GAO/AIMD-98-85, April 30, 1998.

this subcommittee.

STATE AND LOCAL GOVERNMENTS
FACE SIGNIFICANT YEAR 2000 RISKS

Just as the federal government faces significant Year 2000 risks, so too do state and local governments. If the Year 2000 problem is not properly addressed, for example, (1) food stamps and other types of payments may not be made or could be made for incorrect amounts; (2) date-dependent signal timing patterns could be incorrectly implemented at highway intersections, with safety severely compromised; and (3) prisoner release or parole eligibility determinations may be adversely affected. Nevertheless, available information on the Year 2000 readiness of state and local governments indicates that much work remains.

According to information on state Year 2000 activities reported to the National Association of State Information Resource Executives as of June 17, 1999,²⁵ states²⁶ reported having thousands of mission-critical systems.²⁷ With respect to completing the implementation phase for these systems,

- 5 states²⁸ reported that they had completed between 25 and 49 percent,
- 13 states²⁹ reported completing between 50 and 74 percent, and
- 30 states³⁰ reported completing 75 percent or more.³¹

All of the states responding to the National Association of State Information Resource Executives survey reported that they were actively engaged in internal and external contingency planning and that they had established target dates for the completion of

²⁵Individual states submit periodic updates to the National Association of State Information Resource Executives. For the June 17 report, over half of the states submitted their data in May and June 1999. The oldest data were provided on March 4 and the most recent data on June 16. All but three states responded to the survey.

²⁶In the context of the National Association of State Information Resource Executives survey, the term "states" includes the District of Columbia, Guam, and Puerto Rico.

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

²⁸Three states reported on their mission-critical systems, one state reported on its processes, and one reported on its functions.

²⁹Eleven states reported on their mission-critical systems, one reported on all systems, and one reported on projects.

³⁰Twenty-five states reported on their mission-critical systems, two states reported on their applications, one reported on its "priority business activities," one reported on its "critical compliance units," and one reported on all systems.

³¹Of the states that responded to the survey, two did not respond to this question.

these plans; 14 (28 percent) reported the deadline as October 1999 or later.

State audit organizations have also identified significant Year 2000 concerns. In January, the National State Auditors Association reported on the results of its mid-1998 survey of Year 2000 compliance among states.³² This report stated that, for the 12 state audit organizations that provided Year 2000-related reports, concerns had been raised in areas such as planning, testing, embedded systems, business continuity and contingency planning, and the adequacy of resources to address the problem.

We identified additional products by 15 state-level audit organizations and Guam that discussed the Year 2000 problem and that had been issued since October 1, 1998. Several of these state-level audit organizations noted that progress had been made. However, the audit organizations also expressed concerns that were consistent with those reported by the National State Auditors Association. For example:

- In December 1998 the Vermont State Auditor reported³³ that the state Chief Information Officer did not have a comprehensive control list of the state's information technology systems. Accordingly, the audit office stated that, even if all mission-critical state systems were checked, these systems could be endangered by information technology components that had not been checked or by linkages with the state's external electronic partners.
- In April, New York's Division of Management Audit and State Financial Services reported that state agencies did not adequately control the critical process of testing remediated systems.³⁴ Further, most agencies were in the early stages of addressing potential problems related to data exchanges and embedded systems and none had completed substantive work on contingency planning. The New York audit office subsequently issued 7 reports on 13 of the state's mission-critical and high-priority systems that included concerns about contingency planning and testing.
- In February, the California State Auditor reported³⁵ that key agencies responsible for emergency services, corrections, and water resources, among other areas, had not fully addressed embedded technology-related threats. Regarding emergency services, the California report stated that if remediation of the embedded technology in its

³²Year 2000: State Compliance Efforts (National State Auditors Association, January 1999).

³³Vermont State Auditor's Report on State Government's Year 2000 Preparedness (Y2K Compliance) for the Period Ending November 1, 1998 (Office of the State Auditor, December 31, 1998).

³⁴New York's Preparation for the Year 2000: A Second Look (Office of the State Comptroller, Division of Management Audit and State Financial Services, Report 98-S-21, April 5, 1999).

³⁵Year 2000 Computer Problem: The State's Agencies Are Progressing Toward Compliance but Key Steps Remain Incomplete (California State Auditor, February 18, 1999).

networks were not completed, the Office of Emergency Services might have to rely on cumbersome manual processes, significantly increasing response time to disasters.

- In March, Oregon's Audits Division reported³⁶ that 11 of the 12 state agencies reviewed did not have business continuity plans addressing potential Year 2000 problems for their core business functions.
- In March, North Carolina's State Auditor reported³⁷ that resource restrictions had limited the state's Year 2000 Project Office's ability to verify data reported by state agencies.

It is also critical that local government systems be ready for the change of century since critical functions involving, for example, public safety and traffic management, are performed at the local level. Recent reports on local governments have highlighted Year 2000 concerns. For example:

- On June 23, the National Association of Counties announced the results of its April survey of 500 randomly selected counties. This survey found that (1) 74 percent of respondents had a countywide plan to address Year 2000 issues, (2) 51 percent had completed system assessments, and (3) 27 percent had completed system testing. In addition, 190 counties had prepared contingency plans and 289 had not. Further, of the 114 counties reporting that they planned to develop Year 2000 contingency plans, 22 planned to develop the plan in April-June, 64 in July-September, 18 in October-December, and 10 did not yet know.
- The National League of Cities conducted a poll during its annual conference in March 1999 that included over 400 responses. The poll found that (1) 340 respondents stated that over 75 percent of their cities' critical systems would be Year 2000 compliant by January 1, 2000, (2) 35 stated that 51-75 percent would be compliant, (3) 16 stated that 25-50 percent would be compliant, and (4) 16 stated that less than 25 percent would be compliant. Moreover, 34 percent of respondents reported that they had contingency plans, 46 percent stated that they were in the process of developing plans, 12 percent stated that plans would be developed, and 8 percent said they did not intend to develop contingency plans.
- In January 1999, the United States Conference of Mayors reported on the results of its survey of 220 cities. It found that (1) 97 percent had a citywide plan to address Year 2000 issues, (2) 22 percent had repaired or replaced less than half of their systems, and (3) 45 percent had completed less than half of their testing.

³⁶Department of Administrative Services Year 2000 Statewide Project Office Review (Secretary of State, Audits Division, State of Oregon Report No. 99-05, March 16, 1999).

³⁷Department of Commerce, Information Technology Services Year 2000 Project Office (Office of the State Auditor, State of North Carolina, March 18, 1999).

Of critical importance to the nation are services essential to the safety and well-being of individuals across the country, namely 9-1-1 systems and law enforcement. For the most part, responsibility for ensuring continuity of service for 9-1-1 calls and law enforcement resides with thousands of state and local jurisdictions. For example, in April, the Kansas Legislative Post Audit Committee reported on the Year 2000 status of the state's 94 counties that have Enhanced 9-1-1 systems or Identification 9-1-1 systems.³⁸ Of these 94 counties, the Kansas audit office found that 38 were in compliance, 26 were upgrading, 3 were a mixture of compliance and upgrading, 10 were under review, 12 had not been tested, and 5 were designated as "other."

On April 29 we testified that not enough was known about the status of either 9-1-1 systems or of state and local law enforcement activities to conclude about either's ability during the transition to the year 2000 to meet the public safety and well-being needs of local communities across the nation.³⁹ While the federal government planned additional actions to determine the status of these areas, we stated that the President's Council on Year 2000 Conversion should use such information to identify specific risks and develop appropriate strategies and contingency plans to respond to those risks.

Recognizing the seriousness of the Year 2000 risks facing state and local governments, the President's Council has developed initiatives to address the readiness of state and local governments. For example:

- The Council established working groups on state and local governments and tribal governments.
- Council officials participate in monthly multistate conference calls.
- In July 1998 and March 1999, the Council, in partnership with the National Governors' Association, convened Year 2000 summits with state and U.S. territory Year 2000 coordinators.
- On May 24, the Council announced a nationwide campaign to promote "Y2K Community Conversations" to support and encourage efforts of government officials, business leaders, and interested citizens to share information on their progress. To support this initiative, the Council has developed and is distributing a toolkit that provides examples of which sectors should be represented at these events and issues that should be addressed.

³⁸Reviewing the 911 Emergency Phone Systems in Kansas, Part I: Identifying the Current Status (Kansas Legislative Post Audit Committee, April 13, 1999).

³⁹Year 2000 Computing Challenge: Status of Emergency and State and Local Law Enforcement Systems Is Still Unknown (GAO/T-AIMD-99-163, April 29, 1999).

State-Administered Federal Human Services Programs Are At Risk

Among the critical functions performed by states are the administration of federal human services programs. As we reported in November 1998, many systems that support state-administered federal human services programs were at risk, and much work remained to ensure that services would continue.⁴⁰ In February of this year, we testified that while some progress had been achieved, many states' systems were not scheduled to become compliant until the last half of 1999.⁴¹ Accordingly, we concluded that, given these risks, business continuity and contingency planning was even more important in ensuring continuity of program operations and benefits in the event of systems failures.

Subsequent to our November 1998 report, OMB directed federal oversight agencies to include the status of selected state human services systems in their quarterly reports. Specifically, in January 1999, OMB requested that agencies describe actions to help ensure that federally supported, state-run programs will be able to provide services and benefits. OMB further asked that agencies report the date when each state's systems will be Year 2000-compliant. Tables 1 and 2 summarize the information gathered by the Departments of Agriculture and Health and Human Services, respectively, on the compliance status of state-level organizations. The information indicates that a number of states do not plan to complete their Year 2000 efforts until the last quarter of 1999.

Table 1: Reported State-level Readiness for Federally Supported Programs, Department of Agriculture, May 1999^a

Program	Compliant	April-June	July-September	October-December	Unknown ^b
Food Stamps	25	12	14	3	0
Child Nutrition	29	9	10	4	2
Women, Infants, and Children	33	11	7	3	0

^aThis chart contains readiness information from the 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands.

^bUnknown indicates the state did not provide a date or the date was unknown.

Source: Department of Agriculture.

⁴⁰Year 2000 Computing Crisis: Readiness of State Automated Systems to Support Federal Welfare Programs (GAO/AIMD-99-28, November 6, 1998).

⁴¹Year 2000 Computing Crisis: Readiness of State Automated Systems That Support Federal Human Services Programs (GAO/T-AIMD-99-91, February 24, 1999).

Table 2: Reported State-level^a Readiness for Federally Supported Programs, Department of Health and Human Services^b

Program	Compliant ^c	Jan.- March	April- June	July- Sept.	Oct.- Dec.	Unk. ^d	N/A ^e
Child Care	24	5	5	8	2	6	4
Child Support Enforcement	15	4	13	8	8	6	0
Child Welfare	20	5	9	11	3	5	1
Low Income Housing Energy Assistance Program	10	0	3	7	1	32	1
Medicaid – Integrated Eligibility System	20	0	15	15	4	0	0
Medicaid – Management Information System	17	0	19	14	4	0	0
Temporary Assistance for Needy Families	19	3	12	15	1	4	0

^aThis chart contains readiness information from the 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands.

^bThe OMB report stated that this information was as of January 31, 1999. However, OMB provided a draft table to the National Association of State Information Resource Executives which, in turn, provided the draft table to the states. The states were asked to contact HHS and provide corrections by June 1, 1999. For its part, HHS submitted updated state data to OMB in early June.

^cIn many cases the report indicated a date instead of whether the state was compliant. We assumed that states reporting completion dates in 1998 or earlier were compliant.

^dUnknown indicates that, according to OMB, the data reported by the states were unclear or that no information was reported by the agency.

^eN/A indicates that the states or territories reported that the data requested were not applicable to them.

Source: Progress on Year 2000 Conversion: 9th Quarterly Report (OMB, issued on June 15, 1999).

In addition, in June 1999, OMB reported that, as of March 31, 1999, 27 states' unemployment insurance systems were compliant, 11 planned to be completed between April and June 1999, 10 planned to be completed between July and September, and 5 planned to be completed between October and December.

Along with obtaining readiness information from the states, agencies have initiated additional actions to help ensure the Year 2000 compliance of state-administered programs. About a quarter of the federal government's programs designated high-impact

by OMB are state-administered, such as Food Stamps and Temporary Assistance for Needy Families. In response to OMB's March memorandum regarding the high-impact programs, the Departments of Agriculture, Health and Human Services, and Labor reported on various actions that they are taking or plan to take to help ensure the Year 2000 compliance of their state-administered programs. For example:

- The Department of Agriculture reported in May that its Food and Nutrition Service requested that states provide their contingency plans and had contracted for technical support services to review these plans, as needed, and to assist in its oversight of other state Year 2000 activities.
- The Department of Health and Human Services reported that its Administration for Children and Families and Health Care Financing Administration had contracted for on-site assessments of state partners, which will include reviews of business continuity and contingency plans.
- The Department of Labor reported that states are required to submit a certification of Year 2000 compliance for their benefit and tax systems along with an independent verification and validation report. In addition, Labor required that state agencies prepare business continuity and contingency plans, which will be reviewed by Labor officials. Further, the department plans to design and develop a prototype PC-based system to be used in the event that a state's unemployment insurance system is unusable due to a Year 2000-induced problem.

An example of the benefits that federal/state partnerships can provide is illustrated by the Department of Labor's unemployment services program. In September 1998, we reported that many State Employment Security Agencies were at risk of failure as early as January 1999 and urged the Department of Labor to initiate the development of realistic contingency plans to ensure continuity of core business processes in the event of Year 2000-induced failures.⁴² Just last month, we testified that four state agencies' systems could have failed if systems in those states had not been programmed with an emergency patch in December 1998. This patch was developed by several of the state agencies and promoted to other state agencies by the Department of Labor.⁴³

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

Beyond the risks faced by federal, state, and local governments, the year 2000 also poses a serious challenge to the public infrastructure, key economic sectors, and to other

⁴²Year 2000 Computing Crisis: Progress Made at Department of Labor, But Key Systems at Risk (GAO/T-AIMD-98-303, September 17, 1998).

⁴³Year 2000 Computing Challenge: Labor Has Progressed But Selected Systems Remain at Risk (GAO/T-AIMD-99-179, May 12, 1999).

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.⁴⁴ 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 has formed 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.

Our April 1998 report also recommended that the President's Council 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 then planned to issue quarterly public reports summarizing these assessments. The first such report was issued on January 7, 1999.

The Council's second report was issued on April 21, 1999.⁴⁵ The report stated that substantial progress had been made in the prior 6 to 12 months, but that there was still much work to be done. According to the Council, most industries had projected completion target dates between June and September and were in, or would soon be moving into, the critical testing phase. Key points in the Council's April assessment included the following:

- National Year 2000 failures in key U.S. infrastructures such as power, banking, telecommunications, and transportation are unlikely.
- Organizations that are not paying appropriate attention to the Year 2000 problem or that are adopting a "wait and see" strategy—an attitude prevalent among some small businesses and local governments—are putting themselves and those that depend upon them at great risk.
- International Year 2000 activity, although increasing, is lagging and will be the source of the greatest risk.

The Council's assessment reports have substantially increased the nation's understanding of the Year 2000 readiness of key industries. However, the picture remained incomplete in certain key areas because the surveys conducted did not have a high response rate, the

⁴⁴GAO/AIMD-98-85, April 30, 1998.

⁴⁵Both of the Council's reports are available on its web site, www.y2k.gov.

assessment was general, or the data were old. For example, according to the assessment report, only 13 percent of the nation's 9-1-1 centers had responded to a survey being conducted by the Federal Emergency Management Agency in conjunction with the National Emergency Number Association, calling into question whether the results of the survey accurately portrayed the readiness of the sector. In the case of drinking water, both the January and April reports provided a general assessment but did 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). Finally, in some cases, such as the transit industry, the sector surveys had been conducted months earlier.

The President's Council is to be commended on the strides that it has made to obtain Year 2000 readiness data 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, in testimony this January, we suggested that the Council consider additional actions such as continuing to aggressively pursue readiness information in the areas in which it is lacking.⁴⁶ If the current approach of using associations to voluntarily collect information does not yield the necessary information, we suggested that the Council may wish to consider whether legislative remedies (such as requiring disclosure of Year 2000 readiness data) should be proposed. In response to this suggestion, the Council Chair stated that the Council has focused on collaboration and communication with associations and other groups as a means to get industries to share information on their Year 2000 readiness and that the Council did not believe that legislation would be necessary. The Council's next sector report is expected to be released later this month.

Subsequent to the Council's April report, surveys in key sectors have been issued. In addition, we have issued several products related to several of these sectors. I will now discuss the results of some of these surveys and our reviews.

Energy Sector

In April, we reported that while the electric power industry had concluded that it had made substantial progress in making its systems and equipment ready to continue operations into the year 2000, significant risks remained since many reporting organizations did not expect to be Year 2000 ready within the June 1999 industry target date.⁴⁷ We, therefore, suggested that the Department of Energy (1) work with the Electric Power Working Group to ensure that remediation activities were accelerated for the utilities that expected to miss the June 1999 deadline for achieving Year 2000 readiness and (2) encourage state regulatory utility commissions to require a full public disclosure of Year 2000 readiness status of entities transmitting and distributing electric power. The Department of Energy generally agreed with our suggestions. We also suggested that the Nuclear Regulatory Commission (1) in cooperation with the Nuclear

⁴⁶GAO/T-AIMD-99-50, January 20, 1999.

⁴⁷Year 2000 Computing Crisis: Readiness of the Electric Power Industry (GAO/AIMD-99-114, April 6, 1999).

Energy Institute, work with nuclear power plant licensees to accelerate the Year 2000 remediation efforts among the nuclear power plants that expect to meet the June 1999 deadline for achieving readiness and (2) publicly disclose the Year 2000 readiness of each of the nation's operational nuclear reactors. In response, the Nuclear Regulatory Commission stated that it plans to focus its efforts on nuclear power plants that may miss the July 1, 1999 milestone and that it would release the readiness information on individual plants that same month.

Subsequent to our report, on April 30, 1999, the North American Electric Reliability Council released its third status report on electric power systems. According to the North American Electric Reliability Council, as of March 31, 1999, reporting organizations, on average, had completed 99 percent of the inventory phase, 95 percent of the assessment phase, and 75 percent of the remediation/testing phase.

In May, we reported⁴⁸ that while the domestic oil and gas industries had reported that they had made substantial progress in making their equipment and systems ready to continue operations into the year 2000, risks remained. In particular, a February industrywide survey found that over a quarter of the oil and gas industries reported that they did not expect to be Year 2000 ready until the second half of 1999—leaving little time for resolving unexpected problems. Moreover, although over half of our oil is imported, little was known about the Year 2000 readiness of foreign oil suppliers. Further, while individual domestic companies reported that they were developing Year 2000 contingency plans, there were no plans to perform a national-level risk assessment and develop contingency plans to deal with potential shortages or disruptions in the nation's overall oil and gas supplies. We suggested that the Council's oil and gas working group (1) work with industry associations to perform national-level risk assessments and develop and publish credible, national-level scenarios regarding the impact of potential Year 2000 failures and (2) develop national-level contingency plans. The working group generally agreed with these suggestions.

Water Sector

As I previously mentioned, the Council's January and April assessment reports provided only a general assessment of the drinking water sector and did not contain detailed data. Similarly, in April we reported⁴⁹ that insufficient information was available to assess and manage Year 2000 efforts in the water sector, and little additional information was expected under the current regulatory approach. While the Council's water sector working group had undertaken an awareness campaign and had urged national water sector associations to continue to survey their memberships, survey response rates had been low. Further, Environmental Protection Agency officials stated that the agency

⁴⁸Year 2000 Computing Crisis: Readiness of the Oil and Gas Industries (GAO/AIMD-99-162, May 19, 1999).

⁴⁹Year 2000 Computing Crisis: Status of the Water Industry (GAO/AIMD-99-151, April 21, 1999).

lacked the rules and regulations necessary to require water and wastewater facilities to report on their Year 2000 status.

Our survey of state regulators found that a few states were proactively collecting Year 2000 compliance data from regulated facilities, a much larger group of states was disseminating Year 2000 information, while another group was not actively using either approach. Additionally, only a handful of state regulators believed that they were responsible for ensuring facilities' Year 2000 compliance or overseeing facilities' business continuity and contingency plans. Among our suggested actions was that the Council, the Environmental Protection Agency, and the states determine which regulatory organization should take responsibility for assessing and publicly disclosing the status and outlook of water sector facilities' Year 2000 business continuity and contingency plans. The Environmental Protection Agency generally agreed with our suggestions but one official noted that additional legislation may be needed if the agency is to take responsibility for overseeing facilities' Year 2000 business continuity and contingency plans.

Health Sector

The health sector includes health care providers (such as hospitals and emergency health care services), insurers (such as Medicare and Medicaid), and biomedical equipment. With respect to biomedical equipment, on June 10 we testified⁵⁰ that, in response to our September 1998 recommendation,⁵¹ HHS, in conjunction with the Department of Veterans Affairs, had established a clearinghouse on biomedical equipment. As of June 1, 1999, 4,142 biomedical equipment manufacturers had submitted data to the clearinghouse. About 61 percent of these manufacturers reported having products that do not employ dates and about 8 percent (311 manufacturers) reported having date-related problems such as an incorrect display of date/time. According to the Food and Drug Administration, the 311 manufacturers reported 897 products with date-related problems. However, not all compliance information was available on the clearinghouse because the clearinghouse referred the user to 427 manufacturers' web sites. Accordingly, we reviewed the web sites of these manufacturers and found, as of June 1, 1999, a total of 35,446 products.⁵² Of these products, 18,466 were reported as not employing a date, 11,211 were reported as compliant, 4,445 were shown as not compliant, and the compliance status of 1,324 was unknown.

⁵⁰Year 2000 Computing Challenge: Concerns About Compliance Information on Biomedical Equipment (GAO/T-AIMD-99-209, June 10, 1999).

⁵¹Year 2000 Computing Crisis: Compliance Status of Many Biomedical Equipment Items Still Unknown (GAO/AIMD-98-240, September 18, 1998).

⁵²Because of limitations in many of the manufacturers web sites, our ability to determine the total number of biomedical equipment products reported and their compliance status was impaired. Accordingly, the actual number of products reported by the manufacturers could be significantly higher than the 35,446 products that we counted.

In addition to the establishment of a clearinghouse, our September 1998 report also recommended that HHS and the Department of Veterans Affairs take prudent steps to jointly review manufacturers' test results for critical care/life support biomedical equipment. We were especially concerned that the departments review test results for equipment previously deemed to be noncompliant but now deemed by manufacturers to be compliant, or equipment for which concerns about compliance remained. In May 1999, the Food and Drug Administration, a component agency of HHS, announced that it planned to develop a list of critical care/life support medical devices and the manufacturers of these devices, select a sample of manufacturers for review, and hire a contractor to develop a program to assess manufacturers' activities to identify and correct Year 2000 problems for these medical devices. In addition, if the results of this review indicated a need for further review of manufacturer activities, the contractor would review a portion of the remaining manufacturers not yet reviewed. Moreover, according to the Food and Drug Administration, any manufacturer whose quality assurance system appeared deficient based on the contractors review would be subject to additional reviews to determine what actions would be required to eliminate any risk posed by noncompliant devices.

In April testimony⁵³ we also reported on the results of a Department of Veterans Affairs survey of 384 pharmaceutical firms and 459 medical-surgical firms with whom it does business. Of the 52 percent of pharmaceutical firms that responded to the survey, 32 percent reported that they were compliant. Of the 54 percent of the medical-surgical firms that responded, about two-thirds reported that they were compliant.

Banking and Finance Sector

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 agencies⁵⁴ to ensure that the institutions that they oversee are ready to handle the Year 2000 problem.⁵⁵ We concluded that the regulators had made significant progress in assessing the readiness of member institutions and in 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.

⁵³Year 2000 Computing Crisis: Action Needed to Ensure Continued Delivery of Veterans Benefits and Health Care Services (GAO/T-AIMD-99-136, April 15, 1999).

⁵⁴The 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.

⁵⁵Year 2000 Computing Crisis: Federal Depository Institution Regulators Are Making Progress, But Challenges Remain (GAO/T-AIMD-98-305, September 17, 1998).

In April, we reported that the Federal Reserve System--which is instrumental to our nation's economic well-being, since it provides depository institutions and government agencies services such as processing checks and transferring funds and securities, has effective controls to help ensure that its Year 2000 progress is reported accurately and reliably.⁵⁶ We also found that it is effectively managing the renovation and testing of its internal systems and the development and planned testing of contingency plans for continuity of business operations. Nevertheless, the Federal Reserve System still had much to accomplish before it is fully ready for January 1, 2000, such as completing validation and implementation of all of its internal systems and completing its contingency plans.

In addition to the domestic banking and finance sector, large U.S. financial institutions have financial exposures and relationships with international financial institutions and markets that may be at risk if these international organizations are not ready for the date change occurring on January 1, 2000. In April, we reported⁵⁷ that foreign financial institutions had reportedly lagged behind their U.S. counterparts in preparing for the Year 2000 date change. Officials from four of the seven large foreign financial institutions we visited said they had scheduled completion of their Year 2000 preparations about 3 to 6 months after their U.S. counterparts, but they planned to complete their efforts by mid-1999 at the latest. Moreover, key international market supporters, such as those that transmit financial messages and provide clearing and settlement services, told us that their systems were ready for the date change and that they had begun testing with the financial organizations that depended on these systems. Further, we found that seven large U.S. banks and securities firms we visited were taking actions to address their international risks. In addition, U.S. banking and securities regulators were also addressing the international Year 2000 risks of the institutions that they oversee.

With respect to the insurance industry, in March, we concluded that insurance regulator presence regarding the Year 2000 area was not as strong as that exhibited by the banking and securities industry.⁵⁸ State insurance regulators we contacted were late in raising industry awareness of potential Year 2000 problems, provided little guidance to regulated institutions, and failed to convey clear regulatory expectations to companies about Year 2000 preparations and milestones. Nevertheless, the insurance industry is reported by both its regulators and by other outside observers to be generally on track to being ready for 2000. However, most of these reports are based on self-reported information and, compared to other financial regulators, insurance regulators' efforts to validate this information generally began late and were more limited.

⁵⁶Year 2000 Computing Crisis: Federal Reserve Has Established Effective Year 2000 Management Controls for Internal Systems Conversion (GAO/AIMD-99-78, April 9, 1999).

⁵⁷Year 2000: Financial Institution and Regulatory Efforts to Address International Risks (GAO/GGD-99-62, April 27, 1999).

⁵⁸Insurance Industry: Regulators Are Less Active in Encouraging and Validating Year 2000 Preparedness (GAO/T-GGD-99-56, March 11, 1999).

In a related report in April,⁵⁹ we stated that variations in oversight approaches by state insurance regulators also made it difficult to ascertain the overall status of the insurance industry's Year 2000 readiness. We reported that the magnitude of insurers' Year 2000-related liability exposures could not be estimated at that time but that costs associated with these exposures could be substantial for some property-casualty insurers, particularly those concentrated in commercial-market sectors. In addition, despite efforts to mitigate potential exposures, the Year 2000-related costs that may be incurred by insurers would remain uncertain until key legal issues and actions on pending legislation were resolved.

Transportation Sector

A key component to the nation's transportation sector are airports. This January we reported on our survey of 413 airports.⁶⁰ We found that while the nation's airports are making progress in preparing for the year 2000, such progress varied. Of the 334 airports responding to our survey, about one-third reported that they would complete their Year 2000 preparations by June 30, 1999. The other two-thirds either planned on a later date or failed to estimate any completion date, and half of these airports did not have contingency plans for any of 14 core airport functions. Although most of those not expecting to be ready by June 30 are small airports, 26 of them are among the nation's largest 50 airports.

On June 18, the Federal Aviation Administration issued an air industry Year 2000 status report that included information on airports and airline carriers. Table 3 provides the assessment, renovation, validation, and implementation information contained in this report.

⁵⁹Year 2000: State Insurance Regulators Face Challenges in Determining Industry Readiness (GAO/GGD-99-87, April 30, 1999).

⁶⁰Year 2000 Computing Crisis: Status of Airports' Efforts to Deal With Date Change Problem (GAO/RCED/AIMD-99-57, January 29, 1999).

Table 3: Industry Segment Percentage Completion of Year 2000 Remediation Phases

Industry Segment	Assessment	Renovation	Validation	Implementation
Large hub airports	98%	63%	31%	26%
Medium hub airports	100%	70%	43%	37%
Small hub airports	94%	61%	55%	48%
Non-hub airports	93%	67%	67%	70%
Major carriers	100%	75%	50%	^a
Low-cost carriers	73%	38%	19%	18%

^aImplementation was occurring as validation and testing were completed.

Note: Airport information was based on data as of March 15, 1999 from the American Association of Airport Executives and the Airports Council International/North America. The major carrier information based on data as of February 22, 1999 from the Air Transport Association of America, and the low-cost carrier information was based on data as of November 30, 1998 from the National Air Carriers Association, Inc.

Source: Federal Aviation Administration.

Manufacturing and Small Business Sector

The manufacturing and small business sector includes the entities that produce or sell a myriad of products such as chemicals, electronics, heavy equipment, food, textiles, and automobiles. With respect to the chemical industry, table 4 contains the latest survey data by Chemical Manufacturers Association--which represents over 190 primarily large chemical companies--and shows that while some companies' systems are Year 2000 ready, others are in varying stages of completion. This survey provided information on the Year 2000 readiness stage of 123 respondents with respect to their business systems, manufacturing, inventory, and distribution systems, embedded systems, and supply chain as of May 12, 1999.

Table 4: Results of May 12, 1999 Survey of Chemical Manufacturers Association^a

Function	Year 2000 Ready	Planning	Inventory/ Assessment	Remediation	Validation
Business systems	26	1	5	51	27
Manufacturing, inventory, and distribution systems	18	2	7	53	28
Embedded systems	15	2	26	52	13
Supply chain	10	4	51	22	21

^aSome respondents did not provide information to all questions or stated that the question was not applicable.

Source: Chemical Manufacturers Association statement before the Senate Special Committee on the Year 2000 Technology Problem, May 14, 1999.

Since the Chemical Manufacturers Association represented mainly large companies, a survey of small and mid-sized chemical companies was sponsored by several industry associations⁶¹ to assist the Congress, the administration, and the U.S. Chemical Safety and Hazard Investigation Board by obtaining information on the preparedness of this segment of the industry. Table 5 contains the results of the survey, which was conducted between March and May 1999.

⁶¹The sponsors of the survey were the American Crop Protection Association, Chemical Producers & Distributors Association, Chemical Specialties Manufacturers Association, International Sanitary Supply Association, National Association of Chemical Distributors, Responsible Industry for a Sound Environment, and the Synthetic Organic Chemical Manufacturers Association.

Table 5: Readiness Stage of Small and Medium-Sized Chemical Companies^a

Function	Year 2000 Ready	Planning	Inventory/ Assessment	Remediation	Validation
Business systems	147	8	4	24	12
Manufacturing, inventory, and distribution systems	133	8	3	21	13
Embedded systems	83	3	7	13	6
Supply chain	80	17	29	17	25

^aSome respondents did not provide information to all questions or stated that the question was not applicable.

Source: Year 2000 Readiness Disclosure Survey of Small & Mid-Sized Chemical Companies, June 9, 1999.

Another key segment of the economy are small businesses. The National Federation of Independent Business and Wells Fargo sponsored a third survey of the Year 2000 preparedness of small businesses between mid-April and mid-May 1999. This survey found that 84 percent of small businesses are directly exposed to a possible Year 2000 problem. Of the small businesses directly exposed to the Year 2000 problem, 59 percent had taken action, 12 percent planned to take action, and 28 percent did not plan to take action (the other 1 percent responded that the question was not applicable). In addition, 43 percent of the small businesses that were aware of the Year 2000 problem had made contingency plans to minimize the impact of potential problems.

In summary, while improvement has been shown, much work remains at the national, federal, state, and local levels to ensure that major service disruptions do not occur. Specifically, remediation must be completed, end-to-end testing performed, and business continuity and contingency plans developed. Similar actions remain to be completed by the nation's key sectors. Accordingly, whether the United States successfully confronts the Year 2000 challenge will largely depend on the success of federal, state, and local governments, as well as the private sector working separately and together to complete these actions. Accordingly, strong leadership and partnerships must be maintained to ensure that the needs of the public are met at the turn of the century.

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

APPENDIX I

APPENDIX I

Federal High-Impact Programs and Lead Agencies

Agency	Program
Department of Agriculture	Child Nutrition Programs
Department of Agriculture	Food Safety Inspection
Department of Agriculture	Food Stamps
Department of Agriculture	Special Supplemental Nutrition Program for Women, Infants, and Children
Department of Commerce	Patent and trademark processing
Department of Commerce	Weather Service
Department of Defense	Military Hospitals
Department of Defense	Military Retirement
Department of Education	Student Aid
Department of Energy	Federal electric power generation and delivery
Department of Health and Human Services	Child Care
Department of Health and Human Services	Child Support Enforcement
Department of Health and Human Services	Child Welfare
Department of Health and Human Services	Disease monitoring and the ability to issue warnings
Department of Health and Human Services	Indian Health Service
Department of Health and Human Services	Low Income Home Energy Assistance Program
Department of Health and Human Services	Medicaid
Department of Health and Human Services	Medicare
Department of Health and Human Services	Organ Transplants
Department of Health and Human Services	Temporary Assistance for Needy Families
Department of Housing and Urban Development	Housing loans (Government National Mortgage Association)

Department of Housing and Urban Development	Section 8 Rental Assistance
Department of Housing and Urban Development	Public Housing
Department of Housing and Urban Development	FHA Mortgage Insurance
Department of Housing and Urban Development	Community Development Block Grants
Department of the Interior	Bureau of Indians Affairs programs
Department of Justice	Federal Prisons
Department of Justice	Immigration
Department of Justice	National Crime Information Center
Department of Labor	Unemployment Insurance
Department of State	Passport Applications and Processing
Department of Transportation	Air Traffic Control System
Department of Transportation	Maritime Safety Program
Department of the Treasury	Cross-border Inspection Services
Department of Veterans Affairs	Veterans' Benefits
Department of Veterans Affairs	Veterans' Health Care
Federal Emergency Management Agency	Disaster Relief
Office of Personnel Management	Federal Employee Health Benefits
Office of Personnel Management	Federal Employee Life Insurance
Office of Personnel Management	Federal Employee Retirement Benefits
Railroad Retirement Board	Retired Rail Workers Benefits
Social Security Administration	Social Security Benefits
U.S. Postal Service	Mail Service

GAO REPORTS AND TESTIMONY ADDRESSING THE YEAR 2000 CRISIS

Defense Computers: Management Controls Are Critical To Effective Year 2000 Testing (GAO/AIMD-99-172, June 30, 1999)

Year 2000 Computing Crisis: Customs is Making Good Progress (GAO/T-AIMD-99-225, June 29, 1999)

Year 2000 Computing Challenge: Delivery of Key Benefits Hinges on States' Achieving Compliance (GAO/T-AIMD/GGD-99-221, June 23, 1999)

Year 2000 Computing Challenge: Estimated Costs, Planned Uses of Emergency Funding, and Future Implications (GAO/T-AIMD-99-214, June 22, 1999)

GSA's Effort to Develop Year 2000 Business Continuity and Contingency Plans for Telecommunications Systems (GAO/AIMD-99-201R, June 16, 1999)

Year 2000 Computing Crisis: Actions Needed to Ensure Continued Delivery of Veterans Benefits and Health Care Services (GAO/AIMD-99-190R, June 11, 1999)

Year 2000 Computing Challenge: Concerns About Compliance Information on Biomedical Equipment (GAO/T-AIMD-99-209, June 10, 1999)

Year 2000 Computing Challenge: Much Biomedical Equipment Status Information Available, Yet Concerns Remain (GAO/T-AIMD-99-197, May 25, 1999)

Year 2000 Computing Challenge: OPM Has Made Progress on Business Continuity Planning (GAO/GGD-99-66, May 24, 1999)

VA Y2K Challenges: Responses to Post-Testimony Questions (GAO/AIMD-99-199R, May 24, 1999)

Year 2000 Computing Crisis: USDA Needs to Accelerate Time Frames for Completing Contingency Planning (GAO/AIMD-99-178, May 21, 1999)

Year 2000 Computing Crisis: Readiness of the Oil and Gas Industries (GAO/AIMD-99-162, May 19, 1999)

Year 2000 Computing Challenge: Time Issues Affecting the Global Positioning System (GAO/T-AIMD-99-187, May 12, 1999)

Year 2000 Computing Challenge: Education Taking Needed Actions But Work Remains (GAO/T-AIMD-99-180, May 12, 1999)

Year 2000 Computing Challenge: Labor Has Progressed But Selected Systems Remain at Risk (GAO/T-AIMD-99-179, May 12, 1999)

Year 2000: State Insurance Regulators Face Challenges in Determining Industry Readiness (GAO/GGD-99-87, April 30, 1999)

Year 2000 Computing Challenge: Status of Emergency and State and Local Law Enforcement Systems Is Still Unknown (GAO/T-AIMD-99-163, April 29, 1999)

Year 2000 Computing Crisis: Costs and Planned Use of Emergency Funds (GAO/AIMD-99-154, April 28, 1999)

Year 2000: Financial Institution and Regulatory Efforts to Address International Risks (GAO/GGD-99-62, April 27, 1999)

Year 2000 Computing Crisis: Readiness of Medicare and the Health Care Sector (GAO/T-AIMD-99-160, April 27, 1999)

U.S. Postal Service: Subcommittee Questions Concerning Year 2000 Challenges Facing the Service (GAO/AIMD-99-150R, April 23, 1999)

Year 2000 Computing Crisis: Status of the Water Industry (GAO/AIMD-99-151, April 21, 1999)

Year 2000 Computing Crisis: Key Actions Remain to Ensure Delivery of Veterans Benefits and Health Services (GAO/T-AIMD-99-152, April 20, 1999)

Year 2000 Computing Crisis: Readiness Improving But Much Work Remains To Ensure Delivery of Critical Services (GAO/T-AIMD-99-149, April 19, 1999)

Year 2000 Computing Crisis: Action Needed to Ensure Continued Delivery of Veterans Benefits and Health Care Services (GAO/T-AIMD-99-136, April 15, 1999)

Year 2000 Computing Challenge: Federal Government Making Progress But Critical Issues Must Still Be Addressed to Minimize Disruptions (GAO/T-AIMD-99-114, April 14, 1999)

Year 2000 Computing Crisis: Additional Work Remains to Ensure Delivery of Critical Services (GAO/T-AIMD-99-143, April 13, 1999)

Tax Administration: IRS' Fiscal Year 2000 Budget Request and 1999 Tax Filing Season (GAO/T-GGD/AIMD-99-140, April 13, 1999).

Year 2000 Computing Crisis: Federal Reserve Has Established Effective Year 2000 Management Controls for Internal Systems Conversion (GAO/AIMD-99-78, April 9, 1999)

Year 2000 Computing Crisis: Readiness of the Electric Power Industry (GAO/AIMD-99-114, April 6, 1999)

Year 2000 Computing Crisis: Customs Has Established Effective Year 2000 Program Controls (GAO/AIMD-99-37, March 29, 1999)

Year 2000 Computing Crisis: FAA Is Making Progress But Important Challenges Remain (GAO/T-AIMD/RCED-99-118, March 15, 1999)

Insurance Industry: Regulators Are Less Active in Encouraging and Validating Year 2000 Preparedness (GAO/T-GGD-99-56, March 11, 1999)

Year 2000 Computing Crisis: Defense Has Made Progress, But Additional Management Controls Are Needed (GAO/T-AIMD-99-101, March 2, 1999)

Year 2000 Computing Crisis: Readiness Status of the Department of Health and Human Services (GAO/T-AIMD-99-92, February 26, 1999)

Defense Information Management: Continuing Implementation Challenges Highlight the Need for Improvement (GAO/T-AIMD-99-93, February 25, 1999)

IRS' Year 2000 Efforts: Status and Remaining Challenges (GAO/T-GGD-99-35, February 24, 1999)

Department of Commerce: National Weather Service Modernization and NOAA Fleet Issues (GAO/T-AIMD/GGD-99-97, February 24, 1999)

Year 2000 Computing Crisis: Medicare and the Delivery of Health Services Are at Risk (GAO/T-AIMD-99-89, February 24, 1999)

Year 2000 Computing Crisis: Readiness of State Automated Systems That Support Federal Human Services Programs (GAO/T-AIMD-99-91, February 24, 1999)

Year 2000 Computing Crisis: Customs Is Effectively Managing Its Year 2000 Program (GAO/T-AIMD-99-85, February 24, 1999)

Year 2000 Computing Crisis: Update on the Readiness of the Social Security Administration (GAO/T-AIMD-99-90, February 24, 1999)

Year 2000 Computing Crisis: Challenges Still Facing the U.S. Postal Service (GAO/T-AIMD-99-86, February 23, 1999)

Year 2000 Computing Crisis: The District of Columbia Remains Behind Schedule (GAO/T-AIMD-99-84, February 19, 1999)

High-Risk Series: An Update (GAO/HR-99-1, January 1999)

Year 2000 Computing Crisis: Status of Airports' Efforts to Deal With Date Change Problem (GAO/RCED/AIMD-99-57, January 29, 1999)

Defense Computers: DOD's Plan for Execution of Simulated Year 2000 Exercises (GAO/AIMD-99-52R, January 29, 1999)

Year 2000 Computing Crisis: Status of Bureau of Prisons' Year 2000 Efforts (GAO/AIMD-99-23, January 27, 1999)

Year 2000 Computing Crisis: Readiness Improving, But Much Work Remains to Avoid Major Disruptions (GAO/T-AIMD-99-50, January 20, 1999)

Year 2000 Computing Challenge: Readiness Improving, But Critical Risks Remain (GAO/T-AIMD-99-49, January 20, 1999)

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 23, 1998)

Year 2000 Computing: EFT 99 Is Not Expected to Affect Year 2000 Remediation Efforts (GAO/AIMD-98-272R, August 23, 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)

(511771)

**STATEMENT OF MOREY SULLIVAN, INFORMATION RESOURCE
MANAGER, KANSAS DEPARTMENT OF ADMINISTRATION**

Mr. SULLIVAN. Thank you Congressman Ryun and Congressman Horn and thank you for the invitation to show and share how we in State government are progressing toward our year 2000 efforts.

The Department of Administration first started serious year 2000 discussion in 1995. Knowing that a great deal of work would have to be done, we out-sourced some of that work, proposals were made by several nationally respected information technology firms. The successful bidder in our case was Computer Technology Associates or CTA from Bethesda, MD. A contract was put in place in December 1996. Since that time hundreds of applications have been assessed, they have been repaired and they have been tested. To date over 16 million lines of mainframe COBOL code have been remediated. We have identified 662 mission-critical applications that exist across Kansas State government. These are software applications that are critical to the running of the day to day operations of State government.

Knowing that State government and local units of government have common goals, Don Heiman, chief information technology officer, our boss, of the executive branch instituted a project called Outreach to the New Millennium in the fall of 1998. This program took nationally known speakers and IT professionals on the road across Kansas to share with local units of government successful strategies for dealing with year 2000 computer problems. Materials covering the remediation disciplines were printed and shared with each person who attended the Outreach summit. And I have copies of all these books that we have printed and will be glad to share them with you. Because of this program we feel that State government and local units are now better prepared to deal with Y2K concerns.

Currently the State government is approximately 95 percent complete toward our goal of full compliance. To date the State government has expended over 171,000 staff hours, we have got about 17,000 hours left. Although we are close to being finished, there are still lots of things to do. We are in the middle of Y2K auditing at the present time. We are in the middle of contingency planning in case some of those applications we have talked about don't respond the way we want it to when we roll over on December 31st.

Year 2000 has taught us in the IT community many things. Among them is we are more interdependent now upon one another than we have ever been. Just because your computer systems are year 2000 compliant, you should not feel safe, because we have linked our computers in so many ways, we must also be interested in our neighbors' Y2K compliance. State and Federal Government are much the same way. There are myriad links that exist between the two entities. Links that manifest in Kansas receiving funding from the Federal Government for literally dozens of programs. This funding then finds its way to thousands of Kansans across the State. Not an unimportant issue. Our Y2K efforts have included

tracking the Federal interfaces for just such compliancy. The gentleman who has guided us in this effort is Larry Kettlewell, seated to my left, and Larry will now report on Federal interfaces and share with you some other 2000 issues.

[The prepared statement of Mr. Sullivan follows:]

Statement by Morey Sullivan
Information Resource Manager
Division of Information Systems and Communications
Kansas State Government

Testimony

Mr. Chairman, thank you for the invitation to share how, we, in Kansas State Government are progressing in our Year 2000 efforts.

The Department of Administration first started serious year 2000 discussion and action in 1995. Knowing that a great deal of work would have to be out-sourced, proposals were made by several nationally respected information technology firms. The successful bidder was Computer Technology Associates or CTA from the state of Maryland. The contract was put into place in December of 1996. Since that time hundreds of applications have been assessed, repaired and tested. To date over 16 million lines of mainframe COBOL code as been remediated. We have identified that 662 mission critical applications exist across Kansas state government. These are software applications that are critical to running the day to day business of state government.

Knowing that state government and local units of government have common goals, Don Heiman, Chief Information Technology Officer of the Executive Branch instituted a project called Outreach to the New Millennium in the fall of 1998. This program took nationally known speakers and IT professionals on the road across Kansas to share with local units of government successful strategies for dealing with year 2000 computer problems. Materials covering all the remediation disciplines were printed and shared with each person who attended and Outreach Summit. Because of this program we feel that state government and local units are now better prepared to deal with Y2K concerns.

Currently we are approximately 95% complete towards y2k compliancy. To date State government has expended over 171,000 staff hours towards y2k we have about 17,000 left. Although we are close to being finished there are things still left to do. Such as y2k audits and contingency planning in case some applications don't respond the way we wanted at millennium roll-over on December 31st.

Year 2000 has taught the IT community in state government many things. Among them is we are more interdependent upon one another than ever before. Just because your computer systems are year 2000 compliant you should not feel safe, because we have linked our computers in so many ways we must also be interested in our neighbors y2k health. State and Federal Government are much the same way. There are myriad links between the two entities. Links that manifest in Kansas receiving funding from the federal Government for literally dozens of programs. This funding then finds it's way to thousands of Kansans. Not an unimportant issue. Our Y2K efforts have included tracking the federal interfaces for just such compliancy. The gentleman who has guided us in this effort is Larry Kettlewell. Larry will now report on federal interfaces and share with you other year 2000 Issues. Larry...

STATEMENT OF LARRY KETTLEWELL, INFORMATION RESOURCE MANAGER FOR FEDERAL AND STATE AFFAIRS, KANSAS DEPARTMENT OF ADMINISTRATION

Mr. KETTLEWELL. Thank you, Morey. Good afternoon, Mr. Chairman, Congressman Horn, we are glad to have you back in Kansas.

I'm very pleased to be part of the panel here today to give a status report on the efforts by the State of Kansas with respect to the year 2000 problem as it relates to our Federal and local interface.

A word for a moment about the Division of Information Systems and Communications [DISC], as it is known around here. Just so that people inside the Beltway don't think that we are a small time operation, we have a \$167 million budget. We are on the level of about a Fortune 300 information technology organization. We have 1,500 workers and manage 18,000 intelligent devices throughout the State. With that, Morey touched a little bit upon not what we derive over all from this information technology architecture. And very important to that is what we get from the Federal Government. The State of Kansas right now receives over \$1.8 billion in Federal funds, principally through automated processes known as interfaces or data exchange. Kansas has 138 of these interfaces disbursed amongst 14 Federal agencies. The year 2000 readiness of these interfaces obviously is very important in moving that \$1.8 billion back to the State.

I'm very happy to report that as of this morning, and I would like to make a correction for the record, from the State's end we are now 93.8 percent complete in terms of our compliance with Federal interface. As of early May, Kansas was second nationally in its overall Federal interface readiness. We no longer have available to us statistics on our status vis-a-vis other States. That said, I believe this figure gives our citizens some measure of how well we are doing.

Despite what some in Washington are saying about the Fed being 92 to 94 percent compliant, I would like to point out that that is an overall sort of figure. The Federal agencies that we deal with here in the State and their relevant interfaces right now have only about 72 percent compliance rate. This was, again, as of this morning and as reported on the GSA Federal Website.

This brings me to raise a couple of issues in keeping with Congressman Ryun's call for "straight talk." That 72 percent figure mentioned may be even lower. The figures that we have received from the Federal end have always been without reporting on critical programs from the Health Care Financing Administration [HCFA]. Mr. Willemsen touched briefly on Medicare and Medicaid problems, this is exactly what we are talking about here. This continues to be a very serious concern to us.

On June 2nd we were told by the President's Year 2000 Conversion commission that HCFA is "ready to go." Further, there is the thought about certain end-to-end testing on the top 10 programs from the Office of Management and Budget, and that they should commence with this end-to-end testing forthwith. Despite the assertions and assurances of HCFA's readiness in the Medicare and Medicaid programs, we remain skeptical.

Part of that skepticism is in part related to testimony by one of our witnesses today, Joel Willemsen, from the General Accounting

Office. In testimony before Congressman Horn's subcommittee on April 27th Mr. Willemsen presented a statement broadly aimed at the "Readiness of Medicare and the Health Care Sector." A great deal of that testimony, by the way, was relating to HCFA and its readiness. While that statement was made in April, it is clear that the current environment surrounding HCFA's mission-critical systems does not allow it to be "ready to go" now to test end-to-end. I'm sure, Mr. Chairmen, both of you have seen this report, it is very, very sobering.

The second aspect of this is the Payment Management System. Congressman Horn, you have already alluded to the fact in earlier testimony in your committee, this system moves \$165 billion worth of money back and forth between the Federal Government and the States, yet it is not year 2000 ready. We are ready out here to move money. We are confident that the Department of Revenue, Office of the Treasury, Division of Accounts and Reports, they have all gone through rigorous testing, we are ready to receive that money from this end. The concern, however, is that we are going to be treading water here outside the beltway and there is not going to be much left to give us.

Finally, let me just note here a couple of real reasons why we are here today. First, absent the work done by you, Congressman Horn, to bring this issue to the public attention, and even to the attention of some managers in Washington, we probably wouldn't be here today discussing this issue.

Second, as I understand from my years in Washington, there is nothing like member-to-member contact to get things done in Washington. Congressman Ryun has been very positive in continuing to reach out and inform people on this issue as you have done here today. We thank you both.

[The prepared statement of Mr. Kettlewell follows:]

**Statement by
Larry G. Kettfellow
Federal and Local Interface Manager
Division of Information Systems and Communication, Department of Administration
Kansas State Government**

Thank you Morey and Good afternoon Mr. Chairman,

I am very pleased to be a part of the panel here today and to be able to give a status report on the efforts by the State of Kansas with respect to the Year 2000 problem as it affects our Federal and Local interfaces.

First a word on the Division of Information Systems and Communications or DISC as it is known around here. It's the Kansas State division principally responsible for overall oversight and management of the Year 2000 problem. DISC is on the order of a Fortune 300 information technology organization. We have a \$167 million budget, around 1,500 workers and manage over 18,000 intelligent devices. Morey Sullivan has just given you some statistics on the effort that this "army" has put forth. Let me turn to a part of that effort and one that has a very significant impact on our state-- our interaction with the Federal government.

The State of Kansas receives over \$1.8 billion in Federal funds principally through automated electronic processes known as interfaces. Kansas has 138 of these interfaces disbursed amongst 14 Federal agencies. The Year 2000 readiness from both the Federal and Kansas sides depends on many of these interfaces which are critical to the delivery of goods and services to the citizens of our State. From the State's standpoint, we are now 91.5% compliant on our end of these interfaces. As of early May, Kansas was 2nd nationally in its Federal interface readiness. We no longer have available to us statistics on our status vis-à-vis other States-- but I believe this figure gives our citizens some measure of how well we're doing.

Despite some saying in Washington, that the Fed is now 92-94% compliant, I would quickly point out that is an overall figure. The Federal agencies that we deal with here in the State and their relevant interfaces leave the Fed end with 72% compliance-- a lessor figure.

This brings me to raise a couple of issues in keeping with Congressman Ryan's call for "straight talk". That 72% figure mentioned may be even lower. The figures from the Federal end have always been without reporting on the critical programs from the Health Care and Financing Administration (HCFA)-- namely Medicaid and Medicare. This area continues to be of concern to us.

At the same time, we were told by the President's Year 2000 Conversion Commission on June 2nd that HCFA is "...ready to go". Further, there is the thought that end-to-end testing of programs on the Office of Management and Budget's top 10 programs should commence forthwith. Despite the assertions and assurances of HCFA's readiness in the Medicare and Medicaid programs, we remain skeptical.

Part of that skepticism is based in part on testimony by one of our panelists today-- Joel Willemssen of the GAO. In that testimony, before the Congressman Horn's Subcommittee on April 27th, Mr. Willemssen presented a statement broadly aimed at the "Readiness of Medicare and the Health Care Sector". A great deal of the testimony was devoted to HCFA and its readiness. While this statement was made in April, it is clear that the current environment surrounding HCFA's mission-critical systems does not allow it to be "...ready to go". Without wanting to be too technical at this point, perhaps what we have here is a difference in definitions as to what's "ready". It strikes us that if end-to-end testing is to occur, the results will be rather hollow-- they will represent only a snapshot in time. Throughout this end-to-end testing, various changes mentioned by Mr. Willemssen will be taking place. With every change made to a program, testing must follow. According to the testimony, adequate testing had not even begun

on programs not receiving the aforementioned future changes. Hence, the fall time frame seems likely before the Fed end is truly ready. To add to this, as late as June 10, 1999 Kevin Thurm, the Deputy Secretary of the Department of Health and Human Services, before the Senate Special Committee on the Year 2000 Technology Problem stated "Because of the complexity of the Medicare program and the numerous small changes that need to be made to systems between now and this fall, HCFA *will continue to check and retest its systems for the remainder of 1999*". The bottom line is, what's the point of end-to-end testing if we know that one end is not truly ready?

With this in mind, we'd like to have at least a little say in our own destiny. We have already envisioned a "code freeze" or halt to programmatic changes to critical and other programs on a schedule that starts taking effect in the 3rd quarter of 1999. The testing regime on the Washington end of these programs will have a considerable effect on the way we practice change management. Obviously, we do not wish to deal with "new systems" and desire to deal with emergency fixes that are true emergencies.

A second issue and as important as the above is our, and our partner's, ability to "move money". On our end we are very confident that the work done by the Kansas Department of Revenue, the State Treasurers Office and the Department of Administration's Division of Accounts and Reports are all capable and ready to go. But these entities and our larger executive branch agencies to one degree or another depend on a Payment Management System that is not yet Year 2000 compliant. This was re-emphasized by Congressman Horn in a June 15th hearing dealing with the Federal Government's readiness. He noted at the time that "...this computer system processes nearly \$165 billion in payments and grant programs, such as Medicaid." This is a serious problem, which requires immediate attention given the consequences of payments not only to Kansas but also to all States. We look forward to some early statement as to what is being done to correct this problem.

With that said, to some here in the State, it would almost appear as if some Federal government agencies are trying to shift readiness concerns to the States. We hope this is not the case. In Kansas we are confident because of all of the measures that we have taken that we'll be in good shape. This begins with support from Governor Graves who has given us the policy approvals and guidance needed to manage this problem from the beginning. It continues on a daily basis with our relationship with the Secretary of Administration, Dan Stanley, a manager who understands technology. Our Legislature has also been instrumental in giving us the necessary resources needed to deal with this problem. In short everyone on this end is pulling together.

To return to our Washington partnership, we should give some examples as to agencies who we've noted are and have been very responsive. Department of Labor stands out as reaching out to do what they can to make a successful relationship with us. Not far behind would be the Department of Agriculture-- they've also been very helpful.

Finally, I'd like to note a couple of the real reasons we're here today. First, absent the work done by Congressman Horn to bring this issue to the public attention-- and even to the attention of some managers in Washington, we probably wouldn't be here today discussing this issue. Second, there's nothing like member-to-member contact to get things done in Washington. Congressman Ryun, you've been very positive in continuing to reach out and help inform people on this issue-- as you've done here today. We're thankful for both of your roles here today.

**STATEMENT OF JEFF WHITE, DIRECTOR, BUDGET RESEARCH
AND INFORMATION TECHNOLOGY, CITY OF TOPEKA**

Mr. WHITE. I feel like small potatoes here today when Mr. Kettlewell talked about the size of his organization. Let me give you a little bit of scale, as well, about the city of Topeka. We have 1,350 employees, \$135 million total annual budget for all city operations. We serve about 25 sites around the city in different city facilities. Again, I'm thankful today that I'm me and not Mr. Kettlewell as we look at the scope of this Y2K issue.

I'm going to give you today primarily the information technology perspective because that's my primary scope. But because information technology touches every corner of our organization, I hope to give you a bigger picture view as well.

We did begin in earnest with our Y2K preparedness effort in January 1998. Everybody is working hard on this and it's touched every facet of the organization. We have a full-time information technology staff of about 14 people, so we have relied on really a team approach to ensure Y2K preparedness and have many Y2K experts in every one of our operating departments.

We found ourselves in the situation of taking primarily a replacement strategy. We coupled our Y2K preparedness with a new information infrastructure. It certainly has been a cause of concern for our governing body in terms of the cost, but we have been able to achieve some improvements in our information infrastructure as we have addressed Y2K.

I'm really glad that Morey Sullivan is here today so I can thank him again for the efforts that the State of Kansas has made on their outreach efforts to local governments in terms of Y2K preparedness. The information they have provided has been an excellent road map for us to follow and we have used that every day as we move toward Y2K preparedness. So thanks again, Morey.

We are using the State Model for Compliance which involves assessment, application, mission-critical applications, remediating those that have problems, testing, and auditing our fixes and, of course, providing for business continuity through contingency planning. Also looking at tiers of mission-critical applications, those that are absolutely critical we can't do without and we can't work around them, if they don't work, we are dead in the water. Those that have to work without fail, but if they do fail, we can provide or work around. And those that if they don't work, we can live without it, there are work arounds available. So if the automatic coffee makers don't happen to come on at the right time, that's not a big deal for us.

As of today, assessment is complete, although we are continuing to keep our eyes open, as organizations change and we go through time, we have to be continually cognizant of additions that may create new Y2K problems that we have not taken a look at.

Our remediation efforts are almost complete as well. We have a few software replacements that are scheduled in the late summer to early fall, the majority of those are not mission-critical or at least mission-critical in the sense that we don't have work arounds.

I feel very positive that we have very few mission-critical applications that are home grown. Mr. Sullivan talked about all of the lines of code they had to rewrite, we simply don't find ourselves in

that situation, we do not have a lot of in-house code redevelopment that we have had to do. That's a double-edged sword. We don't have to go through the effort of 171,000 staff hours to recode those lines. The other is the fact that we rely very heavily on statements by our vendors that when they say they are Y2K compliant, that they really are. Again, we are using the testing protocol and such provided by the State, as well as some interesting things like a test lab where we can take our AS/400 or our legacy system, payroll and finance, and actually, rather than taking the city on line go to a testing environment, run those, and make sure they run correctly.

Testing has commenced and will continue through the Y2K turnover. And contingency planning has also commenced and will continue through Y2K. In our mind we look at Y2K in a lot of cases the same as any other disaster, man-made or naturally that might occur, and we have contingency plans already in place. Ice storms, tornadoes, whatever might hit, and a lot of those same rules apply as we look at Y2K. So I think we have got a head start as to contingency planning effort.

What's left? Continuing to work with the vendors, as I mentioned, is critical for us. Clean management, making sure that the fixes we make stay fixed. And that's an issue with the State as well. Public information is something I don't think we have done a terribly good job at and we need to do more as we get closer to the century turnover. And then interdependency on other organizations, those links are also in place. We have to make sure our neighbors are Y2K compliant as well.

People are mostly interested in the critical systems that we talked about; water, wastewater, and public safety. Water, we are ready to go. Contingency plans are mostly in place. We are going to deal with full stocks of chemicals at the turnover. And, again, we have contingency planning in place already for floods or power outages or those type of things. Most of the operations of the water plant are electromechanical. That means we can operate them manually. And we have folks trained that know how to operate those manually, which is important as well.

Wastewater is almost the same deal. Again, a contingency plan is in place. Public safety, although the county here runs our 911 operation, we are obviously a big partner with them and they are ready to go with 911. Southwestern Bell has been an excellent partner with us to make sure that that's the case.

Our biggest concern is lack of power, that really drives everything. We have worked closely with Western Resources to make sure that we will have power. And we do have standby emergency generation capabilities if we need them.

A couple of other concerns are civil unrest. What happens if people get a little weird in this Y2K turnover. The police and fire folks are taking a look at that and making sure we are staffed up and ready to go. And hoarding behavior is a concern as well. If everybody, for instance, goes to the bank and withdraws \$5,000 in cash on New Year's Eve, the criminals are going to love it. And so we want to be sure that the public information is out there to make sure that people have taken appropriate precautions. It's winter,

it's January, the power may go out due to an ice storm, folks ought to have a few days supply of food on hand and they ought to have blankets and warm bedding and just take the general precautions for any kind of emergency.

[The prepared statement of Mr. White follows:]

City of Topeka's Y2K Status
Presented by Jeff White

Year 2000 Issue (Unaudited)

The year 2000(Y2K) issue is the result of shortcomings in many electronic data processing systems and other electronic equipment that may adversely affect the City's operations as early as fiscal year 1999.

The City of Topeka has completed an inventory of computer systems and other electronic equipment that may be affected by the Y2K issue and that are necessary to conducting City operations.

The City's Y2K planning model includes these elements:

1. Assessment of Y2K problems
2. Remediating those problems
3. Testing/Auditing the remediations
4. Contingency planning for mission-critical applications

Assessment

The City is 90% complete with assessment of mission-critical applications and Y2K's potential impact on those. The City will be at 100% by 7/1/99.

The remaining 10% is proprietary, used by only one or two departments. Examples include the industrial treatment equipment used by Water Treatment, Auto-external defibrillators by the Fire Department and embedded chip-based systems.

Remediation

The City is 80% remediated. We plan to be 95% complete with remediation of known concerns by 7/1/99 and 100% by 10/1/99.

Our wide and local area networks are 100% complete. All hubs, routers, switches, and CSU/DSU unites (ISDN modems) are Y2K compliant. All permanent servers are Y2K compliant. All network firmware (management modules) and administrative software are Y2K compliant.

Our PCs are 100% compliant

All standard PC operating system software and business application software are 100% compliant.

We have a number of small, single-department-user database and information collection programs, which are in varying states of compliance. These are being converted to compliant software or rewritten to accommodate the new century. This is about 50% complete at this point; many of these systems are not mission-critical.

Two of our three AS/400s are 100% compliant on the hardware and operating software side. The Fire Department AS/400 is not compliant due to operating system version. Upgrades to assure Y2K compliance will be complete by 7/1/99.

On the AS/400 software side, our financial accounting, personnel, payroll, purchasing, and fleet maintenance software is certified compliant by the vendor, HTE, Inc.

We have a number of 3rd party and home grown applications for the AS/400 platform that are not compliant. We are either replacing, rewriting, or porting to PC platforms these applications. We are approximately 70% complete at this point. Many of these are mission-critical.

Except for the AS/400 application problems expressed above, we are down to the smaller, non-uniform technologies used by individual departments. We are working with the departments to ensure Y2K is addressed for these items.

The City has completed all testing and validation on its portion of the 911 Police and Fire reporting system. The 911 Police and Fire reporting systems have data interchanges with several other such systems, some of which have not been tested and validated. The Shawnee County Consolidated Emergency Communication Center bears primary responsibility for 911 call handling.

The traffic control system has been assessed and all problems remedied. Validation and testing of these systems have yet to be completed, and will be by October 1, 1999.

Testing

Testing has begun and will continue through the end of the year.

Contingency

Contingency planning has begun and will continue through the end of the year.

Summary

Despite our best efforts at compliance, industry experts indicate that a 95% confidence level on Y2K compliance is reasonable. This means that we will have failures; we will have troubles; and we will have a challenging first quarter of 2000. Our plan is that these failures will be more nuisance than crisis and that our Contingency Planning will provide for successful work-arounds to these problems.

We are compiling documentation of every mission-critical application throughout the City to show our Assessment, Remediation, Testing/Auditing, and Contingency Planning efforts. This provides the benefit. We know absolutely that we won't overlook anything critical.

For 1999, the City will commit in excess of \$750,000 to address Y2K issues. This commitment includes personnel and contract staff time, equipment, software and related technologies. These costs are included in the operating budgets of the various departments.

Because of the unprecedented nature of the Year 2000 issue, its effects and the success of related remediation efforts will not be fully determinable until the year 2000 and thereafter. Management cannot assure that the City is or will be Year 2000 ready, that the City's remediation efforts will be successful in whole or in part, or that parties with whom the City does business will be year 2000 ready.

Previous item entered by Bill Stephens

**STATEMENT OF JOY MOSER, ADJUTANT GENERAL'S
DEPARTMENT, PUBLIC AFFAIRS OFFICE**

Ms. MOSER. Thank you, Congressman. The Adjutant General's Department is the emergency response agency in Kansas and it has been dealing with disasters for many years. The difference that we have here is that Y2K we know when it is expected. With a tornado or snowstorm or flood, there is little to no warning. With Y2K, December 31st is certainly a crucial time. And, therefore, we are working to prepare ourselves and to provide preparation for the public.

Preparedness is what we do in the Adjutant General's Department. It has the Division of Emergency Management whose mission is to prepare for and coordinate the response and recovery activities in the event of a disaster. It also has the Kansas National Guard whose State mission is to provide emergency response when called upon to assist the citizenry. So both the groups in our department are working hard to be ready for a response in case it's needed on December 31st or in the days that are following.

There are three areas that we are addressing. First of all, what we are doing prior to December 31st; the plans that we have in place for December 31st and January 1st; and then what we think the public ought to do to prepare themselves to help themselves.

The Division of Emergency Management and the Kansas National Guard are planning and training to respond if there is an infrastructure failure due to Y2K related problems. We are preparing by doing the same kinds of things that we do for snowstorms, ice storms, floods and tornadoes. So it's that type of thing.

For instance, in a thunderstorm or a snowstorm, or flood, or tornado, you might have power outages and you also might have telephone communication losses. Those are things that we are also planning for with Y2K. We know that we need to look at getting water, making water available, making sure that there is food, and that there is warmth and shelter during the winter months. And that's the kind of thing that we deal with regularly when we respond to snow or ice storms and tornadoes and flooding. The Division of Emergency Management coordinates State and volunteer agencies efforts to provide relief as indicated in their operations plan. We want the public to know that we are in fact doing that for Y2K. It's just a different type of disaster or emergency that we need to plan for.

Internally, the Kansas National Guard is testing equipment to make sure they are ready and it will be functioning at midnight on December 31st. All level logistics systems in the State have been upgraded. So those computer systems are working and they can fulfill the tasks of supply and service, should that be needed. Also, in May, a communications exercise was held with high frequency radios and we communicated with the Pentagon in Washington, DC. And we are a communication node so, we communicated with the seven States that are in our area. So we will be able to communicate if there is a disaster for Y2K. We also have inception for another communications exercise. At this time we are going to go to the armories within the State and we will be communicating with each one of the armories. We will have people avail-

able so that if there is a need on December 31st we can help the citizenry.

Prior to December 31st, State agencies will also be coordinating public service information so that we can provide informational preparation to the citizenry. A campaign is expected to begin in September, and will continue through December 31st. We believe this is beneficial to the public because it will help the public to understand the steps that we are taking to respond in case of an emergency. It will also provide them with the information to help them help themselves.

On the 31st, we intend to have people in our Emergency Operations Center here in Topeka to communicate with the media about what is going on. We expect also to have personnel in the Division of Emergency Management that will respond to requests that we may get. And we also will have a Kansas National Guard military operation center in effect here in Topeka. That center will be open at 6 p.m. on December 31st and it will go through the night, through January 1st, and will end at midnight on January 1st. And then we will have people at the battalion headquarters that will also be able to communicate and help.

The third area that are we were talking about was to help people help themselves. And some of the things that we are talking about there is backup heat sources such as fireplace, blankets, extra batteries if the power goes out, bottled water, extra food supplies, all of these are things that we suggest you use for any other disaster. And we will continue to provide that information. Thank you.

[The prepared statement of Ms. Moser follows:]

Meeting the Year 2000 Challenge
Sponsored by Congressman Jim Ryun
July 7, 1999

Joy D. Moser
The Adjutant General's Department
Public Affairs Office

With a little less than six months left before Y2K becomes a reality, it is certainly time to talk about what we in the State of Kansas are planning for the potential crisis of the year. The Adjutant General's Department, as the emergency response agency in Kansas, has been dealing with disasters for many years. The difference with Y2K is that we know when it is expected. With a tornado, snowstorm, or a flood, there is little to no warning. With Y2K, December 31 is clearly a crucial time. Therefore we need to prepare, and make the public aware.

Preparedness is what we do in the Adjutant General's Department. The Division of Emergency Management's mission is to prepare for and coordinate response and recovery activities in the event of a disaster. The Kansas National Guard's state mission is to provide emergency response when called upon to assist the citizenry. Both groups in our department are working hard to be ready if a response is needed on December 31 and the days following.

There are three areas that we are addressing as we prepare for Y2K. What are we doing prior to December 31 to prepare for Y2K? What is the plan for response if needed on December 31? What should the public be doing to prepare themselves for possible problems of Y2K?

Currently the Kansas Division of Emergency Management and the Kansas National Guard are planning and training to respond if infrastructure fails due to Y2K related problems. And they are preparing by doing the same types of things that are needed for floods, tornadoes and snowstorms.

In a thunderstorm or snowstorm there is a good chance of power outages and some telephone communications loss. In Y2K these are two of the areas that have a potential for loss also. So there may be a problem with getting water, preparing food, or keeping the shelter warm since this event will occur during the winter months. These are things

we deal with on a regular basis whenever we respond to snow or ice storms, tornadoes and flooding. The Division of Emergency Management then coordinates state and volunteer agencies efforts to provide relief as indicated in their operations plan. We want the public to know that we will respond to the Y2K problems as we would to any other emergency.

Internally, the Kansas National Guard is testing its equipment to make sure it is ready and will be functioning at midnight December 31. All unit level logistics systems in the state have been upgraded so those computer systems can fulfill the tasks of supply and service. In addition, the Kansas Army National Guard just completed one communications exercise in May, using high frequency radios to communicate with the Pentagon in Washington, D.C., and seven of the surrounding states. Another communications exercise will be held in September, which will also include communications to all the armories in the state so that contact can be maintained with all the Guard units if there is a communications failure.

Prior to December 31, state agencies will be coordinating Public Service information efforts to keep the public informed on ongoing Y2K preparations and to promote emergency planning. A campaign is expected to begin in September and continue through December 31. We believe keeping the public informed is beneficial because it will help the public to understand the steps we are taking to respond in case of an emergency and it will provide the public with information to help them help themselves.

The Public Affairs Office also plans to conduct meetings with news media prior to the event to discuss communications plans for the evening of December 31.

In addition to plans for personnel on duty to communicate with the media, there will be personnel on duty with the Kansas Division of Emergency Management in their operations center in Topeka to respond quickly to any requests for assistance. Also, the Kansas National Guard will have a military operations center open at the state headquarters in Topeka from 6 p.m. December 31 through the night and day until midnight on January 1, 2000. Subordinate headquarters down through the battalion level will also be available to communicate and provide a quick response. Each site has a plan to contact its members in the event they are needed.

If other state agencies are needed for response on December 31 and January 1, a procedure is available to do that.

Our third area is to assist the public in preparing for Y2K. Again it is important that the public prepare for this potential emergency like any other emergency. Natural disasters disrupt power and communications all the time. There are specific preparations advised in those events. For example, to prepare for power failures associated with winter storms, the public is advised to have a backup heat source such as a fireplace, blankets and sleeping bags. A good light source in a power failure is a flashlight with extra batteries. A battery-powered radio with extra batteries would be a good idea. Bottled water, extra food supplies and other emergency supplies such as a first aid kit, extra prescription medicines, changes of clothing, rain gear, credit cards and cash are other emergency precautions citizens should have available for any emergency.

Citizens should also be prepared for what may be the main disruptions of Y2K. Predictions now indicate that Y2K disruptions may more often be problems with record keeping. It makes sense then to keep hard copies of credit card bills, bank statements and other such personal and financial information to make adjusting these records easier if in fact a problem develops because of Y2K.

We are preparing for the end of the century. We encourage you to prepare for it too.

Mr. RYUN. I want to thank all of our panelists. We are going to go to some questions. I know we have some questions that are being generated on the cards. There are cards that are still being handed out. If you would like to write a question, one thing that I have to respect is the fact that the chairman has a plane to catch, so we will have maybe another 15 minutes roughly of questions and then we will move to the second panel. But I actually would like to begin with Mr. Sullivan. And one of the concerns that we have is a continuing readiness aspect of compliance with Y2K issues as we enter into the millennium. You had said earlier that you're 95 percent ready, you're still about 5 percent before you can be completed. Can you identify what that 5 percent is? You said also that it will take probably another 17,000 hours roughly to finish what has to be done. Is there sufficient time?

Mr. SULLIVAN. Yes, there is. Much of what remains to be done is testing continuity planning. We have looked at primarily all of our COBOL codes, we have assessed everything, we have repaired most everything. There are a few applications out there in the State government that have received a little attention, but not as much as what there needs to be. So in answer to your question, yes, there is sufficient time to get there because that 17,000 hours is spread across State government and across the many thousands of employees that we have. So that is not a problem. We just need to continue to complete our auditing.

Mr. RYUN. Chairman Horn, any questions?

Mr. HORN. Let me read some from the audience because we know the panelists have to leave for other engagements, we know you are all busy people. But one of them is this: "During this period of correcting Y2K problems is the entire information network of government agencies becoming vulnerable to computer hackers? What security is there?"

Mr. Willemsen, do you know the answer to that? Let's have the power of the GAO and its thousands of reports hone in on this question.

Mr. WILLEMSSEN. I think that's an excellent question. One issue that we have previously addressed as Y2K is being addressed and as systems are increasingly opened up to make the fixes and also bringing in other parties to help make the fixes and test those fixes, there is enhanced risk from a security perspective. And we have previously testified that managers, therefore, must be very attuned to that security risk when going about their Y2K programs.

And therefore, I think it is an excellent issue. One that information security is the next Y2K, as we see it. It's increasing in scope and severity and an issue that the Federal Government I know will have to increasingly begin to focus on.

Mr. HORN. I think you will all enjoy the second question, we are in the middle of some of this, "Why can't we as the people just decide to change the date similar to daylight savings time so the problem is solved? We all agree and then later change it back."

At first appearance you might think there is something wrong with that question, but I'm planning to hold a hearing on one of my colleagues' bills, Mr. Linder of Georgia, that will move the January 1st date to Monday if it isn't there now, and that will give them the whole weekend to be working on it should something go

wrong. In order to get this good idea explored, we also have to get the Subcommittee on the Civil Service, which is part of the Government Reform Committee, and I don't know how many other hands want to get into it or don't want to get into it.

But you tell us, Mr. Willemsen, has some thought been given to this and what has the discussion been about?

Mr. WILLEMSSEN. There has been discussion about making January 3rd, which is a Monday, an additional holiday. Based on information we know, however, from the standpoint of several agencies they already have very detailed plans in place, assuming that is not a holiday, and, therefore, to make a change at this relatively late date could potentially for those organizations cause more problems than solutions. So we need to be very careful about doing that. Especially some of the leading agencies such as the Social Security Administration, they have their time table down to the minute on exactly what they are going to be doing every minute through the roll over period. And upsetting that apple cart at this point could introduce more risk than solve.

Mr. HORN. If we get that hearing, we will make sure you're there.

Mr. RYUN. I know this morning as we were talking on Jim Cates' show you expressed great confidence in the ability to fly on January 1 after you said that a few moments ago. Part of what I think the question is going to be dealing with is the understanding, if you will, that part of what this issue relates to is the labor intensive having to go back and change little chips in different places. You expressed great confidence that your flight would leave Washington and land in L.A. In fact, you have expressed greater confidence in that than the elevators in Canada would work for you, I think you had some difficulty there.

So I think part of what we are dealing with is that a lot of places where the light needs to shine with regard to the Y2K issue and we have begun the process of making the changes in some of those areas.

Mr. HORN. Along that line, one of the things, and maybe you would like to respond to it, having to go through this tedious operation in order to make up and adapt and all of that, I hope a lot of you have said, "Hey, do we really need this system? Let's get rid of that." How much of that really was part of what you did and you just got rid of it because it isn't working?

Mr. WHITE. We have used this opportunity to do a lot of standardization on types of software we use, desktop on PC's. And we have used a lot of old stuff our AS/400 systems and found out that people weren't really using them and if they were, there were easier ways to do it.

Mr. SULLIVAN. We found that to be true in the State government as well.

Mr. KETTLEWELL. I'll just comment on that. One of the things about this is that the United States being so information technology driven, if you will, this has been an excellent opportunity for all of industry to stop the train, assess what they have done and for all intents and purposes. Like with, for instance, the city of Topeka has done, edit what they have got, throw away the old programs that are not standard and so old they are no longer efficient.

And we have done that in the State, we have a program like that we have gone through and pitched a lot of programs. So there is a degree of standardization and modernization.

Mr. HORN. Ms. Moser, did the Adjutant General do some of that? Did you get rid of some of that stuff?

Ms. MOSER. We got rid of some of our old junk, yes, sure.

Mr. HORN. Was that the COBOL? That's a language of the 1960's. And, believe me, people that retired and were experts in COBOL, the Civil Service Commission, now called the Office of Personnel Management for Federal employees, is getting them out of retirement, they can keep the \$100,000 contract, to solve the COBOL problem, and keep their pension. So it's a good deal for people that mastered COBOL. I remember making a program out of one, only one, in the 1960's.

But that's a language that is all over the Federal Government, I don't know about the State governments. Do a lot of yours use COBOL?

Mr. KETTLEWELL. Most of them do, yes.

Ms. MOSER. We went to mainframe last year. So we should be OK.

Mr. HORN. That's great. One question here is: "Will the Congress watch the President over Christmas? We have heard the President will declare martial law while the Congress is on vacation." There is nothing to that, folks. The courts of the United States are open and the Congress is open. We are very careful, not just under this President, any of the last Presidents. If there is a need for us to get into session, that's the way the adjournment resolution is written by both the Senate and the House. The Speaker of the House can call the House together, the Majority Leader of the Senate can call the Senate together. So there no chance of that. But these rumors hop around all of the time.

"Please make a statement about security of bank accounts and balances, availability of cash, availability of fresh food supplies, state of police, fire, military, medical." Well, we have got good people here in the Adjutant General's Office to deal with that and we have got Mr. Willemsen on broad international as well as National review. So the security of bank accounts and balances, the Federal Reserve I think has done a terrific job, Mr. Greenspan, 2 or 3 years ago when I talked to him when we started in on our operations, he appointed Board of Governors member Kelly to be in charge of this. And most of the banks of the United States you don't have to worry about. Some of the State banks you might have to through your own regulatory authority in Kansas. I don't know where you are on that. Maybe some of the officials in the State of Kansas like Mr. Kettlewell knows that question on the banks.

Mr. KETTLEWELL. In a broad way I do, yes. The Kansas Corp. Commission really is a controlling factor in that. That said, about 3 weeks ago I was down in Hillsboro, KS addressing about 150 citizens. At the time we had the regional FDIC examiner come in from Memphis, TN and he told me that of the I believe it was around 10,000 or so banks, there are only about 10 or 15 that are doomed for failure, and those banks are going to be taken over. It is one of the most heavily regulated industries, so that the failure rate there—the bottom line is you need to keep your money in the bank,

don't put it under the mattress, don't hide it in the silo, don't hide it in the barn, keep it in the bank.

Mr. HORN. I think we will ask panel two's group because there are some talents there, bankers and others. On the fresh food supply, I think it's prudent, and I think Mr. Ryun agrees with me on that, just to be reasonable about it. You don't need all of the food for a year, but you might need 1 or 2 weeks, vegetables—now, remember, your refrigerator might go out if there is a power failure. So you have got all those things that could happen.

But when you come from California as I have, where you have got fires, earthquakes, floods, I have got the biggest flood project in the Nation in my district. For example, 500,000 people are affected by it and we are trying to get it done in the next year and a half so that the levees won't overflow. And you know what that's like in Kansas and Iowa and Illinois, to say the least. I think somebody said this morning, I think it was, that quoted one of the newsmen, was it, when Cates talked to us and said there would be a shortage of toilet paper. This is on something 10 years ago, and indeed the next day all of the toilet paper disappeared from the grocery stores.

So little things like that you might just use common sense on. I don't think it's something to panic about. A lot of people are going to make money on books they write on Y2K. I've got a long shelf of them. I have just packed them to send to the National Archives. Maybe the next millennium they can pull that box out and see what happens. But I'm not going to collect them anymore. But you will have all of the little papers that you see in the grocery lines for a couple of bucks they want to scare the living daylights out of you. And some people fall for that stuff, we don't exactly—in some areas—have a very literate constituency to work with on this. But even sometimes people get a panic there might be some reason behind it and we in government need to do the best we can to avoid that situation to keep our heads calm to solve the problem, not just talk about it.

Any comments, Mr. Willemsen, on the food supply, the fresh food supply to be exact, availability of cash? Mr. Greenspan has ordered an extra amount of Federal Reserve notes to be in the bank so if there is a run on them, they have plenty of money. And it was said, and you're right, to take it and put it in your pocket at home is where the burglars will head. They also watch television. If you're smart, you will leave it in the bank and let them hold the responsibility for it.

Mr. RYUN. I have one final question. I know we are just about out of time. I want to ask Mr. Kettlewell very quickly about an issue I know is very important to a lot of our seniors out here. You said earlier that HCFA is not—that the administration keeps saying that they are ready, but they really aren't ready in your opinion. What can we do to make that correction? What sort of contingency plans are there for our seniors that are out there?

Mr. KETTLEWELL. Well, a couple of thoughts on that, Congressman Ryun. First of all, you're going to have to have a contingency backup plan, obviously. As I heard one representative from HCFA testify in front of Congressman Horn's subcommittee last fall and their contingency plan at that point was manually processing

claims. Now, they process 20 billion claims in a year. I don't know how many temp workers they are going to be able to bring in and process those claims and that amount of money. So I don't know what the good solution is in terms of their business continuity. What I do know is that some way or another Health and Human Services in Washington, DC has to provide better information with respect to its status on Medicare and Medicaid. People in Washington have to be singing off the same song sheet or they have to have one spokesman to tell what the real story is, because there is just a tremendous amount of confusion out there right now. From one person we get one story.

As I say, as I quoted in my statement, but if I listen to your committee and listen to the GAO, and I again go back to that testimony of Mr. Willemsen, they are not going to be able to perform. There is not a really good short answer to your question. I think right now they are besieged, they are in a very difficult situation in HCFA. How they are going to solve that problem perhaps is add more resources to it, maybe stop coming out here and auditing the State agencies, for instance. We have already been through a State Aging audit, we passed with flying colors, both from HCFA and the Administration on Children and Families.

So I think really what they need is they need to focus back in Washington and less focus out here in the States, because I think the States by and large are doing a lot better job in managing their systems than what's going on in Washington.

Mr. HORN. We did have the problem a year ago where Social Security, which has led the pack since 1989, found that they forgot to include their State supported operations.

Mr. KETTLEWELL. Yes. We found that out in March, sir.

Mr. HORN. And those have been fixed.

Mr. KETTLEWELL. Yes, they have.

Mr. HORN. Joel, do you have anything to say on HCFA? HCFA means the Health Care Financing Administration.

Mr. WILLEMSSEN. It does administer Medicare and helps the States administer Medicaid. Just to provide a broader context to this, unfortunately HCFA got an extremely late start on Y2K for Medicare. Second, they have an extremely complicated set of computer systems and data exchanges, much of which is not under their direct control. You combine those factors with the limited amount of time available and also their relatively poor track record in managing information technology, and that's why they are in the risk status they are currently in.

I'm a little more optimistic now with the Health Care Financing Administration than I would have been last fall, in part because the leadership of the Administrator, she's done what she can in the limited time remaining. She also has put a primary emphasis on contingency planning and they have done some good work in that area. Those plans now include options beyond just manual processing of claims. Some of those options cannot be publicly disclosed because they give a security perspective that we talked about before. But it's possible there will be some disruptions in Medicare. Again, I feel more confident, though, that they have gotten their act together on contingency plans. So to the extent those disruptions occur, they have backups in place to address them.

Mr. HORN. Thank you. I want to ask Mr. White, here's a question for you. "What is the city of Topeka doing as a contingency plan for emergency services such as police, fire and hospital, the 911 and so forth?" That seems to be a nationwide problem.

Mr. WHITE. Absolutely. Really good question. Again, we have contingency plans already in place for any kind of disaster and certainly work very closely with the Adjutant General's office and with Shawnee County who runs our 911 system. They have secondary backup plans for running 911. And certainly, as she mentioned, this is a potential disaster that we can prepare for.

So the police chief and the fire chief are coordinating very closely with the other emergency providers to ensure that if we have a police emergency, we will have a police car there. If we have a fire, we will have a fire truck there. If you need an ambulance, ambulance service will be available. If you have any concerns, questions, emergencies, you can call 911, somebody knowledgeable will pick up and dispatch the appropriate folks to you.

Mr. HORN. In other words, you have a real human being there at that center.

Mr. WHITE. We have about nine of them at any given time.

Mr. HORN. I take it, because this has nothing to do with the millennium, but it's something we have had to deal with for years, and that is the relationships of surrounding fire departments, police, law enforcement agencies, and do you have enough frequencies for them to communicate with each other?

Mr. WHITE. I'm not involved with the radio issues. The Adjutant General's office might be able to speak better to that. I would imagine that's one of those things they are looking quite closely at.

Ms. MOSER. Certainly we are looking to communicate within our own system and then we will communicate out to the local level. So I think that we could make that connection.

Mr. HORN. When I was a university president 10 years ago, the county of Los Angeles went into an extensive emergency situation, we have 81 cities in that county, 10 million people, and we have about probably 15 universities with their own police force and jurisdiction for several miles around, but we didn't have the frequencies, they were all sitting in New York on the east coast and we had to work it out. We couldn't communicate with each other. When you have got that many people, 81 cities, it's pretty tough. So they are slowly working that one out and they have had 10 years to do that because we knew we had real problems.

Ms. MOSER. That is always a problem is whether or not the frequencies are the ones you can communicate across. But we are working on that and I think that we will be able to do that.

Mr. HORN. Here's a very well written one. It says, "Coal is used to power a majority of our Kansas electric utilities. From all of that I have read, the railroads absolutely will not be ready. How will we keep our electricity up and going if they cannot get coal?"

Any comments from State government, Mr. Kettlewell?

Mr. KETTLEWELL. I defer to my colleague from Western Resources on that, but basically, from my conversations with them before, they have weighed in extensive amounts of coal, even if the railroad ceased to run, so that reserve supplies for coal for coal

fired utilities would be available. But, again, I defer to my colleague from Western Resources.

Mr. HORN. Here's a question for Topeka, it's on the water. And I might say this is the best water I have tasted in a long time, so you have got a good water department, it's very marvelous. I have been getting all I can get. We have to get bottled water in Washington. The Corps of Engineers did a wonderful job in 1859 with the distribution system. But the city of Washington has not replaced much since 1859. And when the metal starts to glow when we were having x rays, we went to bottled water. That's what they say happened to the Rose Republic, for those who want to talk about it. That's about it. We will pursue some with the next panel. We need to move to panel two, Mr. Chairman. I think we have got a good round on that.

Mr. RYUN. Thank you all very much for coming. I appreciate it.

[Applause.]

[Witnesses sworn.]

Mr. RYUN. The second panel is going to be dealing more with industry. For those of you who would like to participate, there will be some staffers around the edges who will have cards, if you would like to write out questions and submit them, we will ask those questions as we proceed.

Let me begin by introducing the first panelist, it's Bud Park. Bud is the year 2000 project office manager for Western Resources who provides power to homes and businesses. The KPL division is a Kansas Gas and Electric subsidiary that provides electricity to over 614,000 retail and 75 wholesale customers in more than 500 Kansas communities. It is a member of the three power tools, coal, nuclear, natural gas, oil, diesel fuel, these units generate a net capacity of nearly 5,300 megawatts.

**STATEMENT OF BUD PARK, YEAR 2000 PROJECT OFFICE
MANAGER, WESTERN RESOURCES**

Mr. PARK. Chairman Horn, Congressman Ryun, distinguished guests and ladies and gentlemen, good afternoon. I thank you for this opportunity to speak with you today.

Mr. RYUN. Mr. Park, let me interrupt you just a moment. If you would like to submit your comments and just speak off the record, you can add those to the record and we will be happy to include them.

Mr. HORN. Automatically we put the full comments in the record when the chairman calls your name. In order to get through the day, we would like you to take 5 minutes and express yourself on it and then we will go to the next witness. And that gives us more of an opportunity to have a dialog on your panel, as well as the members here today.

Mr. PARK. Certainly, I'll be happy to. Basically we come here to tell you the message that as of last week Western Resources is now year 2000 ready.

We started our project over 3 years ago, I think that's a little earlier. I think we had a jump on a lot of companies. And so we have had plenty of time to address the year 2000 issue. We have done what has become the de facto standard year 2000 program, including all of the steps that you have probably heard many times

before. And we concluded the project last week on June 30th with the dispatch of a letter to the North American Electric Reliability Council who, as you know, has been doing an assessment since last year of the nationwide power grid. That letter essentially told NERC that Western Resources had concluded its assessment, remediation and testing of all of our NERC critical systems, software and hardware that contain embedded chips and we have tested them all and our testing shows that we expect to be able to provide service to our customers after January 1st, 2000 just like we do now.

We have established extensive contingency plans as part of our program. We have also put into place clean management procedures to ensure that all readiness work that we have done to date doesn't get undone by some well-meaning programmer who makes a change that might not be compliant with the year 2000 roll over before January 1st.

So the bottom line is we expect to keep the lights on. Our testing has shown that we believe that will be true. We will participate in a drill that NERC is hosting on September 9th. We expect that the results of that nationwide drill will help prove what we have come here to say, that we expect no service interruptions.

[The prepared statement of Mr. Park follows:]

WESTERN RESOURCES Y2K UPDATE - JULY 7, 1999

GOOD MORNING, LADIES AND GENTLEMEN. MY NAME IS BUD PARK. I'M THE YEAR 2000 PROJECT OFFICE MANAGER FOR WESTERN RESOURCES. DURING THE NEXT FEW MINUTES, I'D LIKE TO TELL YOU ABOUT WESTERN RESOURCES' PREPARATIONS FOR THE UPCOMING CALENDAR ROLLOVER TO 2000, COMMONLY REFERRED TO AS "Y2K".

WESTERN RESOURCES BEGAN ITS YEAR 2000 WORK IN 1996 WITH SOME OF OUR COMPUTER DEPARTMENT'S LARGER MAINFRAME PROGRAMS. WE SOON REALIZED THAT THE SCOPE OF THE Y2K ISSUES WAS MUCH LARGER THAN WE INITIALLY THOUGHT. THUS, IN EARLY 1997 WE EXPANDED OUR READINESS EFFORTS TO INCLUDE THE REST OF THE COMPANY'S DEPARTMENTS AND BUSINESS UNITS BY ESTABLISHING THE YEAR 2000 PROJECT OFFICE, PUBLISHING A CORPORATE YEAR 2000 READINESS POLICY, AND IDENTIFYING 16 DEPARTMENT AND BUSINESS UNIT Y2K PROJECTS, EACH WITH ITS OWN PROJECT MANAGER. SINCE THAT TIME, WE HAVE BEEN WORKING DILIGENTLY ON FINDING AND FIXING ALL THE CALENDAR ROLLOVER-RELATED ISSUES THAT MIGHT POTENTIALLY AFFECT OUR ABILITY TO PROVIDE ELECTRIC SERVICE TO OUR CUSTOMERS.

WESTERN RESOURCES' Y2K PROJECT TOOK THE FORM THAT HAS BECOME THE DE FACTO INDUSTRY STANDARD. IT INCLUDED THE PHASES OF AWARENESS, INVENTORY, ASSESSMENT, REMEDIATION, TESTING, CONTINGENCY PLANNING, AND CLEAN MANAGEMENT. CLEAN MANAGEMENT IS THE SET OF PROCEDURES WE IMPLEMENTED TO ENSURE THAT NONE OF OUR COMPLETED Y2K PREPARATION WORK GETS "UNDONE" BEFORE JANUARY FIRST BY THE ADDITION OF SUBSEQUENT SYSTEM MODIFICATIONS OR UPGRADES THAT MIGHT NOT BE Y2K COMPLIANT.

WE ESTABLISHED GOALS OF DECEMBER 31, 1998 FOR FINDING AND FIXING ALL THE POTENTIAL PROBLEMS IN OUR MISSION-CRITICAL SYSTEMS, AND JUNE 30, 1999 FOR HAVING THOSE SYSTEMS TESTED AND MAKING THE COMPANY "YEAR 2000 READY". I AM HAPPY TO REPORT THAT WE ACHIEVED BOTH THOSE GOALS, AND ON JUNE 30TH REPORTED TO THE NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL (NERC), WHO HAS BEEN CONDUCTING A NATION-WIDE ASSESSMENT OF ELECTRIC SYSTEM RELIABILITY AT THE REQUEST OF THE U.S. DEPARTMENT OF ENERGY, THAT WESTERN RESOURCES IS NOW YEAR 2000 READY. WE WERE ONE OF MANY ELECTRIC UTILITY COMPANIES THAT PARTICIPATED IN THE NERC ASSESSMENT, REPORTING OUR READINESS STATUS TO THEM ON A MONTHLY BASIS, AND USING THE NERC-DEFINED CRITERIA FOR IDENTIFYING CRITICAL SYSTEMS.

DURING OUR PROJECT, WE IDENTIFIED THE COMPUTER SOFTWARE, HARDWARE, AND DEVICES WITH EMBEDDED CHIPS WHICH ARE NECESSARY FOR US TO PROVIDE ELECTRIC SERVICE TO OUR CUSTOMERS. OUR TESTING OF THESE MISSION-CRITICAL SYSTEMS, WHICH WAS COMPLETED LAST MONTH, HAS REVEALED NO Y2K ISSUES THAT WILL INTERFERE WITH OUR ABILITY TO PROVIDE ELECTRICITY TO OUR CUSTOMERS AS WE ENTER THE NEXT CENTURY. OUR COLLABORATION WITH THE EDISON ELECTRIC INSTITUTE AND THE ELECTRIC POWER RESEARCH INSTITUTE HAS ASSISTED US IN OUR EFFORTS TO COMPLETE OUR Y2K PROJECT. IT FACILITATED THE EXCHANGE OF PRODUCT Y2K READINESS INFORMATION AND TESTING RESULTS, AND CONFIRMED THE ACCURACY OF OUR ASSESSMENT, REMEDIATION, AND TESTING BY REVEALING SIMILAR RESULTS IN OTHER ELECTRIC POWER UTILITIES.

HOWEVER, TO ADDRESS UNFORSEEN EVENTS, EACH DEPARTMENT AND BUSINESS UNIT HAS DEVELOPED CONTINGENCY PLANS WHICH WILL PROVIDE FOR APPROPRIATE WORKAROUNDS FOR EACH IMPORTANT BUSINESS FUNCTION IN THE EVENT OF AN UNPLANNED INTERRUPTION OF, OR OTHER PROBLEM WITH THAT FUNCTION. WE HAVE ALSO IDENTIFIED A NUMBER OF ACTION PLANS WHICH WE WILL IMPLEMENT BEFORE THE END OF THE YEAR TO PRECLUDE OR FORESTALL POTENTIAL PROBLEMS. FOR EXAMPLE, ONE SUCH ACTION WE DO ON A ROUTINE BASIS IS TO STOCKPILE RESERVES OF COAL AT EACH OF OUR FOSSIL-FUEL POWER PLANTS. ANOTHER IS THAT WE WILL HAVE EXTRA GENERATING CAPACITY ON LINE ON NEW YEAR'S EVE. WE DO NOT EXPECT PROBLEMS, BUT WE INTEND TO BE IN A POSITION TO BE READY TO RESPOND TO THEM, SHOULD ANY OCCUR.

LOOKING BACK ON OUR EFFORTS OF THE PAST FEW YEARS, WE FOUND THAT THERE WAS A MUCH LOWER INCIDENCE OF THE Y2K BUG IN OUR SYSTEMS THAN WE ORIGINALLY EXPECTED. THIS ALLOWED US TO KEEP OUR PROJECT COSTS LOWER THAN THEY MIGHT HAVE BEEN HAD WE NOT ALREADY HAD NEWER SYSTEMS IN PLACE WHICH WERE Y2K COMPLIANT AND DID NOT NEED TO BE REPAIRED OR REPLACED. NEVERTHELESS, WE STILL EXPENDED OVER 60,000 MAN-HOURS IN ARRIVING AT THIS POINT OF Y2K READINESS.

EVEN THOUGH WE HAVE NOW ACHIEVED OUR GOAL OF Y2K READINESS, OUR PROJECT WILL CONTINUE THROUGH THE END OF THE YEAR WITH ADDITIONAL TESTING, UPDATES TO OUR CONTINGENCY PLANS, AND IMPLEMENTATION OF OUR CLEAN MANAGEMENT PROCEDURES. WE WILL PARTICIPATE IN THE NATIONWIDE DRILL ON SEPTEMBER 9TH, AND EXPECT THAT THE RESULTS WILL DEMONSTRATE CONCLUSIVELY THAT OUR REMEDIATION EFFORTS HAVE BEEN SUCCESSFUL.

IN SUMMARY, WESTERN RESOURCES IS READY TO FACE THE CHALLENGES OF THE NEW MILLENNIUM. WE EXPECT TO PROVIDE QUALITY SERVICE TO OUR CUSTOMERS IN THE NEXT CENTURY AS WE DO TODAY. FOR MORE INFORMATION ON OUR Y2K PROGRAM, PLEASE CONTACT THE WESTERN RESOURCES YEAR 2000 PROJECT OFFICE, OR VISIT US ON THE WORLDWIDE WEB AT WR.COM.

THIS CONCLUDES MY BRIEFING, THANK YOU FOR YOUR ATTENTION.

Mr. RYUN. Thank you very much. We will go to our next panelist here. Fortune Magazine has described Southwestern Bell as the most admired telecommunications company in the world. Shawn McKenzie is here to give us his testimony. Southwestern Bell is the largest or the biggest local telephone provider in Kansas, it provides service to 1.4 million customers. We are pleased to have you here.

STATEMENT OF SHAWN MCKENZIE, SOUTHWESTERN BELL

Mr. MCKENZIE. Thank you, Congressman Ryun, thank you, Chairman. I appreciate you giving me the opportunity to do this, especially since I'm sure much of what I'm saying and what other panelists are saying today you have heard before. I really appreciate the opportunity to address the constituents that are here today. I'm going to be talking from a set of about 15 slides that are in the packet. I'm holding this up with the back to you so that the folks behind me can see what I'm talking about.

I wish I had more time to talk, not necessarily because I have a lot to say, but because my preacher is here today, Dr. Jim Congdon is over here in the bright shirt. Every Sunday morning he gets 30 minutes of my time and I thought it would just be fair if I get 30 minutes of his time.

[Applause.]

Mr. MCKENZIE. I apologize for any levity with which I address this, but as I mentioned to Matt before we started, we see the light at the end of the tunnel now and we have a little levity that we didn't have just 3 years ago when we started this process.

Dr. Congdon made a comment in his sermon a couple months ago when he was talking about potential Y2K problems that the telephone system may fail on January 1st, 2000 and I was about the third row and under my breath I said "not a chance," apparently it was a little too loud and he noted that I had said that and I became part of the sermon for the following week. What I want to do now is just substantiate what I said that morning and what I repeat now. Southwestern Bell's telephone network in Kansas and in the other States served by SBC communication companies, which includes Pacific Bell, Nevada Bell, Cellular One, Southern New England Telephone and many, many, many wireless companies will be ready January 1st.

There is a potential for problems. The biggest problem we have a potential for is the same one outlined concerning the toilet paper. If everybody on January 1st picks up the phone at the same time, I guarantee you it will not work. I guarantee you that if everyone got up tomorrow morning and picked up the phone at the same time, it will not work. Much like the Nation's highways are not designed for every car to be on them at the same time, nor are the Nation's telephone networks designed for everybody to be on them at the same time.

SBC Communications is a large company, 37 million access line telephone customers are what we serve in seven different States. We have had a lot of resources since 1996 devoted to solving the problems with our systems. We've spent over \$190 million, we are doing 3,000 hours of work a day on this issue. We have rewritten

340 million lines of software already to have this problem taken care of. We are about 98 percent ready to go.

On January 1st our system will be ready, but we are not going forward as if everything will be OK. We are also making our own contingency plans just in case things don't go OK. I think Western Resources will be ready January 1st as Bud just described, but just in case there is some glitch, we have our generators ready to go to provide our own power.

So we suggest to our customers that if they want to be as ready as they can and make sure their phones work that day, that they have a telephone available to them that's not dependent on commercial power, because our system on January 1st will not be dependent on commercial power and you will be able to use your phone even if commercial power fails.

We are going to be ready to move forward. We have groups of employees that are going to be staffed in addition to the normal work hours that day to respond to any problems that may come up that we had not foreseen. So if something doesn't come up that we don't foresee right now, come January 1st everything will be working. And rather than work my way through the rest of these slides, I'll yield time and answer questions later. Thank you.

[The prepared statement of Mr. McKenzie follows:]



**SBC's Year 2000
(Y2K) Project**

Shawn McKenzie

Year 2000 Readiness Disclosure Statement of SBC



SBC Overview

- ◆ SBC is global leader in telecommunications
 - ◆ 36.9M lines and 6.5M wireless customers
 - ◆ Southwestern Bell, Pacific Bell, Nevada Bell, Cellular One, Southern New England Telephone
 - ◆ Telecommunications interests in 11 countries
 - ◆ 129,000 employees
- 



SBC's Year 2000 Commitment

- ◆ **Importance** - The Year 2000 project is one of SBC's top business priorities.
 - ◆ **Goal** - to upgrade our business systems and operations by the millennium deadline without interrupting or degrading the service we provide our customers.
- 



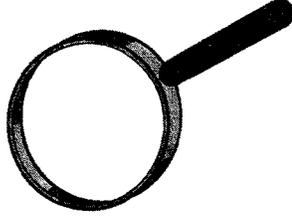
SBC Y2K Resources

- ◆ Spending \$3M per week--\$194M to date
- ◆ More than 3,000 hours per day
- ◆ 56 organizational coordinators designated
- ◆ Monthly meetings & updates to CEO



SBC Project Scope

- ◆ 1,400 vendors who provide more than 15,000 products
- ◆ 1,200 network switches
- ◆ 117,000 personal computers
- ◆ 340 million lines of code
- ◆ 7,000 building facilities



Y2K Readiness Steps

- ◆ **Inventory & Assessment** - find it
- ◆ **Conversion/Fix** - repair it
- ◆ **Testing** - Unit, system, regression, time box, interoperability test
- ◆ **Implementation** - Try it in live environment
- ◆ **Y2K Readiness** - When all steps are completed satisfactorily, Y2K readiness is achieved.



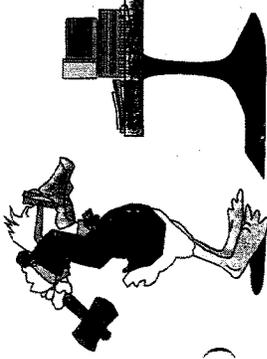
Strategy & Solutions

- ◆ Replace Systems
- ◆ Retire Systems
- ◆ Repair Systems

- Field Expansion (98 becomes 1998)
- Windowing

- 60/40 Windowing - 00-59 = Century 2000
and 60-99 = Century 1900

- ◆ Actual solution based on the applications





The Network

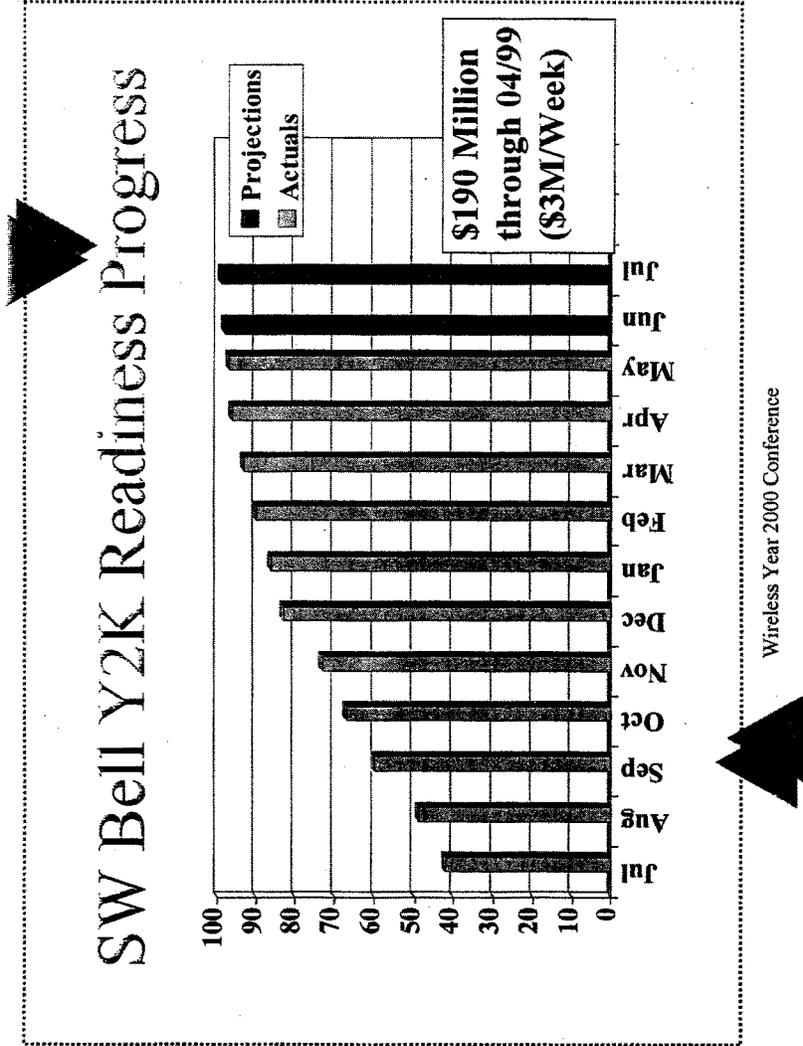
Year 2000 upgrades are tested multiple times

- ◆ Guest tested at the supplier's location
 - ◆ Monitored the supplier's testing
 - ◆ Conducted lab, unit and interoperability testing
 - ◆ Participated in the National Year 2000 Telco Forum interoperability testing
 - ◆ Participated in interoperability testing of local and long distance networks through ATIS (Alliance for Telecommunications Industry Solutions)
- 



911 Service Readiness

- ◆ Network upgrades needed to carry 911 calls are nearly completed.
 - ◆ We're moving our 911 database, called ALISA, to a new platform which is Y2K ready.
 - ◆ Working with local emergency agencies to ensure 911 equipment is updated.
- 



Progress Report (as of May 99)

Major Project Elements	Quantity	Progress
Overall Project		97% Complete
Lines of Code	340 million	100% Fixed 97% Tested
Central Office Switches	1,200	98% Completed
Personal Computers	117,000	94% Ready
Vendor Products	15,000	95% ready
Building Facilities	7,000	99.9% Ready

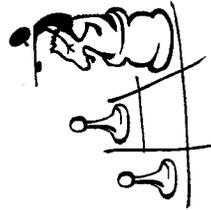


Contingency Planning

- ◆ Contingency Planning is not a NEW concept... we do it every day.
 - ◆ Look at all the HOT-Lines and help desks that are in operation today!!
 - ◆ We are always ready to solve a problem.
 - ◆ We have customer service departments and repair bureaus established because something could happen, and does happen!
- 



Continuity Plans



- ◆ 22 Coordinators Assigned
- ◆ Increased staffing in key customer contact centers
- ◆ Battery/diesel powered generators
- ◆ Y2K Command Center
- ◆ Links across industry via Telco Forum
- ◆ Vendor emergency contact centers and numbers identified





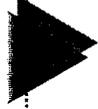
Calling Tips for 1/1/2000

- ◆ Place important phone calls, particularly those overseas, before or after New Year's Day.
 - ◆ Minimize phone and modem use on that day. Heightened traffic volume could overtax the network.
 - ◆ Have at least one phone available that doesn't rely on electric power to operate. Cordless phones require electricity.
- 

The Bottom Line



- ◆ Will calls go through? Yes!
- ◆ Will 911 service work? Yes!
- ◆ Will I be properly billed? Yes!
- ◆ Equipment - Check with manufacturer





Important Web Sites

◆ **SBC**

– www.sbc.com/year2000

◆ **Telco Forum**

– www.telcoyear2000.org

◆ **ATIS**

– www.atis.org



Mr. RYUN. Our next panelist is Anne Rubeck, who is the director of Communications Technology for the Kansas Hospital Association, of which there are 143 hospitals that are part of this organization. And I'm particularly interested in her testimony with regard to readiness for critical areas in rural areas, because I know that I have a great deal of rural people that are very concerned about what's going to be available. We certainly look forward to your testimony.

STATEMENT OF ANNE RUBECK, DIRECTOR, COMMUNICATION TECHNOLOGY, KANSAS HOSPITAL ASSOCIATION

Ms. RUBECK. Thank you, Congressman Ryun. We do appreciate the opportunity to speak with you about hospitals and the Y2K issue.

Hospitals and other health care organizations really face a unique challenge in dealing with year 2000 issues. Not only must their business and financial systems be ready for the date change, but be ready to work with various insurance companies, as well as the Federal Government. But advanced medical devices must also be compliant so as not to jeopardize patient safety. Hospitals recognize the tremendous amount of trust placed in them to safeguard the health and well-being of those for whom they care. Hospitals concern is first and foremost for the patients that they serve.

Kansas hospitals have been working diligently on the Y2K issue for quite some time. The Kansas Hospital Association for whom I work has provided voluminous amounts of information and educational programs to its members regarding identifying and possibly replacing affected equipment, creating and implementing Y2K readiness plans, creating awareness and information materials for use with their communities in the preparation of contingency plans. We have also contracted with the Georgia Hospital Association to provide access for Kansas hospitals to their ongoing Y2K educational series via teleconference. Hospitals are very well aware of this issue and we should make sure that they are.

The KHA has also participated and cooperated with the three surveys that have been conducted by the Docking Institute of Public Affairs which is part of Fort Hays State University. The final report on the second survey was published in December 1998. The third survey is currently in progress. The December 1998 report states that hospitals reported the highest level of preparation in many aspects of delivery of services.

Hospitals are also involved in contingency planning as well as continuing to identify and work with vendors of medical equipment. Some of the biggest challenges that hospitals face is that each entity is unique in and of itself in the kind of systems that they run, and in many cases the kind of equipment that they use. So there is not going to be one solution that every hospital can use. Each hospital has to come up with its own way of dealing with the problem and its own way of being ready.

But just to show that hospitals are on top of the issue, the American Hospital Association has also conducted a survey of the Nation's hospitals which indicates that they are hard at work to ensure patient safety and a smooth transition of business affairs at the end of this year. The survey shows that 90.4 percent of hos-

pitals report that they are predicting compliance of their medical devices or expect no adverse effect. It is very important to note that if a medical device is noncompliant, that does not necessarily mean it will be nonfunctional. Many times the date chips inside a piece of medical equipment will possibly create paperwork type errors as opposed to anything that would have anything to do with patient safety. Obviously this isn't true for 100 percent of medical devices, but noncompliance does not necessarily mean nonfunctionality. And hospitals have prepared for those kind of situations in their contingency planning. The vast majority of hospitals, 94.2 percent, report that their information systems are either currently Y2K compliant or are moving toward total compliance without major difficulties. This is the business end, so they have two major areas that they have to follow.

As everyone knows, I think, the Y2K event is completely unprecedented and therefore presents a tremendous challenge for anyone who has to deal with technological devices. Hospitals are doing everything they can to be as ready for the event as possible, as well as making the detailed contingency plans I mentioned before. We will continue to work unceasingly through January 1st and beyond to ensure that patient care and safety are protected. And that concludes my comments.

[The prepared statement of Ms. Rubeck follows:]

**TESTIMONY OF THE KANSAS HOSPITAL ASSOCIATION FOR THE
"MEETING THE YEAR 2000 CHALLENGE" FORUM**

Wednesday, July 7, 1999

Presented by:

Anne L. Rubeck, Director of Communication Technologies

Hospitals and other health care organizations face a unique challenge in dealing with Year 2000 (Y2K) issues. Not only must their business and financial systems be ready for the date change, but advanced medical devices must also be compliant so as not to jeopardize patient safety. Kansas hospitals have been working diligently on this project for quite some time. The Kansas Hospital Association (KHA) has provided information and educational programs to its members regarding identifying and replacing affected equipment, creating and implementing Y2K readiness plans, and creating awareness and information materials for use with their communities. KHA has also contracted with the Georgia Hospital Association to provide access for Kansas hospitals to Georgia's ongoing Y2K educational series via teleconference.

KHA has also participated and cooperated with the three surveys conducted by the Docking Institute of Public Affairs, which is part of Fort Hays State University. The final report on the second survey was issued in December of 1998. The third survey is in progress to assess the readiness of hospitals, local governments, and school districts for the Y2K event. The December 1998 report states that "hospitals reported the highest level of preparation in many aspects of delivery of services." This was as of March 1998, and work has been steadily progressing in the past year. Hospitals are involved in contingency planning, as well as continuing to identify and work with vendors of medical equipment to ensure readiness for Y2K.

The American Hospital Association also conducted a survey of the nation's hospitals which indicates that hospitals are hard at work to ensure patient safety and a smooth transition of

business affairs at the end of this year. The survey shows that 90.4% of hospitals report that they are predicting compliance of their medical devices, or expect no adverse effect. It is important to note that if a medical device is non-compliant, it does not necessarily mean that it will be non-functional. Many times non-compliance may only affect paper-work type issues. Hospitals have prepared for those situations in their contingency planning. The vast majority of hospitals, 94.2%, report that their information systems are either currently Y2K compliant, or are moving toward total compliance without major difficulty.

The Y2K event is completely unprecedented and therefore presents a tremendous challenge for all who use technological devices. Hospitals are doing everything they can to be as ready for the event as possible, as well as making detailed contingency plans to cover any unexpected effects of the date change. We will continue to work unceasingly through January 1, 2000, and beyond, to ensure that patient care and safety are protected.

Sources:

Year 2000 Readiness of Kansas Public Institutions Survey (March 1998). Docking Institute of Public Affairs. (www.fhsu.edu/docking/center_survey_research/y2k2/y2k2.htm)

Year 2000 Readiness Status Survey Results (March 1999). American Hospital Association. (www.aha.org/y2k/y2k.pdf)

Mr. RYUN. Thank you very much. The next panelist we have been watching what's been going on in banking for some time and I hope I'm saying your name correctly, Ed Splichal. Mr. Splichal is with the Kansas Bankers Association with approximately 400 members throughout the State of Kansas, total assets of \$34 billion. As we have heard before, you have done a lot to get prepared for Y2K and we are looking forward to your testimony.

STATEMENT OF EDWIN SPLICHAL, CHAIRMAN, Y2K TASK FORCE KANSAS BANKERS ASSOCIATION

Mr. SPLICHAL. Thank you Mr. Chairman and Congressman Ryun, I appreciate this opportunity to appear before you to discuss Y2K and its impact on the banking industry here in Kansas. I'm serving currently as the president-elect of the Kansas Bankers Association and am chairman of the Association's Y2K Task Force. The KBA represents 99 percent of the 400 plus banks presently doing business in Kansas. Our banks have been working diligently for many months in preparation for the century date change. Untold hours and millions of dollars have been expended by these banks to make certain that banking operations throughout the State will make a smooth transition into the new year.

One of the major reasons why the preparedness has gone so well has been the leadership role assumed by the various regulatory agencies. I firmly believe the banking industry here in Kansas and throughout the Nation would not be as well prepared if it had not been for the well-planned procedures that the Federal and State regulatory agencies required the banks to complete by June 30th of this year.

By requiring banks to complete each phase of the Y2K preparedness procedures by a time certain, it kept the banks on top of the situation and avoided hurried, last-minute attempts to be ready for business on January 1st, 2000. These procedures included identification of possible problems, correction of problems, testing of all date sensitive procedures, development of business resumption contingency plans, and, finally, verification. Banks are well aware of the serious consequences Y2K noncompliance can have not only on their customers, but also on the future viability of their banks and their communities.

I'm happy to report that as of this date the technical phases have gone well for Kansas banks. During the final months of this year our banks will also be placing a major focus on their customer awareness plans.

It is this phase where the Y2K Task Force of the KBA has been most involved. The Task Force, composed of nine bankers from various regions of the State, has established six main goals to accomplish before the end of the year.

They include: (1) providing materials that Kansas banks could use to in keeping their customers informed about Y2K issues; (2) working with the regulatory agencies to exchange pertinent information on technical, liquidity, and customer awareness issues; (3) meeting with newspaper, radio, and television personnel to discuss Y2K; (4) meeting with public officials to seek their assistance in keeping the public accurately informed about Y2K; (5) sharing pertinent information on Y2K with all member banks in the State

through mailings and articles in the Association magazine; and, finally, (6) implementing a statewide radio and newspaper campaign that emphasizes the Y2K readiness of Kansas banks.

To implement one of the goals the Task Force held a meeting with representatives from the FDIC, OCC, Federal Reserve and the State Banking Department in March. This proved to be a very valuable meeting for the exchange of information on what the regulatory agencies and the banks had done to that point. We plan to meet with the same regulators again in early September.

We have also worked to involve public officials in the Y2K awareness campaign. Representatives of the Federal Reserve and the FDIC plan to appear at a press conference with the Kansas Attorney General, Carla Stovall, here in Topeka tomorrow. At that press conference the Attorney General will discuss the need for Kansas citizens to not be misled by Y2K rumors and their need to be aware of possible scams that may be perpetrated based on those rumors. I would once again emphasize how pleased we have been with the cooperative attitude displayed by the regulatory agencies and public officials in working with us on these issues.

In the articles I have written for our Association magazine I have tried to stress the need for banks in each county to work together in developing their customer awareness plans, organizing community informational meetings, and initiating discussions with the local media. I have also emphasized that banks must also develop a strong customer awareness program so that all customers will understand what the banks have done to make sure all systems will function smoothly as the new year begins. The response that we have had to the customer awareness packet prepared for us by the KBA Task Force would indicate that banks are taking this responsibility very seriously and will continue to do so for the next 6 months.

We have also discussed with the banks the need to have sufficient liquidity at the end of the year in case it's needed. The Federal Reserve has been very helpful in working through these details since Kansas is a large State and many of our community banks are located in areas many miles from urban centers. This is an area of the Y2K preparation process that our Task Force will continue to monitor closely in the coming months.

We appreciate the efforts in Congress to try to bring some common sense to the area of Y2K litigation. We have no objection to legal action against any corporation that has failed to properly prepare for the date change. But there should be limitations that would diminish the possibility for frivolous litigation relating to Y2K problems. Without such legislation there is a very significant risk that litigation may be even more costly than the technical preparedness for Y2K has been.

We are well aware there is no margin for complacency in and bankers in this State plan to continue testing our systems, working with our customers and staying in close contact with our regulators to make sure it will be business as usual when the year 2000 dawns.

[The prepared statement of Mr. Splichal follows:]

TESTIMONY OF

EDWIN SPLICHAL

on behalf of

THE KANSAS BANKERS ASSOCIATION

presented to the

**COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION AND TECHNOLOGY
THE HONORABLE STEVE HORN, CHAIRMAN**

U.S. HOUSE OF REPRESENTATIVES

JULY 7, 1999

Mr. Chairman and Congressman Ryun, I appreciate this opportunity to appear before you to discuss the upcoming century date change, commonly referred to as Y2K, and its impact on the banking industry here in Kansas. I am Ed Splichal, President of the First National Bank of Belleville, Kansas. Our bank has assets of \$50 million and is located in the county seat of Republic County in north central Kansas.

I am also currently serving as the President-elect of the Kansas Bankers Association (KBA) and the chairman of the Association's Y2K Task Force. The KBA represents nearly 99% of the 400+ banks presently doing business in Kansas. Our banks have been working diligently for many months in preparation for the century date change. Untold hours and millions of dollars have been expended by these banks to make certain that banking operations throughout the state will make a smooth transition into the new year.

One of the major reasons why the preparedness has gone so well has been the leadership role assumed by the various regulatory agencies. Bankers are often times critical of what they perceive to be undue regulatory burden or interference. The Y2K situation is a distinct exception to that rule. I firmly believe the banking industry, here in Kansas and throughout the nation, would not be as well prepared if it had not been for the well-planned procedures that the federal and state regulatory agencies required the banks to complete by June 30th of this year.

By requiring banks to complete each phase of the Y2K preparedness procedures by a time certain it kept the banks on top of the situation and avoided hurried last-minute

attempts to be ready for business on January 1, 2000. These procedures included identification of possible problems, correction of those problems, testing of all date sensitive procedures, development of business resumption contingency plans and, finally, verification. Bankers are well aware of the serious consequences Y2K noncompliance can have not only for their customers, but also for the future viability of their banks and their communities. I am happy to report that, as of this date, the technical phases have gone well for Kansas banks. During the final months of this year our banks will also be placing a major focus on their customer awareness plans.

It is this phase where the Y2K Task Force of the KBA has been most involved. The Task Force, composed of nine bankers from various regions of the state, has established six main goals to accomplish before the end of the year. They include:

- (1) providing materials that Kansas banks could use in keeping their customers informed about Y2K issues;
- (2) working with the regulatory agencies to exchange pertinent information on technical, liquidity, and customer awareness issues;
- (3) meeting with newspaper, radio, and television personnel to discuss Y2K;
- (4) meeting with public officials to seek their assistance in keeping the public accurately informed about Y2K;
- (5) sharing pertinent information on Y2K with all member banks in the state through mailings and articles in the Association magazine; and

(6) implementing a statewide radio and newspaper campaign that emphasizes the Y2K readiness of Kansas banks.

To implement one of the goals the Task Force held a meeting with representatives from the FDIC, OCC, Federal Reserve and the State Banking Department in March. This proved to be a very valuable meeting for the exchange of information on what the regulatory agencies and the banks had done to that point. We plan to meet with the same regulators again in early September. In the meantime, we have had a number of telephone conversations on Y2K and have involved an officer of the Federal Reserve in a Y2K panel discussion at one of our major Association seminars.

We have also worked to involve public officials in the Y2K awareness campaign. Representatives of the Federal Reserve and the FDIC plan to appear at a press conference with the Kansas Attorney General, Carla Stovall, here in Topeka tomorrow. At that press conference the Attorney General will discuss the need for Kansas citizens to not be misled by Y2K rumors and their need to be aware of possible scams that may be perpetrated based on those rumors. I would once again emphasize how pleased we have been with the cooperative attitude displayed by the regulatory agencies and public officials in working with us on these issues.

In the articles I have written for our Association magazine I have tried to stress the need for banks in each county to work together in developing their customer awareness plans, organizing community informational meetings, and initiating discussions with the local media. I have also emphasized that banks must also develop a strong customer

awareness program so all customers will understand what the banks have done to make sure all systems will function smoothly as the new year begins. The response that we have had to the "customer awareness packet" prepared for banks by the KBA Task Force would indicate that banks are taking this responsibility very seriously and will continue to do so for the next six months.

We have also discussed with banks the need to have sufficient liquidity at the end of the year in case it is needed. The Federal Reserve has been very helpful in working through these details since Kansas is a large state and many of our community banks are located in areas many miles from an urban center. This is an area of the Y2K preparation process that our Task Force will continue to monitor closely in the coming months.

I would also like to express the support of the members of our Association for the Y2K legislation currently pending before Congress. We have no objection to legal action against any corporation that has failed to properly prepare for the date change, but there should be limitations enacted that would diminish the possibility for frivolous litigation relating to Y2K problems. Without such legislation there is a very significant risk that such litigation may be even more costly than the technical preparedness for Y2K has been.

We are encouraged that certain dates that had been identified as possible dates where computer problems could occur have passed without difficulty. However, we are well aware there is no margin for complacency and the bankers in this state plan to continue testing our systems, working with our customers, and staying in close touch with our

regulators to make sure it will be business as usual when the year 2000 dawns.

Thank you, Mr. Chairman, for holding this hearing here in our capital city and for allowing me this time to present these comments on behalf of the banking industry of Kansas and the Kansas Bankers Association. The bankers of Kansas look forward to working with you and Congressman Ryun and your Congressional colleagues on this and other banking issues. I will be happy to answer any questions you may have at this time.

Mr. RYUN. Our last panelist is Al Lobeck from WIBW, he represents the Kansas Association of Broadcasters which represents 90 percent of all the TV and radio stations in the State, it includes 22 TV stations and 140 radio stations. He also represents Jim Cates, who this morning was gracious enough and throughout the week to make people aware of this time today. I appreciate your support and am looking forward to your comments.

**STATEMENT OF AL LOBECK, NEWS DIRECTOR, WIBW RADIO,
KANSAS BROADCASTERS**

Mr. LOBECK. Thank you very much. We go from the KBA to the KAB.

The Kansas Association of Broadcasters has prepared a handout that's in the packet that you have that goes into quite a bit of detail illustrating not only what Kansas broadcasters, but nationally broadcasters are doing and what the Federal Communications Commission has advised to be done.

As one Kansas Association of Broadcasters board member said, Y2K is like a tornado warning for which we have months to prepare. Like a tornado, Y2K could be very serious, or it might not be serious at all. No one will know until the time is here. As in any disaster, preparation is the key to minimizing the impact of a potential Y2K disaster.

Broadcasters throughout the State and the Nation are working diligently to prepare for any possible problems that might occur. And, for example, the Kansas Association of Broadcasters at their annual convention, which will be in September, are having several panels to discuss fine tuning any plans that are out there.

A bit of background about our particular operation so that you can understand the impact that our stations could have for communication in the community and to show you what we have done to prepare ourselves. WIBW the AM station is the 14th most powerful signal in the United States, it has the 14th largest coverage area. We broadcast farm news in the mornings, regular news and sports and talk programming such as you commented on. Our FM station is Topeka's most listened to radio station, 97 Country, and broadcast news and weather as needed at times.

Our five person news staff also operates the Kansas Information Network which is a news organization that broadcasts via satellite to about 40 stations throughout the State of Kansas. So we have the ability to communicate statewide on a regular basis, and we do.

We also originate the Kansas Agricultural Network which has about 40 stations that also broadcast agricultural news on a daily basis.

We are also a key entry point for the emergency broadcast system which, as you well know, is designed to notify the public here as well as statewide almost instantaneously of any kind of emergency. And we are also the emergency notification station for the Wolf Creek power plant, so if there is a problem there, they call us and we broadcast it.

I want to give you that background so you can understand that we do take the coverage of news and providing news to the public very seriously. As a result, for years we have had the capability to be able to broadcast completely without the benefit of telephone

lines or electricity from the public utilities. We have emergency power generators at both of our transmitter sites for the AM and FM as well as at our studios. So we don't anticipate that there will be any interruption of any kind for our broadcasting and would be ready to do anything that would be necessary to communicate to the general public.

I would point out that the Federal Communications Commission has made a couple of comments that I would like to read from this particular sheet. And according to their assessment, they said the public should continue to have access to critical broadcast news, emergency information, and entertainment services on January 1, 2000. Individual Y2K related disruptions should be isolated and because virtually all listeners and viewers have several free over the air broadcast servers available, service outages that may occur likely will leave affected viewers and listeners with several alternative broadcast stations.

They also point out some hints which I thought were rather interesting and I wanted to mention them here in case someone doesn't get a copy of that. The Federal Communications Commission suggests that you consider having a battery powered radio or television set available with sufficient supply of batteries. If a station suffers technical difficulties, tune to another station in your area for information. If you use your VCR tuner to change stations on your TV set, be sure you know how to bypass the VCR in case it has technical problems.

And, finally, they suggest you have a television antenna handy in case there would be a disruption of cable TV.

[The prepared statement of Mr. Lobeck follows:]

**Y2K Forum Comments
July 7, 1999
Al Lobeck,
General Manager WIBW AM-WIBW FM, Kansas
Radio Networks**

The Kansas Association of Broadcasters has prepared a handout with much information about what the broadcasters in Kansas and the nation are doing in order to prepare for the turning of the year.

As one Kansas Association of Broadcasters Board Member said, "Y2K is like a tornado warning for which we have months to prepare." Like a tornado, Y2K could be very serious...or, it might not be serious at all. No one will know until after the fact. As in any disaster, preparation is the key to minimizing the impact of a potential Y2K disaster.

Broadcasters throughout the State of Kansas and across the nation are working diligently to prepare for any possible problems that might conceivably be caused by the change of the year. For example, let me give you some background about WIBW Radio, the services we provide and the preparation we have completed in order to be ready for the year change. AM 580 WIBW has the fourteenth largest coverage area of all radio stations in the United States. We program news and discussion programming in addition to numerous sports programs to audiences in a six state area.

WIBW-FM, 97 Country, is Topeka's most listened to radio station, featuring country music with news and weather broadcasts as needed.

WIBW Radio's five person news staff also operates the Kansas Information Network, a statewide news network with forty radio stations carrying our news and information. In addition, we are the United Press International hub for the state of Kansas.

We also originate the Kansas Agriculture Network, an agriculture information radio network with about forty radio stations statewide carrying our farm related news and information programs.

Kansas Radio Networks and WIBW are also a key entry point for the state's Emergency Broadcast Service, a system designed to immediately notify as many people in the state as possible of any impending emergencies from war to nuclear power plant failures. WIBW is the emergency notification station for the Wolf Creek nuclear power plant.

I want to give you this background to help you understand that we at WIBW Radio take the duties of providing news and information to the people of Kansas very seriously.

As a result, for years we have had the capability to be able to broadcast without the need for public utility power or telephone lines, should we have to. At our studios and transmitter sites we have diesel powered auxiliary power generators, and our audio signals are sent to the transmitters through microwave systems, which we own and maintain.

If the turning of the year to 2000 should bring any loss of power, or telephone service, which we do not believe it will, our radio and network signals would continue to operate without interruption.

A listener would only have to tune their battery powered radio to AM 580 or 97.3 on the FM dial and all news and information that was deemed necessary to transmit would be available.

Any loss of computer systems within our offices and studios would go unnoticed to the listening public, even though we have been thoroughly checking them for compliance at the changing of the year.

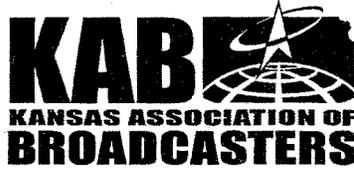
Our parent company, Morris Communications Corporation also takes the changing of the year and its potential for disruption seriously, and as a result in 1998 appointed a senior level management person to oversee a very thorough analysis of systems within the company. That compliance analysis is continuing today, even though most systems company-wide were checked by the end of the year 1998. Morris Communications Corporation provides an internet web site where any interested customers, or vendors can investigate the level of readiness that our entire corporation has in place for this potential problem. That website is: <http://www.morriscomm.com/year2000>

Let me assure you that WIBW AM and FM stations will be on the air as usual on January 1, 2000, just as we have been during a number of other emergencies including June 8, 1966 when Bill Kurtis said those unforgettable words, "God's sake take cover!"

Finally, let me leave you with some "consumer tips" that The Federal Communications Commission has offered for listeners and viewers.

Those suggestions, which are one the KAB handout, include:

- Consider having a battery powered radio or television set available along with sufficient batteries.
- If a station suffers technical difficulties, tune to another station in your area for information.
- If you use your VCR tuner to change stations on your TV set, know how to bypass the VCR in case it has technical problems, and
- Have a television antenna handy for the reception of over-the-air television signals in the event your cable system has difficulties.



1916 SW Sieben Ct, Topeka KS 66611
 TEL (785) 235-1307 * FAX (785) 233-3052 * www.kab.net
 Harriet J Lange, President/Executive Director * harriet@kab.net

Kansas Broadcasters & Y2K

"Y2K is like a tornado warning for which we have months to prepare." - Kansas Association of Broadcasters (KAB) Board Member

Like a tornado, Y2K could be very serious. . . or, it might not be serious at all. No one will know for sure until after the fact. As in any disaster, **preparation is the key** to minimizing the impact of a potential Y2K disaster.

Virtually every Kansan depends on radio and television for news, entertainment and emergency information. Kansas broadcasters take seriously their responsibility to serve the public interest. **Broadcasters** in Kansas and all across the United States **are preparing** for the Year 2000 to insure their listeners and viewers will continue to receive the news, information and entertainment on which they've come to depend.

Radio and television stations are assessing and testing their internal and transmission operations for Y2K readiness. Industry organizations such as KAB and National Association of Broadcasters (NAB) have developed educational programs and initiatives for broadcasters' Y2K readiness.

NAB maintains a Web site - www.nab.org/y2k/ - featuring Y2K information for broadcasters and relevant links; and has presented educational sessions about Y2K at industry meetings.

KAB's Y2K Task Force has explored: 1) how KAB can assist stations through the Y2K readiness process and; 2) how broadcasters may best fulfill their public trust obligations to inform, educate, prepare and communicate with the public about problems which may or may not occur with the rollover to the Year 2000.

The Task Force determined that education is the key in helping stations achieve Y2K readiness. To that end KAB

has planned a Y2K session during KAB's 1999 convention. And KAB provides Y2K information and resources to Kansas broadcasters through its monthly newsletter - *KAB Transmitter*.

In regard to Kansas broadcasters communicating with the public about Y2K - KAB recently undertook a survey of stations, suggesting broadcasters meet with local community emergency preparedness/civil defense and law enforcement officials - to seek information about their concerns with Y2K and to get their input about local broadcast coverage of the Y2K issue. Results of the statewide survey should be available in early August. KAB will distribute to members a summary of the information gathered by broadcasters, from local officials statewide - their concerns and suggestions for covering the issue.

The Federal Communications Commission (FCC) has issued their "Y2K Communications Sector Report" which reports on the status of Y2K remediation in the communications industry. The report covers five industry sectors, including broadcast radio and television. The report is available from the FCC's Web site at : www.fcc.gov/year2000/y2kcsr.html.

According to the FCC's assessment, the public should continue to have access to critical broadcast news, emergency information and entertainment services on January 1, 2000. Individual Y2K-related disruptions should be isolated and "because virtually all listeners and viewers have several free, over-the-air broadcast signals available, service outages that may occur likely will leave affected viewers and listeners with several other alternative broadcast stations to rely on." The report states that "Given the number of TV and radio stations available to most individuals, and the steps that broadcasters are taking, the public is at low risk of being without radio and TV broadcasts as a source of information."

The FCC offers these "Consumer Tips" to listeners and viewers:

- Because radio and TV are important sources of information about news, weather, and emergency situations, consider having a battery operated radio or TV along with sufficient batteries.
- If a station suffers technical difficulties, tune to another station for information - preferably one that broadcasts from your local area.
- If you use your VCR tuner to change stations on your TV set, know how to bypass the VCR in case it has technical problems.
- Have a television antenna handy for the reception of over-the-air television signals in the event your cable system has difficulties.

Mr. RYUN. Thank you for your comments. We are looking forward to some questions. I would like to begin with Mr. Park, if I may.

As I have traveled and as we have all tried to evaluate all of what's going on with regard to readiness for Y2K and the new millennium. There seems to be a single threat that ties all this together and that comes back to the electricity. What assurances can you give us that everything is going to work, that the lights will be on whether we have a holiday January 1st or not? Have you had an entire systems check, so to speak, or how have you proceeded in that regard.

And then kind of a part (b) if I may, it was actually asked during the first panel questions with regard to rail cars, whether you have enough rail cars to get coal to your plant to provide sufficient energy.

Mr. PARK. That's a mouthful. I'll try to address all of those. First of all, as far as assurances that there will be no power outages, of course I can't do that because I can't give you assurance that the next thunderstorm that comes through wouldn't cause a power outage. What I can assure you is that we have tested all of the critical systems necessary for us to provide power. We have simulated moving those systems into the 21st century. We have tested the critical dates many of the people are unaware of. Everybody knows January 1st is the date that we seem to be concerned with, but there are about 14 other dates that we have also tested that we feel could cause problems if a computer chip misbehaves.

Mr. HORN. For the sake of the record, could you maybe identify some of those dates that have already passed, so they will understand that.

Mr. PARK. Of the dates that have passed, January 1st, 1999, because any program that does a year forward look would be looking forward to January 1st, 2000. So we passed January 1st, 1999 without a problem. September 9th, 1998 would also be the same one year look forward for September 9, 1999 which deals with the 9/9/99 situation. July 1st was the beginning of the fiscal year for many organizations, and that is essentially 2000 in the fiscal year. That date is now relatively in the past.

So we have done this testing. The results of our testing shows no issues that would cause power to have any outage that wasn't connected with an ice storm, a thunderstorm, lightning strike, an errant driver hitting a utility pole and knocking wires down. Those kind of outages could still occur, certainly. But we don't expect system-wide outages.

I would like to address this rail service question that was asked of the earlier panel. I don't know where the person who asked the question got his information, but that is 180 degrees opposite from the information we have from the railroad. The assurances we have from them is that they have done similar remediations of their systems, they don't expect interruptions to rail service. Because we cannot control the rail service, however, one of our contingency plans is to stockpile coal. Three of our power plants are coal fired and we have on a normal basis anywhere from 30 to 45 days of coal stockpiled. So even if there is a brief interruption of a few days to

even a few weeks in the rail service, which we don't expect, but if it happens we will be ready for it with coal on hand.

Mr. HORN. I'm just picking up also some of the things from the previous panel. "How can you have unknown ready dates for key programs in Federal Government . . .", and Mr. Willemsen we will have you come back and bring your chair, we always include Mr. Willemsen with the second panel because he brings the national and international perspective to this, ". . . on various dates for key programs? Does this mean anticipated failure of those systems on January 1, 2000?" No, I don't believe they do. I will leave it to Mr. Willemsen.

Mr. WILLEMSSEN. I think some of the dates that were talked about earlier, some of the key dates that Federal agencies are testing for also. In addition, obviously the 2/28, 2/29, 3/1 roll over next year. So many of those dates are also being tested for.

Mr. HORN. A question for Western Resources. "How much have you spent on Y2K to date?"

Mr. PARK. Chairman Horn, we have spent approximately \$6.5 million on our efforts, and our total budget we are estimating is right at \$7 million.

Mr. HORN. For Western Resources also, "What are you doing to combat terrorism via hacking?"

Mr. PARK. We have systems in place to prevent that. I would prefer not discussing them publicly because that would defeat the purpose of some of the protective measures that we have put in place. We do have measures put in place to protect our computer systems, though.

Mr. RYUN. Mr. Chairman, may I interrupt for a question along the lines of what you're talking about?

Mr. HORN. Sure.

Mr. RYUN. Following the line of thinking with Mr. Park on the cost involved. The Federal Government has at this point spent roughly \$9 billion.

Mr. HORN. Right, by the end of this fiscal year.

Mr. RYUN. How many billions of dollars will the private sector have spent?

Mr. HORN. Well, the original estimate of the computer consultants, they were one of our witnesses when we started in on this in April 1996, they said this is a \$600 billion worldwide problem. Since we are half of the computers in the world we are \$300 billion and the rest of the world was \$300 billion. And I asked what do you think the executive branch will cost us, they said it will be about \$30 billion. And within about 5 months I said my instincts looking at this is that it will be around \$10 billion. Right now I'm closer than the experts are. That's simply a hunch. It turned out that way. But they are going to spend about \$9 billion through this fiscal year, and that's 3 months, October, November, and December, prior to January 1st.

So let me ask you on Western Resources, how many plants do you have that you have to worry about? Did you go plant by plant?

Mr. PARK. Yes. We have seven power plants that we went through all of the systems, and each of them were tested.

Mr. HORN. And each of them are now in conformity?

Mr. PARK. Yes.

Mr. HORN. As part of the grading of the Federal Government progress we recently evaluated readiness of 43 essential Federal programs, I'm just reading that inclusion to a number of questions. For some programs like food safety inspection, public housing, we remarked that the program readiness was unknown because we needed more data as to when the computer systems and contingency plans would be ready. Social security has had an A from us in every corner. Social Security also gets an A on the program money going out. They not only started it, but they stuck with it. It took them really 10 or 11 years.

And so the other I mentioned was the weather system, they have got a fancier name now, but it's still the weather system as far as I'm concerned, it means the farmers will find out when a storm is coming in Kansas. And we have obviously a whole series of things such as Medicaid and Medicare that we aren't convinced yet that they have got this thing working right up to January and in compliance before January 1st, I think they will.

Federal Aviation is another one. I've held four hearings on that this last year and the Aviation Committee of the House has held another hearing and so it goes. But we think that will be in good shape based on the current administrator and what she's doing. So I think we can fly. As I have said to many, she and I are both flying that night. I'm going to Los Angeles, she's going to New York. I hope the plays are good and I hope Los Angeles' weather will be good because it will be snowing at Dulles or getting ready for it to snow on January 1st. My wife thinks I'm crazy, but that's OK, that isn't a new thought. I just thought I should give my faith over to the air controllers. And I have told the Administrator not to mess with them before we get on board.

Southwestern Bell, "Just last week there was a software problem that created a temporary 3 hour phone outage. Supposedly this was not Y2K related. And realizing there can be problems at any time, when will the contingency plan be implemented, 1 hour, 2 hours, 3 hours, etc.?" Do you have any estimate on that?

You're absolutely right. When President Kennedy was assassinated everybody picked up the phone in Washington and everything came to a standstill, and that can happen any day as people wonder about their friends and relatives and so forth.

Mr. MCKENZIE. Our network has been improved since the Kennedy assassination so that when everyone does pick up their phone, there are essential lines that are maintained such as pathways between emergency agencies, so it won't be as serious of a problem as it was back then. Contingency plans for us kick in instantly once we realize there is a problem. We have dealt with disasters since the beginning of telecommunications, we know how to deal with disasters.

The problem last week, and I'm glad it came up because it was not Y2K related. A very good technician of ours made an error when making a software upgrade. And he instantly knew he made an error, we ended up rebooting the system to make it work right. The system never completely failed, it just moved slow. We are now working with the provider of that piece of equipment so that we also have a fail safe should another technician sometime in the future make that error. I have been in this business 20 years and I

know one technician for sure in Topeka, KS that will never make it again.

Mr. HORN. Isn't the Internet designed to solve that problem if there was a catastrophe to get around the obstacles? To what degree are there plans to use the Internet? That's why it was started, it was for National Security.

Mr. MCKENZIE. I was told it was to collect taxes.

Mr. HORN. You have just given us an idea. Frankly, they would try to tax the air if they could.

Mr. MCKENZIE. With the exception of very few, most people access the Internet via Southwestern Bell. So the contingency plans we have in place for local telephone voice calling is the same that we have in place for data communication.

Mr. HORN. But I just wondered, you haven't really tried the Internet at this point to see if that would be helpful?

Mr. MCKENZIE. I do not have a specific contingency plan that depends on the Internet to answer your question directly, no.

Mr. HORN. I just wondered if anybody has given thought to that. I probably should ask the Vice-President, apparently he invented it. He would take that in good spirit.

"If hospitals can't get their bills out correctly over the systems they have now, how can they truly assure us, convince us, that things will go smoothly?"

What's the answer to that, Ms. Rubeck?

Ms. RUBECK. Well, as I said before, each hospital has to deal with its own unique situation. Billing errors are not unique to the health care industry, as I myself can attest, and errors do occur. Because humans are entering the data, errors do occur. What I can assure you is that first and foremost the very first line of attack that hospitals took was inventorying every piece of medical equipment in their hospitals and contacting vendors, finding out by serial number about compliance, yes or no. If it's no, it's replaced.

So patient safety has always been the very first and foremost concern and was the first thing addressed. The business issues, the business side of it, is also being addressed. And while I can't say that no errors are ever going to occur, because errors occur now, and, like I said, it's not unique to our industry, I know from working with the information systems people in Kansas hospitals that those systems are also being addressed in detail.

Part of our concern and something that was expressed in the earlier panel is the interfaces that we have to make with various insurance companies, including HCFA for Medicare and Medicaid claims. If HCFA isn't ready, hospitals will be affected very adversely or they could be. We also like to make the assurance that regardless of whether that system is up and whether our hospitals are able to communicate with HCFA. That's a separate issue from patient care. Patients will continue to be cared for regardless of what paper snarls we have to untangle.

Mr. HORN. Last year when we were in Cleveland we had excellent testimony as to what they had examined in terms of emergency room particular equipment. There is a Website nationally where all hospitals can plug in their particular thing, whether it be x ray or whatever, MRI. And I take it you're all using that same

thing to save energy, because if you put the model number, manufacturer, it's all there. If it isn't there, you make a new entry.

Ms. RUBECK. Right. It is a fee based service. We have made that available to our hospitals at an extremely reasonable cost because especially many of our rural hospitals, aren't able to pay thousands and thousands of dollars to find this.

But there is a service on the Internet where you can any time of day, 24 hours a day, 7 days a week you can find a piece of equipment by serial number and get the manufacturer's statement of compliance or noncompliance.

Mr. HORN. The Nuclear Energy Regulatory Commission told us that they were monitoring about 10 percent of the reactors. We questioned that and we still haven't heard from them in writing. We wanted 100 percent. They said orally that, "Well, we have different types of reactors than the French do and thank heavens than the Soviets do." So they are not worried as much as some people are. We don't have that many reactors in this country, rather than only 10 percent of them. So I don't know if any of you can comment on that. Any of you use nuclear reactors to generate power? Mr. Park.

Mr. PARK. Chairman Horn, Western Resources is part owner of Wolf Creek Nuclear Power Plant. We are not the operating agent so it's the Wolf Creek Nuclear Operating Corp. that runs that plant. But we have worked very closely with them. And my counterpart at Wolf Creek, Mr. Bill Eils, and I work together on many occasions, share information, share readiness progress on both of our projects. I know that the NRC is looking at Wolf Creek because they have been there to do an audit, which Wolf Creek passed with flying colors.

I also know that the NRC has issued a generic letter to all nuclear power plants that requires them to be ready and certify their readiness to the NRC to keep their operating license valid. To my knowledge Wolf Creek is fully on track to be able to certify to the NRC that they are ready and expect to keep their operating license.

Mr. HORN. The question that gave me the information for the other part says that utilities themselves you have to remember are self-reporting. And that's of course our situation in looking at each Federal agency, those are all self-reporting. When we send the General Accounting Office they verify that, and the Inspector General's of the various agencies verify that, and they also hire outside consultants to verify that. And the proof in the pudding, of course, will be on January 1, 2000 to see if the information given us in the last quarter or last 2 to 3 years is accurate. If it isn't accurate, they will have a few problems. So this nuclear regulatory review apparently was requested by the Department of Energy.

And in fact the author of the question says, "The real test of Y2K readiness on an industry level is set for September when a full dress rehearsal of December 31, 1999 will be simulated." On another question he says, "If electricity is such a critical measure, why was it decided to report via a self reported survey and what level of oversight is provided directly inside the utilities themselves?" Since we have two utilities here, give us your best shot as to your verification system if it's self reported.

Mr. PARK. It is self reported, but I think that if we were reporting anything grossly different from the majority of other utilities, the other electric utilities in the country, that might raise some eyebrows. The fact that that is not true would lend credence to the fact that what we have found through our remediation, and it is admittedly self reported to NRC, we are finding the same sorts of things that the majority of other utilities are finding.

On a different note, we have had an external agency in to audit our year 2000 efforts, an independent auditor, Arthur Andersen. So it wasn't just our own eyes looking at this.

Mr. HORN. Mr. McKenzie.

Mr. MCKENZIE. I'm not familiar with our self-reporting requirements. I know the process we have followed within the company has been to find the problem, fix the problem, test the problem, physically use whatever has been fixed and then we have pretty much celebrated from that point on. There is no gain for us to pretend we did something we didn't do or to hide something that didn't work right.

Mr. HORN. And the individual that wrote this question on the nuclear power industry points out that the banking industry is on-site regulated by various regulatory agencies that require outside verification of that. And apparently the Department of Energy really has not required that, but they have asked the Nuclear Regulatory Commission to take a look at it. And that is in part an outside agency. And presumably some of the State public utilities commissions have done that.

Have you been in States where that's true, where they want outside verification? Say the Kansas Public Utility or if you go outside of Kansas, you have a number of States, I would think, in your area, don't you?

Mr. PARK. Actually, for electric service we deal with Kansas. And the Kansas Corp. Commission has inquired into our readiness. However, they have accepted the NRC status report, that's North American Electric Reliability, the organization that we have been reporting to on a monthly basis. The Kansas Corp. Commission receives that data and accepts that as our input to them.

Mr. HORN. One general question for all of you. "To what extent are you relying on suppliers and how can you be certain that those organizations and its products are year 2000 compliant?"

Mr. MCKENZIE. I'll go first. We have about 1,400 suppliers that provide us with about 15,000 different products, and we are about 96 percent compliant with them right now. They test, we retest and we use it to prove that it really does what the test says it will do. Again, we are 96 percent complete with that process.

Mr. HORN. Any other comment on that?

Ms. RUBECK. Hospitals deal with many suppliers, whether it's from medication to basic medical suppliers, many kinds of things like that. I know that the American Hospital Association is assisting us in making sure that supply lines will be operational given any number of contingencies. And like many other agencies here, much of hospital planning is very similar to disaster planning. If supply lines are down, laying extra supplies, power generators, that kind of thing is all part of a hospital's preparedness for any kind of disaster.

So I know personally, at least anecdotally, of many hospitals that are contacting every single person they do business with to assess their Y2K compliance. I'm filling out four to five surveys from our own members every week wondering whether the Association is year 2000 compliant. Even though we have no connection with how they provide patient care or how they do any kind of billing. Every single entity that they do business with, they are contacting.

Mr. HORN. Any other comments? Mr. Willemsen, any comments?

Mr. WILLEMSSEN. No.

Mr. HORN. Let me close out the questions with posing an answer, and the question is obvious. Our staff director, Mr. George, happened to buy the Kansas City Star today and the Ann Landers column is worth reading.

It says,

Dear Ann, please warn your readers about a scam I just heard about, elderly folks are particularly vulnerable. Here's the way it works. The con artist calls and says he or she represents the person's bank, he informs the person that the bank is having difficulty meeting requirements to be computer ready for Y2K. The con artist says, "The bank needs you to transfer your money to a bond account structured to protect your money until the bank can be fully Y2K compliant." Then he asks the person to confirm his or her account number and give verbal authorization to transfer the funds. This is a huge scam, banks are almost all Y2K compliant and would never ask a client to confirm a bank account or its number over the telephone. If you give out this information, these con artists could get their hands on your money and you will never see it again.

Please, Ann, tell your readers never to give out this kind of information no matter who asks, and to report such calls to the phone company or the State Attorney General's Office. Thank you for getting the word out. —SP in Missouri.

your neighbor.

Dear Missouri, some scam artists are so smooth and sound so convincing that the average person would suspect nothing. Your admonition never to give an account number or approval for transferring funds over the phone should be carefully heeded. Thank you for the heads up.

So, you know, scum are scum and the scum are the ones that are now working the Y2K problem. So that's a pretty sad state of affairs.

Mr. Chairman, I'm going to thank the staff who participated in this. J. Russell George, the staff director and chief counsel seated down there. Matthew Ryan is the senior policy director for the year 2000 hearing. Patricia Jones in the middle down there is the American Political Science Association. Grant Newman is the clerk for the subcommittee, and we have the three interns in Washington did a lot of work on this, Lauren Lufton, John Phillips and Justin Schlueter.

And from Congressman Jim Ryun's office, they have been very helpful. I must say Kansas has the nicest people I have run into in a long time. Mr. George is from New York, so he's not used to that kind of treatment. But I kid him a lot. We go up there and we can't find the subway, we went into the mayor, he said, we know where it is.

Anyhow, Michele Butler, chief of staff, we thank her very much. And Amy Glaze, the constituent service representative, Ron Cheevers the department of administration here in the Governor's area, and the court reporter Sandy Rider. Thank you for the help.

And, Mr. Chairman, I am yielding back to you, we are going to recess to the Illinois hearing and then the Michigan hearing, so this is a continuing body here like the U.S. Senate.

Mr. RYUN. Mr. Chairman, first of all, let me say thank you very much for coming to Topeka. I know I can speak for all of us that we have been greatly informed, we have learned a lot, there are still questions to ask, but I also know that as a result of your presence and the panelists and the information that they have provided, you have helped accomplish three of the things that I had hoped to do.

I might mention that my coach Bob Timmons is here, he's the one who taught me at a very young age it's always worthwhile to have a goal and purpose. I actually had three purposes for this time today. One was to dispel the rumors, to be able to provide answers. Another was to provide information, to let those that were listening and also the subcommittee to be able to glean information from this part of the country. And also the third part was to ask and answer questions. And it's been very interactive.

I know we did something today, actually the first time, that is passed out little cards so that there would be interaction from you, the constituents having an opportunity to ask questions.

So on behalf of all of Kansas I would like to thank you and the subcommittee for coming and thank all of you for coming today. And let's just say that if there are other questions or other concerns that you have, the office of the Second District does stand open ready and willing to help you.

And I guess it's mine to say that we are now in recess. Thank you very much.

[Whereupon, the subcommittee was recessed subject to the call of the chair.]

**OVERSIGHT OF THE YEAR 2000 TECHNOLOGY
PROBLEM: LESSONS TO BE LEARNED FROM
STATE AND LOCAL EXPERIENCES**

THURSDAY, JULY 8, 1999

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION, AND TECHNOLOGY,
COMMITTEE ON GOVERNMENT REFORM,
Naperville, IL.

The subcommittee met, pursuant to notice, at 9:10 a.m., at Naperville City Hall, Naperville, IL, Hon. Stephen Horn (chairman of the subcommittee) presiding.

Present: Representatives Horn and Biggert.

Staff present: J. Russell George, staff director and chief counsel; Matthew Ryan, senior policy director; Grant Newman, clerk; Patricia Jones, American Political Science Association congressional fellow; Bonnie Heald, director of communications; Kristin Wolgemuth, legislative director; Kathy Lydon, district chief of staff; John Hoffman, district director; and Yadira Rosas, staff assistant.

Mr. HORN. The hearing of the House Subcommittee on Government Management, Information, and Technology will come to order. I would like to welcome and thank your representative, Congresswoman Judy Biggert, who is the vice chairman of this committee in Washington, for being such a gracious host as the subcommittee meets in her hometown here of Naperville. It's a beautiful area, as we told your distinguished mayor, George Pradel, and we are most grateful for all the courtesies that have been given to the subcommittee in making these arrangements with both Congresswoman Biggert's staff and the mayor's and city's staff. It's a lovely area you're in.

The year 2000 computing program affects just about every aspect of Federal, State, and local government operations. Furthermore, it affects private sector organizations and could impact the lives of most individuals.

From Social Security to utilities to local emergency management, the year 2000 computer bug has certainly been a large management and technological challenge for all of us. No single organization, city, State, even country can solve the problem alone.

The problem, of course, dates back to the mid-1960's, when you had computers that would fill a room this size, and right now your personal computer contains more storage than they had in the sixties. So somebody had the bright idea, look, we use a lot of dates,

why are we punching in 1967, why don't we just put in '67; and we moved from a 4-digit year to a 2-digit year.

And they knew at the time that as you got to the year 2000, you'd have some trouble. In other words, January 1, 2000, on the computer, it's 00. The 20 is not there. So the computer thinks it's 1900 and you're back to the days of McKinley. Might not be too bad, but there it is. And they said, Oh, well, we're Americans, we'll solve that. Technology will solve it. Technology has not solved it.

In the estimates we had in our very first hearing on this in April 1996 when we started this in the Congress was that it was a \$600 billion worldwide problem and since America has half the computers, it is a \$300 billion American problem. And I asked at that time, what would it cost to remedy and adapt the Federal Government's computers, and the Gardner Group estimate was \$30 billion. As the year went on and I held more hearings, I thought they were a little high and turns out I'm right and they're wrong, but they get a lot of money as consultants and we don't; that is, the fact that we are spending \$9 billion in Federal money to get their computers adapted in the executive branch between now and the end of the fiscal year on September 30th. It might well get to \$10 billion before we're done. But again, there's no simple solution to this, but hard work of going through the various codes and all of this.

Current estimates show the Federal Government will spend going on, as I say, \$9 to \$10 billion. The President's Office of Management and Budget has identified 43 essential Federal programs such as Social Security, Medicare, the Nation's air traffic control system. Each day these programs provide critical services to millions of Americans. Of these 43 programs, 10 are federally funded State-run programs, including Medicaid, food stamps, unemployment insurance, and child support enforcement. Several of these State-run programs are not scheduled to be ready for the year 2000 until December, leaving little if any time to fix unforeseen problems.

Data exchanges and interdependencies exist at all levels of government and throughout the private sector. A single failure in the chain of information could have severe repercussions. For example, let me briefly illustrate how the U.S. Social Security program uses computers. The Social Security Administration was the first to deal with this problem. No President told them to do it. They just did it and it's the best run agency, without question, in Washington. It was in the sixties, and it is in the nineties. And so they started on adapting their tapes where they had millions of code that had to be checked. They are fully in compliance now with the year 2000 and there shouldn't be any problem.

But they provide the data to the financial management service of the Department of the Treasury that actually cuts the 43 million checks for one part of Social Security and 50 million checks a month in another part. Turned out the financial management service in the Department of Treasury was having real trouble, and over the last few months, by focusing on them, they've pulled out of that and they now cut the checks and electronically deposit it in your bank account. And there are a number of other organizations that are related to that.

So what we're talking about here is a very interactive, inter-related system and many of the Federal agencies, when we said what's your contingency plan, they said our contingency plan is the post office. In other words, if we can't work the code and we can't get the electronic deposits, we'll just mail it to them. Well, that didn't quite work. We had the post office before us and the post office had no contingency plan if they dropped down. So those are the kind of things that you run into.

The bottom line is if any of these entities fail, from the Federal Government to the local bank or the Postal Service, a deserving individual will not receive the payment. Now multiply the situation by millions of people that receive Social Security benefits. There's 43 million in one program, 50 million in the other, and you can appreciate the magnitude of just one aspect of the year 2000 issue.

Fortunately, the Social Security Administration has been working on the problem. As I say, it's in good shape. But the computers to work, we need power, and that's one of the questions we asked everywhere we go.

We are holding six of these field hearings this summer. We started in Topeka yesterday, recessed to Naperville and will recess to Detroit and then we will be back in Washington for the opening of the session again.

So electric power is key here because thousands of plants, if that power due to either a malfunctioning microchip or whatever it is, is not delivered, we will just have people laid off and everything else. But I don't think that's going to happen if we all do what we have to do and we're going to be glad to hear it from the companies that relate to the power, whether it's coal or hydro or wind or solar, nuclear; whatever it is, we're asking that question.

So we want the lights to stay on. From a personal standpoint, I realize when confronted with a personal emergency, I can call assistance 911 and feel confident the phone will be answered appropriately and a competent authority will respond rapidly.

Well, in some areas we're having a problem on that. Sometimes there aren't enough frequencies for law enforcement areas. When we went through emergency planning in Los Angeles County, it would have been 10 years ago at this time, we realized most of the frequencies were in New England and the East. We needed them in the West. We have 81 cities in the county of Los Angeles which has 10 million people and when you need all those police departments and sheriffs' offices to merge, you have real problems in coordination, be it an earthquake, a fire, a flood, whatever.

And Illinois is used to floods and other things, just as we're used to all of them and we don't have tornadoes that the South seems to have. Although we did have a roof torn off in my hometown last year, which had never happened in 100 years. One thing for sure, there are only about 176 days till January 1, 2000. The clock is ticking and, accordingly, the testimony we receive today is very important and we thank the witnesses for coming.

Let me explain some of the procedure. Mrs. Biggert will preside at this session as the vice chairman of the subcommittee. I'm simply here to ask a few questions now and then. She will swear in the witnesses. This is an investigating committee of the House of Representatives so all of the witnesses, when that panel comes up,

if you would stand before we start, raise your right hands, and Mrs. Biggert will administer the oath. Then we will go down the line, based on the agenda, and one by one we will hear the testimony.

And we have your written presentations. They will automatically go in the record when she calls your name, and then we'd like you to spend 5 minutes, not more than that, to give us sort of a summary orally. We don't want you to read your statement. If that happens we'll be here till midnight, and we can't because we've got to be in Detroit. So 5 minutes will be when the gong comes.

Mr. Ryan, the counsel to the subcommittee, among others here, will put up the 1-minute marker so you know you've got 1 minute to go to finish that particular round. The reason we do this is we want a dialog to occur after you make your key points. We want the panel to interact with itself. We want Mrs. Biggert and myself to interact with you, and we are also asking the audience for questions.

We will be passing out cards, and if you have a question particularly of this panel, please, if you know what the subject is, just enter the type of area, and say here's the question; it will be picked up; we will eliminate the duplicates because seven people will have the same question; and put it to them after the panel is done with its presentations and then that will get the audience into it. It will get Mrs. Biggert and I into it, and our own staff has already given us, I don't know how many questions, which we do just as we go through the testimony. So we hope that way we do get all the issues on the table.

And now it is my great pleasure to turn it over to the vice chairman of the subcommittee who's conducting the rest of the hearing. Thank heavens.

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

DAN BURTON, INDIANA
-CHAIRMAN
BENJAMIN A. SMILAN, NEW YORK
CONSTANCE A. MICHELLA, MARYLAND
CHRISTOPHER BRYANT, CONNECTICUT
ANA ROS LEHTINEN, FLORIDA
AL M. MANSHAK, NEW YORK
ERNEST HORN, CALIFORNIA
JOHN L. BICK, ILLINOIS
THOMAS M. DAVIS, II, VIRGINIA
DAVID M. HORTON, INDIANA
JAMES E. SCHURCK, INDIANA
JESSE SCARBOROUGH, FLORIDA
STEVEN D. LATOURETTE, OHIO
MARSHALL MANN, SAMPSON, SOUTH CAROLINA
BOB BARR, GEORGIA
JAN MILLER, FLORIDA
ISA MITCHELL, ARKANSAS
LEE TERRY, NEBRASKA
LUCH BIGNERT, ILLINOIS
GREG WALDEN, OREGON
DOUG BORE, CALIFORNIA
PAUL RYAN, WISCONSIN
JOHN T. BOGUTTELL, CALIFORNIA
HELEN OCHENOWETH, IDAHO

ONE HUNDRED SIXTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6143

MAJORITY (202) 225-4374
MINORITY (202) 225-6551
TTY (202) 225-8852

HENRY A. WAXMANN, CALIFORNIA
-RANKING MEMBER
TOM LANTOS, CALIFORNIA
ROBERT E. WELLS, JR., WEST VIRGINIA
WALTER B. OWENS, NEW YORK
DOUGLAS TOWNSEND, NEW YORK
PAUL E. HANCOCK, PENNSYLVANIA
SARITA A. CORSETT, CALIFORNIA
PATSY T. MINK, HAWAII
CAROLYN B. MALONEY, NEW YORK
FLEMMING HOLMES, MONTANA
-DISTRICT OF COLUMBIA
CHAKA FATTAH, PENNSYLVANIA
ELLIAM E. CLAMMER, MARYLAND
EDDIE E. KUCIUK, OHIO
BOB B. BRADNEY, ILLINOIS
DANNY K. DAVIS, ILLINOIS
JOHN F. TREDNEY, MASSACHUSETTS
JIM TURNER, TEXAS
THOMAS H. ALLEN, IOWA
HAROLD E. FORD, JR., TENNESSEE

BENJAMIN SANDERS, VERMONT,
INDEPENDENT

“Oversight of the Year 2000 Problem: Lessons to Be Learned from State and Local Experiences”
Opening Statement of Chairman Stephen Horn (R-CA)
Subcommittee on Government Management, Information and Technology
July 8, 1999
Naperville, Illinois

This hearing of the House Subcommittee on Government Management, Information, and Technology will come to order. I would like to welcome and thank Congresswoman Judy Biggert, Vice Chair of the Subcommittee, for being such a gracious host as the subcommittee meets in the city of Naperville.

The Year 2000 computing problem affects just about every aspect of Federal, State, and local government operations. Furthermore, it affects private sector organizations and could impact the lives of most individuals. From Social Security to utilities to local emergency management, the Year 2000 computer bug has certainly been a large management and technological challenge for all of us. No single organization, city, State or even country can solve the Year 2000 problem alone.

The problem, of course, dates back to the mid-1960s when programmers, seeking to conserve limited computer storage capacity, began designating the year in two digits rather than four. The year 1967, for example, simply appeared as '67.' Regardless, now we all must deal with it.

More than three years ago, our subcommittee held the first Congressional hearing on the Year 2000 problem. Since that time, we have held almost 30 hearings and issued 8 “report cards” to monitor the status of the Federal Government’s Year 2000 computer solutions.

Current estimates show that the Federal Government will spend nearly 9 billion dollars to fix its computer systems. I have often said that figure will easily reach 10 billion dollars.

Recently, the President’s Office of Management and Budget identified 43 essential Federal programs such as Social Security, Medicare, and the nation’s Air Traffic Control system. Each day, these programs provide critical services to millions of Americans. Of these 43 programs, 10 are Federally funded, State run programs including Medicaid, Food Stamps, Unemployment Insurance, and Child Support Enforcement. Several of these State run programs are not scheduled to be ready for the Year 2000 until December, leaving little, if any, time to fix unforeseen problems.

Data exchanges and interdependencies exist at all levels of government and throughout the private sector. A single failure in the chain of information could have severe repercussions.

For example, let me briefly illustrate how the United States' Social Security program uses computers. The Social Security Administration maintains data containing pertinent Social Security payment information for eligible citizens. When payments are made, the Social Security Administration sends payment data to the Department of the Treasury's Financial Management Service. This Service then "cuts the Federal check," which is then electronically deposited directly into a person's bank account at a local financial institution. Three organizations move and manipulate data to make these payments; each uses its own network of computers. If a payment is mailed to an individual's home, the United States Postal Service then plays a key role.

The bottom line is: If any one of these entities fails, from the Federal Government to the local bank or Postal Service, a deserving individual will not receive the payment. Now multiply this situation by the millions of people that receive Social Security benefits and you can appreciate the magnitude of just one aspect of the Year 2000 issue. Fortunately, the Social Security Administration has been working on this problem for 10 years and is in good shape.

But, for computers to work, we need power. One of the most essential questions concerning the Year 2000 challenge is, "will the lights stay on?" Without electricity, our modern society would be relegated back to the proverbial "Stone Age".

From a personal standpoint, I realize that when confronted with a personal emergency, I can call 911 for assistance and feel confident that the phone will be answered promptly and that a competent authority will respond rapidly. Year 2000 computer problems present other potentially serious threats at local levels, from the potential interruption of a citizen's call for fire or police assistance to delays in a State's ability to request emergency or disaster assistance from the Federal Government.

One thing is for sure, there are only about 176 days until January 1, 2000, and the clock is ticking. Accordingly, the testimony we receive today will help our understanding of the full extent of the Year 2000 computer problem.

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

Mrs. BIGGERT. Thank you, Mr. Chairman. Welcome to the 13th Congressional District of Illinois. I'd like to say, with as much modesty as possible, that you are in one of the most vibrant and exciting parts of the country right here in Naperville, IL. I'd also like to thank Mayor Pradel and the city council and the city of Naperville for allowing us to conduct the hearing here today. It is a wonderful facility and we really appreciate being able to hold the hearing here. Let me thank all of you for coming here today.

The purpose of our hearing today, which we have entitled are you Y2K OK, is to help people understand what they should expect from the millennium bug and how they can prepare. I think our panelists today will help to answer the questions that many of us have.

The media is full of stories about the Y2K bug. I'm told a disaster movie is on the way. One of my younger staff members even informs me that it was the basis of an episode on "Beverly Hills 90210", obviously I can't—that doesn't roll off my tongue, so I haven't watched it. I suspect also that programmers who dropped the two digits from their computer codes had no idea that they were actually developing plot lines for Hollywood. But the Y2K bug is not simply a creation of the media. It is real and it is coming.

A recent poll showed that more than two-thirds of Americans believe that they will experience at least minor problems related to the bug. I think they are right to be at least a little concerned. There should be some disruptions in services. There may be some shortages. I believe that we should prepare for this as we do for a big snowstorm. This is Chicago land and there may be no serious Y2K problems, in which case you'll be ready for the next snowstorm which inevitably will come probably in January or February, right after the turnover.

So what does it mean to prepare commonsense things? I think we should have extra food and water on hand. Make sure your car's gas tank is half full. If you take prescription medicines, to have at least a week's supply. And I think the panelists will come up with a whole list of things and advice.

Since I don't expect America to suddenly become a set for a disaster movie or even anything close, in many ways our Nation is prepared for the Y2K bug but in other ways we are not. As the vice chairman of the subcommittee, I can say that there has been a lot of progress in the Federal Government, largely because of Chairman Horn's efforts to raise awareness of this issue.

But it troubles me, for example, that the Air Traffic Control System is not yet prepared and we have not been given a date when it will be prepared. Does that mean that the planes are going to be falling out of the sky on December 31st? Absolutely not. But I can tell you that I might not be in the air that day. I don't travel during snowstorms if I can avoid them and I don't plan to travel as the clock ticks over. But if progress continues to be made, and I think it will, there may only be some small glitches. But as a former Girl Scout, I am taking to heart the advice of "be prepared."

So I look forward to hearing from the panelists today and what we should be doing and what we don't have to do because the year 2000, January 1st, should be a time of celebration. It is the turn

of the century so we want to make sure that we can enjoy the rollover and not have to worry about these glitches.

I think I'll swear in the panelists and then introduce them. If you could all stand, please.

[Witnesses sworn.]

Mrs. BIGGERT. Today we'll have three panels and then we'll have questions after the first panel. Speaking first today will be Joel Willemsen. He's from the General Accounting Office in Washington. With the way that the weather has been in Washington, I suspect that he's probably glad to be out of Washington for a few days since they've had weather over 100 degrees. And Joel has testified before our committee many times, and his agency is really the watchdog of what the Federal agencies are doing. So we look forward to his testimony.

Mary Reynolds is the chief technological officer for the Office of Governor Ryan in the State of Illinois and is an old friend. I'm happy to see her. I miss being down in Springfield and seeing all my old friends.

Don Carlsen is the information systems director of the city of Naperville and will be talking about the city services that are being affected. And this is his hometown, and I know we'll hear good things from him.

Tom Mefferd is the coordinator for DuPage County Office of Emergency Management, and we're in the heart of DuPage County, so thank you for coming, Tom.

Robert Martin is the manager of water operations for the DuPage Water Commission, and the water commission provides service to 700,000 residents, so he's got a big job to ensure that that water will be ready for us on the rollover.

So thank you all, and we'll begin with Joel Willemsen. Thank you.

[The prepared statement of Hon. Judy Biggert follows:]



Y2K READINESS GUIDE

U.S. Representative Judy Biggert
13th District, Illinois



"The Y2K 'Millenium Bug' isn't just a problem confronting the worlds of government, finance, and information systems. It is a concern we all face, so we must all be prepared with solutions. I hope this guide will provide you with a few."

- Judy Biggert

SUGGESTIONS

There's a host of things you can do to prepare for midnight on December 31, 1999 and beyond. Doing too little could cause problems well into the next millenium. Doing too much could be a problem too. Here's a summary of some of the sensible suggestions from experts...

...FOR GENERAL PREPAREDNESS

- ✓ Have at least a half tank of gas in your automobile.
- ✓ Keep a week's supply of your prescription medicine available.
- ✓ Be prepared with a battery-operated radio and several flashlights, should electrical service be momentarily lost.
- ✓ Go grocery shopping in advance.

...FOR FINDING AND SOLVING Y2K-SPECIFIC PROBLEMS

- ✓ Make a list of your household products with a calendar function. This list should include personal computers, PC software, fax machines, home security systems, Global Positioning System units, and any other computer-controlled devices. Visit the manufacturer's web site or contact the manufacturer by phone or mail to find out compliance status.
- ✓ If you live in an apartment or condominium building, make sure that the central heating and cooling systems, elevators, fire alarms, and access control systems have been checked for Y2K compliance.
- ✓ If a family member's well-being relies on an electronic device such as a dialysis machine or baby monitor, you may want to consider purchasing a small generator should electrical service be momentarily lost.
- ✓ Keep paper records of any financial transactions that you make at least a year in advance of the millenium, including bank deposits, mortgage payments, and loan payments.
- ✓ Keep copies of insurance policies and records of the payments you make.

ADDITIONAL RESOURCES

One of the best sources for information on Y2K and how it relates to you is the Internet. Using the World Wide Web, you can visit a wide array of informational Web sites, download diagnostic patches to make your PC software Y2K compliant, or even voice your opinion in one of countless discussion groups.

A quick search on Yahoo or Lycos will give you a list of thousands of Y2K-related sites. Some are useful, some are not. Here's a quick run-down of some of the more comprehensive sites. If you don't have Web access, you can probably get connected at your local library.

Happy browsing.

TESTING TOOLS AND SOFTWARE PATCH SITES

Lycos Links to testing and patch software, Y2K products, and Y2K consultants

<http://currents.lycos.com/testfix.htm>

This is one of the best places to go to deal with Y2K problems facing a personal computer. From here, you can download Y2K related software like testing devices and patches.

GENERAL SITES

Ed Paulson's Site (Author, Year 2000 Crisis Survival)

<http://www.edpaulson.com/year2000.htm>

This site provides links to general Y2K sites, government sites, and industry sites. Also, you can find links to the sites of consumer product manufacturers to check if your household appliances are Y2K compliant.

Year 2000 Information Center

<http://www.year2000.com/>

This site provides links to Y2K press clippings, Y2K legal issues, Y2K jobs, and an inventory of technology vendors and their respective Y2K strategies and products. An extensive site to say the least.

Y2K Today

<http://www.y2ktoday.com>

This site contains general Y2K solutions, scenarios, and contingency plans. Also, it provides detailed information on specific industries and links to countless articles on Y2K. A huge site. Luckily, it has a search engine to steer the user in the right direction.

GOVERNMENT SITES

U.S. Federal Government Gateway for Year 2000 Information Directories

<http://www.itpolicy.gsa.gov/mks/yr2000/y2khome.htm>

This site provides no specific information on Y2K, but contains important U.S. government and international links.

President's Council on Y2K Conversion

<http://www.y2k.gov>

This site contains information on the Federal government's efforts to prepare its computer systems, links to information on Y2K compliance for critical sectors of the economy, and other general Y2K resources.



PHONE NUMBERS



Federal Year 2000 Hot Line
1-888-USA-4-Y2K

Small Business Administration
1-800-U-ASK-SBA

STATEMENTS OF JOEL C. WILLEMSSEN, DIRECTOR, CIVIL AGENCIES INFORMATION SYSTEMS, GENERAL ACCOUNTING OFFICE; MARY REYNOLDS, CHIEF TECHNOLOGY OFFICER, ILLINOIS GOVERNOR'S OFFICE; DON CARLSEN, DIRECTOR OF INFORMATION SYSTEMS, DEPARTMENT FOR THE CITY OF NAPERVILLE; TOM MEFFERD, COORDINATOR, DuPAGE COUNTY OFFICE OF EMERGENCY MANAGEMENT; AND ROBERT MARTIN, MANAGER OF WATER OPERATIONS, DuPAGE WATER COMMISSION

Mr. WILLEMSSEN. Thank you, Vice Chair Biggert, Chairman Horn. Thank you for inviting GAO to testify today.

As requested, I'll briefly summarize our statement on the Y2K readiness of the Federal Government, State and local governments and key economic sectors.

Regarding the Federal Government, the most recent reports indicate continued progress in fixing, testing, and implementing mission-critical systems. Nevertheless, numerous critical systems must still be made compliant and must undergo independent verification and validation. Our own reviews of selected agencies have shown uneven progress and remaining risks in addressing Y2K and therefore point to the importance of business continuity and contingency planning.

If we look beyond individual systems and individual agencies, the Federal Government's future actions will need to be increasingly focused on making sure that its highest priority programs are compliant. In line with this, the Office of Management and Budget has identified 43 high-impact programs such as Medicare and Social Security and, as you know, Mr. Chairman, we're currently reviewing those programs for you to determine the executive branch's progress. But what I can tell you at this point, it is very clear that much additional work is needed to make all these programs compliant by the turn of the century.

Available information on the Y2K readiness of State and local governments also indicates that, overall, much work remains. For example, according to recent information on States reported to the National Association of State Information Resource Executives, about 18 States had completed implementing less than 75 percent of their mission-critical systems.

State audit organizations have also identified significant Y2K concerns in areas such as testing, embedded systems, and contingency planning. Recent reports have also highlighted Y2K issues at the local government level. For example, March 1999, the National League of Cities' poll of over 400 representatives found that almost 70 stated that they would finish 75 percent or less of their systems by January 1, 2000.

Another area of risk is represented by Federal Human Services programs administered by States; programs such as Medicaid, food stamps, unemployment insurance and child support enforcement. Of the 43 high-impact priority areas I mentioned earlier, 10 of these are State-administered Federal programs.

OMB reported data on the system supporting these programs shows that numerous States aren't planning to be ready until close to the end of the year. Specifically, a large number of State systems

are not due to be compliant until the last quarter of 1999. Further, this is based on data that has not yet been independently verified.

Beyond the risks faced by our governments, Y2K also poses a serious challenge to the public infrastructure and key economic sectors in other countries. We've made a number of recommendations to John Koskinen and the chair of the President's Y2K Conversion Council, and the council has made strides in obtaining needed readiness information in key sectors. Again, nevertheless, there's a great deal of work remaining in the less than 6 months we have until the turn of the century.

Accordingly, there still needs to be a great deal of emphasis on those areas to make sure that they're ready in time.

That concludes the summary of my statement and after the panel is done, I would be pleased to address any questions you may have. Thanks again.

[The prepared statement of Mr. Willemsen follows:]

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Government Management,
Information and Technology, Committee on Government
Reform, House of Representatives

For Release on Delivery
Expected at
9 a.m. CDT
Thursday,
July 8, 1999

YEAR 2000 COMPUTING CHALLENGE

Readiness Improving Yet Avoiding Disruption of Critical Services Will Require Additional Work

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



Mr. Chairman and Members of the Subcommittee:

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 a high-risk area for the federal government.² Since that time, we have issued over 120 reports and testimony statements detailing specific findings and numerous 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 challenges that remain in correcting its systems; identify state and local government Year 2000 issues; and provide an overview of available information on the readiness of key public infrastructure and economic sectors.

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

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

³A list of these publications is included as an attachment to this statement. These publications can be obtained through GAO's World Wide Web page at www.gao.gov/y2kr.htm.

⁴Year 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 RISK OF
YEAR 2000 DISRUPTIONS

The public faces the 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
- 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 signed an executive order that established the President's Council on Year 2000 Conversion, chaired 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.

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

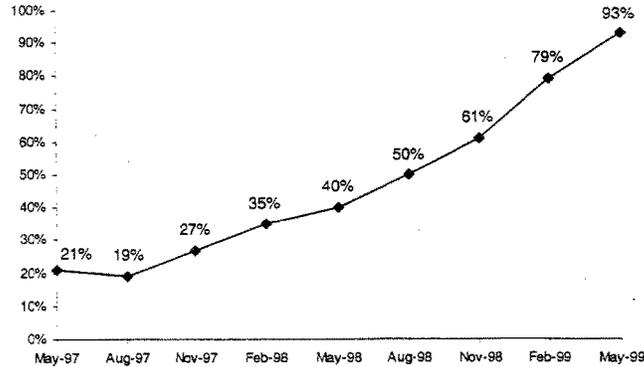
⁶Defense Computers: Year 2000 Computer Problems Threaten DOD Operations (GAO/AIMD-98-72, April 30, 1998).

IMPROVEMENTS MADE BUT
MUCH WORK REMAINS

Addressing the Year 2000 problem is 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 costs and business continuity and contingency plans.

The federal government's most recent reports show improvement in addressing the Year 2000 problem. While much work remains, the federal government has significantly increased its percentage of mission-critical systems that are reported to be Year 2000 compliant, as chart 1 illustrates. In particular, while the federal government did not meet its goal of having all mission-critical systems compliant by March 1999, as of mid-May 1999, 93 percent of these systems were reported compliant.

Chart 1: Mission-Critical Systems Reported Year 2000 Compliant, May 1997-May 1999

Source: May 1997 – May 1999 data are from the OMB quarterly reports.

While this reported progress is notable, OMB reported that 10 agencies have mission-critical systems that were not yet compliant.⁷ In addition, as we testified in April, some of the systems that were not yet compliant support vital government functions.⁸ For example, some of the systems that were not compliant were among the 26 mission-critical systems that the Federal Aviation Administration (FAA) has identified as posing the greatest risk to the National Airspace System—the network of equipment, facilities, and information that supports U.S. aviation operations.

Additionally, not all systems have undergone an independent verification and validation process. For example, in April 1999 the Department of Commerce awarded a contract for independent verification and validation reviews of approximately 40 mission-critical systems that support that Department's most critical business processes. These reviews are to continue through the summer of 1999. In some cases, independent verification and

⁷The 10 agencies were the Departments of Agriculture, Commerce, Defense, Energy, Health and Human Services, Justice, Transportation, Treasury; the National Aeronautics and Space Administration; and the U.S. Agency for International Development.

⁸Year 2000 Computing Challenge: Federal Government Making Progress But Critical Issues Must Still Be Addressed to Minimize Disruptions (GAO/T-AIMD-99-144, April 14, 1999).

validation of compliant systems have found serious problems. For example, as we testified this past February,⁹ none of 54 external mission-critical systems of the Health Care Financing Administration (HCFA) reported by the Department of Health and Human Services (HHS) as compliant as of December 31, 1998, was Year 2000 ready, based on serious qualifications identified by the independent verification and validation contractor.

Reviews Show Uneven Federal Agency Progress

While the overall 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. For example:

- In March we testified that FAA had made tremendous progress over the prior year.¹⁰ However, much remained to be done to complete validating and implementing FAA's mission-critical systems. Specifically, the challenges that FAA faced included (1) ensuring that systems validation efforts were adequate, (2) implementing multiple systems at numerous facilities, (3) completing data exchange efforts, and (4) completing end-to-end testing. Because of the risks associated with FAA's Year 2000 program, we have advocated that the agency develop business continuity and contingency plans.¹¹ FAA agreed and has activities underway, which we are currently reviewing.
- In April 1999, we testified¹² that HCFA had been responsive to prior recommendations.¹³ For example, HCFA had (1) more effectively managed its electronic data exchanges, (2) continued to define its testing procedures, (3) begun to use several Year 2000 analysis tools to measure testing thoroughness, and (4) demonstrated progress in its business continuity and contingency planning. Nevertheless, HCFA still faced many risks and challenges. For example, although reported compliant, HCFA's mission-critical systems were due to undergo a significant amount of change, which would require a complete retest to ensure that they were not contaminated by the changes and that they were still compliant.

⁹Year 2000 Computing Crisis: Readiness Status of the Department of Health and Human Services (GAO/T-AIMD-99-92, February 26, 1999).

¹⁰Year 2000 Computing Crisis: FAA Is Making Progress But Important Challenges Remain (GAO/T-AIMD/RCED-99-118, March 15, 1999).

¹¹FAA Computer Systems: Limited Progress on Year 2000 Issue Increases Risk Dramatically (GAO/AIMD-98-45, January 30, 1998); GAO/T-AIMD-98-251, August 6, 1998; and GAO/T-AIMD/RCED-99-118, March 15, 1999.

¹²Year 2000 Computing Crisis: Readiness of Medicare and the Health Care Sector (GAO/T-AIMD-99-160, April 27, 1999).

¹³Medicare Computer Systems: Year 2000 Challenges Put Benefits and Services in Jeopardy (GAO/AIMD-98-284, September 28, 1998).

Another risk that HCFA faced was that its thousands of data exchanges were not yet compliant. We concluded that given the considerable amount of work that HCFA faces, it is crucial that development and testing of its business continuity and contingency plans move forward rapidly to avoid the interruption of Medicare claims processing next year.

- Our work has shown that the Department of Defense and the military services face significant problems.¹⁴ In March we testified that, despite considerable progress made in the preceding 3 months, Defense was still well behind schedule.¹⁵ We found that DOD faced two significant challenges: (1) completing remediation and testing of its mission-critical systems and (2) having a reasonable level of assurance that key processes will continue to work on a day-to-day basis and key operational missions necessary for national defense can be successfully accomplished. We concluded that such assurance could only be provided if Defense took steps to improve its visibility over the status of key business processes.

End-To-End Testing Must Be Completed

While it is important to achieve compliance for individual mission-critical systems, realizing such compliance alone does not ensure that business functions will continue to operate through the change of century—the ultimate goal of Year 2000 efforts. The purpose of end-to-end testing is to verify that a defined set of interrelated systems, which collectively support an organizational core business area or function, 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—are 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.)¹⁶

In January we testified that 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 the tests.¹⁷ On March 31,

¹⁴Defense 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).

¹⁵Year 2000 Computing Crisis: Defense Has Made Progress, But Additional Management Controls Are Needed (GAO/T-AIMD-99-101, March 2, 1999).

¹⁶GAO/AIMD-10.1.21, November 1998.

¹⁷Year 2000 Computing Crisis: Readiness Improving, But Much Work Remains to Avoid Major Disruptions (GAO/T-AIMD-99-50, January 20, 1999).

OMB and the Chair of the President's Council on Year 2000 Conversion announced that one of the key priorities that federal agencies will be pursuing during the rest of 1999 will be cooperative end-to-end testing to demonstrate the Year 2000 readiness of federal programs with states and other partners.

Agencies have also acted to address end-to-end testing. For example, our March FAA testimony¹⁸ found that the agency had addressed our prior concerns about the lack of detail in its draft end-to-end test program plan and had developed a detailed end-to-end testing strategy and plans.¹⁹ At the Department of Defense, last month we reported²⁰ that the department had underway or planned hundreds of related Year 2000 end-to-end test and evaluation activities and that, thus far, it was taking steps to ensure that these related end-to-end tests were effectively coordinated. However, we concluded that Defense was far from successfully finishing its various Year 2000 end-to-end test activities and that it must complete efforts to establish end-to-end management controls, such as establishing an independent quality assurance program.

Business Continuity and Contingency Plans Are Needed

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, in April 1998 we recommended that the Council require agencies to develop contingency plans for all critical core business processes.²¹

OMB has clarified its contingency plan instructions and, along with the Chief Information Officers Council, has adopted our business continuity and contingency planning guide.²² In particular, on January 26, 1999, OMB called on federal agencies to identify and report on the high-level core business functions that are to be addressed in their business continuity and contingency plans, as well as to provide key milestones for development and testing of such plans in their February 1999 quarterly reports. In addition, on May 13 OMB required agencies to submit high-level versions of these plans by June 15. According to an OMB official, OMB has received almost all of the agency

¹⁸GAO/T-AIMD/RCED-99-118, March 15, 1999.

¹⁹GAO/T-AIMD-98-251, August 6, 1998.

²⁰Defense Computers: Management Controls Are Critical To Effective Year 2000 Testing (GAO/AIMD-99-172, June 30, 1999).

²¹Year 2000 Computing Crisis: Potential for Widespread Disruption Calls for Strong Leadership and Partnerships (GAO/AIMD-98-85, April 30, 1998).

²²GAO/AIMD-10.1.19, August 1998.

plans. This official stated that OMB planned to review the plans, discuss them with the agencies, determine whether there were any common themes, and report on the plans' status in its next quarterly report.

To provide assurance that agencies' business continuity and contingency plans will work if needed, on January 20 we suggested that 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.²³ Our review of the 24 major departments and agencies' May 1999 quarterly reports found 14 cases in which agencies did not identify test dates for their business continuity and contingency plans or reported test dates subsequent to September 30, 1999.

On March 31, OMB and the Chair of the President's Council announced that completing and testing business continuity and contingency plans as insurance against disruptions to federal service delivery and operations from Year 2000-related failures will be one of the key priorities that federal agencies will be pursuing through the rest of 1999. Accordingly, OMB should implement our suggestion and establish a target date for the validation of these business continuity and contingency plans.

Recent OMB Action Could Help Ensure
Business Continuity of High-Impact Programs

While individual agencies have been identifying and remediating mission-critical systems, the government's future actions need to be focused on its high-priority programs and ensuring the continuity of these programs, including the continuity of federal programs that are administered by states. Accordingly, governmentwide priorities need to be based on such criteria as the potential for adverse health and safety effects, adverse financial effects on American citizens, detrimental effects on national security, and adverse economic consequences. In April 1998 we recommended that the President's Council on Year 2000 Conversion establish governmentwide priorities and ensure that agencies set agencywide priorities.²⁴

On March 26, OMB implemented our recommendation by issuing a memorandum to federal agencies designating lead agencies for the government's 42 high-impact programs (e.g., food stamps, Medicare, and federal electric power generation and delivery). (OMB later added a 43rd high-impact program.) Appendix I lists these programs and their lead agencies. For each program, the lead agency was charged with identifying to OMB the partners integral to program delivery; taking a leadership role in convening those partners; assuring that each partner has an adequate Year 2000 plan and, if not, helping each partner without one; and developing a plan to ensure that the program will operate effectively. According to OMB, such a plan might include testing data exchanges across partners, developing complementary business continuity and contingency plans, sharing key information on readiness with other partners and the public, and taking other steps

²³GAO/T-AIMD-99-50, January 20, 1999.

²⁴GAO/AIMD-98-85, April 30, 1998.

necessary to ensure that the program will work. OMB directed the lead agencies to provide a schedule and milestones of key activities in the plan by April 15. OMB also asked agencies to provide monthly progress reports. As you know, we are currently reviewing agencies' progress in ensuring the readiness of their high-impact programs for this subcommittee.

STATE AND LOCAL GOVERNMENTS
FACE SIGNIFICANT YEAR 2000 RISKS

Just as the federal government faces significant Year 2000 risks, so too do state and local governments. If the Year 2000 problem is not properly addressed, for example, (1) food stamps and other types of payments may not be made or could be made for incorrect amounts; (2) date-dependent signal timing patterns could be incorrectly implemented at highway intersections, with safety severely compromised; and (3) prisoner release or parole eligibility determinations may be adversely affected. Nevertheless, available information on the Year 2000 readiness of state and local governments indicates that much work remains.

According to information on state Year 2000 activities reported to the National Association of State Information Resource Executives as of June 17, 1999,²⁵ states²⁶ reported having thousands of mission-critical systems.²⁷ With respect to completing the implementation phase for these systems,

- 5 states²⁸ reported that they had completed between 25 and 49 percent,
- 13 states²⁹ reported completing between 50 and 74 percent, and

²⁵Individual states submit periodic updates to the National Association of State Information Resource Executives. For the June 17 report, over half of the states submitted their data in May and June 1999. The oldest data were provided on March 4 and the most recent data on June 16. All but three states responded to the survey.

²⁶In the context of the National Association of State Information Resource Executives survey, the term "states" includes the District of Columbia, Guam, and Puerto Rico.

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

²⁸Three states reported on their mission-critical systems, one state reported on its processes, and one reported on its functions.

²⁹Eleven states reported on their mission-critical systems, one reported on all systems, and one reported on projects.

- 30 states³⁰ reported completing 75 percent or more.³¹

All of the states responding to the National Association of State Information Resource Executives survey reported that they were actively engaged in internal and external contingency planning and that they had established target dates for the completion of these plans: 14 (28 percent) reported the deadline as October 1999 or later.

State audit organizations have also identified significant Year 2000 concerns. In January, the National State Auditors Association reported on the results of its mid-1998 survey of Year 2000 compliance among states.³² This report stated that, for the 12 state audit organizations that provided Year 2000-related reports, concerns had been raised in areas such as planning, testing, embedded systems, business continuity and contingency planning, and the adequacy of resources to address the problem.

We identified additional products by 15 state-level audit organizations and Guam that discussed the Year 2000 problem and that had been issued since October 1, 1998. Several of these state-level audit organizations noted that progress had been made. However, the audit organizations also expressed concerns that were consistent with those reported by the National State Auditors Association. For example:

- In December 1998 the Vermont State Auditor reported³³ that the state Chief Information Officer did not have a comprehensive control list of the state's information technology systems. Accordingly, the audit office stated that, even if all mission-critical state systems were checked, these systems could be endangered by information technology components that had not been checked or by linkages with the state's external electronic partners.
- In April, New York's Division of Management Audit and State Financial Services reported that state agencies did not adequately control the critical process of testing remediated systems.³⁴ Further, most agencies were in the early stages of addressing potential problems related to data exchanges and embedded systems and none had completed substantive work on contingency planning. The New York audit office

³⁰Twenty-five states reported on their mission-critical systems, two states reported on their applications, one reported on its "priority business activities," one reported on its "critical compliance units," and one reported on all systems.

³¹Of the states that responded to the survey, two did not respond to this question.

³²Year 2000: State Compliance Efforts (National State Auditors Association, January 1999).

³³Vermont State Auditor's Report on State Government's Year 2000 Preparedness (Y2K Compliance) for the Period Ending November 1, 1998 (Office of the State Auditor, December 31, 1998).

³⁴New York's Preparation for the Year 2000: A Second Look (Office of the State Comptroller, Division of Management Audit and State Financial Services, Report 98-S-21, April 5, 1999).

subsequently issued 7 reports on 13 of the state's mission-critical and high-priority systems that included concerns about contingency planning and testing.

- In February, the California State Auditor reported³⁵ that key agencies responsible for emergency services, corrections, and water resources, among other areas, had not fully addressed embedded technology-related threats. Regarding emergency services, the California report stated that if remediation of the embedded technology in its networks were not completed, the Office of Emergency Services might have to rely on cumbersome manual processes, significantly increasing response time to disasters.
- In March, Oregon's Audits Division reported³⁶ that 11 of the 12 state agencies reviewed did not have business continuity plans addressing potential Year 2000 problems for their core business functions.
- In March, North Carolina's State Auditor reported³⁷ that resource restrictions had limited the state's Year 2000 Project Office's ability to verify data reported by state agencies.

In the case of Illinois, on June 30, 1999, the Office of the Auditor General reported³⁸ that the state's Department of Central Management Services had taken the lead to increase agency awareness of the need to ensure that computer systems are Year 2000 compliant. For example,

- monthly meetings were held with agency representatives,
- a central repository of information was developed to share information on, among other items, available tools, and
- beginning this past April, state agencies were required to submit monthly status reports to the Governor.

The Office of the Auditor General urged the Department of Central Management Services to continue to work with the governor's office and to coordinate the state's

³⁵Year 2000 Computer Problem: The State's Agencies Are Progressing Toward Compliance but Key Steps Remain Incomplete (California State Auditor, February 18, 1999).

³⁶Department of Administrative Services Year 2000 Statewide Project Office Review (Secretary of State, Audits Division, State of Oregon Report No. 99-05, March 16, 1999).

³⁷Department of Commerce, Information Technology Services Year 2000 Project Office (Office of the State Auditor, State of North Carolina, March 18, 1999).

³⁸Department of Central Management Services Bureau of Communications and Services: Third Party Review For The Year Ending June 30, 1999 (Office of the Auditor General, State of Illinois, June 30, 1999).

efforts in addressing and reporting on the Year 2000 issue. Further, the audit office stated that the department should continually assess its progress in completing its conversion efforts and develop contingency plans for any systems or applications that may not be Year 2000 ready.

It is also critical that local government systems be ready for the change of century since critical functions involving, for example, public safety and traffic management, are performed at the local level. Recent reports on local governments have highlighted Year 2000 concerns. For example:

- On June 23, the National Association of Counties announced the results of its April survey of 500 randomly selected counties. This survey found that (1) 74 percent of respondents had a countywide plan to address Year 2000 issues, (2) 51 percent had completed system assessments, and (3) 27 percent had completed system testing. In addition, 190 counties had prepared contingency plans and 289 had not. Further, of the 114 counties reporting that they planned to develop Year 2000 contingency plans, 22 planned to develop the plan in April-June, 64 in July-September, 18 in October-December, and 10 did not yet know.
- The National League of Cities conducted a poll during its annual conference in March 1999 that included over 400 responses. The poll found that (1) 340 respondents stated that over 75 percent of their cities' critical systems would be Year 2000 compliant by January 1, 2000, (2) 35 stated that 51-75 percent would be compliant, (3) 16 stated that 25-50 percent would be compliant, and (4) 16 stated that less than 25 percent would be compliant. Moreover, 34 percent of respondents reported that they had contingency plans, 46 percent stated that they were in the process of developing plans, 12 percent stated that plans would be developed, and 8 percent said they did not intend to develop contingency plans.
- In January 1999, the United States Conference of Mayors reported on the results of its survey of 220 cities. It found that (1) 97 percent had a citywide plan to address Year 2000 issues, (2) 22 percent had repaired or replaced less than half of their systems, and (3) 45 percent had completed less than half of their testing.

Of critical importance to the nation are services essential to the safety and well-being of individuals across the country, namely 9-1-1 systems and law enforcement. For the most part, responsibility for ensuring continuity of service for 9-1-1 calls and law enforcement resides with thousands of state and local jurisdictions. On April 29 we testified that not enough was known about the status of either 9-1-1 systems or of state and local law enforcement activities to conclude about either's ability during the transition to the year 2000 to meet the public safety and well-being needs of local communities across the nation.³⁹ While the federal government planned additional actions to determine the status of these areas, we stated that the President's Council on Year 2000 Conversion should

³⁹Year 2000 Computing Challenge: Status of Emergency and State and Local Law Enforcement Systems Is Still Unknown (GAO/T-AIMD-99-163, April 29, 1999).

use such information to identify specific risks and develop appropriate strategies and contingency plans to respond to those risks.

Recognizing the seriousness of the Year 2000 risks facing state and local governments, the President's Council has developed initiatives to address the readiness of state and local governments. For example:

- The Council established working groups on state and local governments and tribal governments.
- Council officials participate in monthly multistate conference calls.
- In July 1998 and March 1999, the Council, in partnership with the National Governors' Association, convened Year 2000 summits with state and U.S. territory Year 2000 coordinators.
- On May 24, the Council announced a nationwide campaign to promote "Y2K Community Conversations" to support and encourage efforts of government officials, business leaders, and interested citizens to share information on their progress. To support this initiative, the Council has developed and is distributing a toolkit that provides examples of which sectors should be represented at these events and issues that should be addressed.

State-Administered Federal Human Services Programs Are At Risk

Among the critical functions performed by states are the administration of federal human services programs. As we reported in November 1998, many systems that support state-administered federal human services programs were at risk, and much work remained to ensure that services would continue.⁴⁰ In February of this year, we testified that while some progress had been achieved, many states' systems were not scheduled to become compliant until the last half of 1999.⁴¹ Accordingly, we concluded that, given these risks, business continuity and contingency planning was even more important in ensuring continuity of program operations and benefits in the event of systems failures.

Subsequent to our November 1998 report, OMB directed federal oversight agencies to include the status of selected state human services systems in their quarterly reports. Specifically, in January 1999, OMB requested that agencies describe actions to help ensure that federally supported, state-run programs will be able to provide services and benefits. OMB further asked that agencies report the date when each state's systems will be Year 2000-compliant. Tables 1 and 2 summarize the information gathered by the

⁴⁰Year 2000 Computing Crisis: Readiness of State Automated Systems to Support Federal Welfare Programs (GAO/AIMD-99-28, November 6, 1998).

⁴¹Year 2000 Computing Crisis: Readiness of State Automated Systems That Support Federal Human Services Programs (GAO/T-AIMD-99-91, February 24, 1999).

Departments of Agriculture and Health and Human Services, respectively, on the compliance status of state-level organizations. The information indicates that a number of states do not plan to complete their Year 2000 efforts until the last quarter of 1999.

Table 1: Reported State-level Readiness for Federally Supported Programs, Department of Agriculture, May 1999^a

Program	Compliant	April-June	July-September	October-December	Unknown ^b
Food Stamps	25	12	14	3	0
Child Nutrition	29	9	10	4	2
Women, Infants, and Children	33	11	7	3	0

^aThis chart contains readiness information from the 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands.

^bUnknown indicates the state did not provide a date or the date was unknown.

Source: Department of Agriculture.

Table 2: Reported State-level^a Readiness for Federally Supported Programs, Department of Health and Human Services^b

Program	Compliant ^c	Jan.- March	April- June	July- Sept.	Oct.- Dec.	Unk. ^d	N/A ^e
Child Care	24	5	5	8	2	6	4
Child Support Enforcement	15	4	13	8	8	6	0
Child Welfare	20	5	9	11	3	5	1
Low Income Housing Energy Assistance Program	10	0	3	7	1	32	1
Medicaid – Integrated Eligibility System	20	0	15	15	4	0	0
Medicaid – Management Information System	17	0	19	14	4	0	0
Temporary Assistance for Needy Families	19	3	12	15	1	4	0

^aThis chart contains readiness information from the 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands.

^bThe OMB report stated that this information was as of January 31, 1999. However, OMB provided a draft table to the National Association of State Information Resource Executives which, in turn, provided the draft table to the states. The states were asked to contact HHS and provide corrections by June 1, 1999. For its part, HHS submitted updated state data to OMB in early June.

^cIn many cases the report indicated a date instead of whether the state was compliant. We assumed that states reporting completion dates in 1998 or earlier were compliant.

^dUnknown indicates that, according to OMB, the data reported by the states were unclear or that no information was reported by the agency.

^eN/A indicates that the states or territories reported that the data requested were not applicable to them.

Source: Progress on Year 2000 Conversion: 9th Quarterly Report (OMB, issued on June 15, 1999).

In addition, in June 1999, OMB reported that, as of March 31, 1999, 27 states' unemployment insurance systems were compliant, 11 planned to be completed between April and June 1999, 10 planned to be completed between July and September, and 5 planned to be completed between October and December.

Along with obtaining readiness information from the states, agencies have initiated additional actions to help ensure the Year 2000 compliance of state-administered programs. About a quarter of the federal government's programs designated high-impact by OMB are state-administered, such as Food Stamps and Temporary Assistance for

Needy Families. In response to OMB's March memorandum regarding the high-impact programs, the Departments of Agriculture, Health and Human Services, and Labor reported on various actions that they are taking or plan to take to help ensure the Year 2000 compliance of their state-administered programs. For example:

- The Department of Agriculture reported in May that its Food and Nutrition Service requested that states provide their contingency plans and had contracted for technical support services to review these plans, as needed, and to assist in its oversight of other state Year 2000 activities.
- The Department of Health and Human Services reported that its Administration for Children and Families and Health Care Financing Administration had contracted for on-site assessments of state partners, which will include reviews of business continuity and contingency plans.
- The Department of Labor reported that states are required to submit a certification of Year 2000 compliance for their benefit and tax systems along with an independent verification and validation report. In addition, Labor required that state agencies prepare business continuity and contingency plans, which will be reviewed by Labor officials. Further, the department plans to design and develop a prototype PC-based system to be used in the event that a state's unemployment insurance system is unusable due to a Year 2000-induced problem.

An example of the benefits that federal/state partnerships can provide is illustrated by the Department of Labor's unemployment services program. In September 1998, we reported that many State Employment Security Agencies were at risk of failure as early as January 1999 and urged the Department of Labor to initiate the development of realistic contingency plans to ensure continuity of core business processes in the event of Year 2000-induced failures.⁴² Just last month, we testified that four state agencies' systems could have failed if systems in those states had not been programmed with an emergency patch in December 1998. This patch was developed by several of the state agencies and promoted to other state agencies by the Department of Labor.⁴³

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

Beyond the risks faced by federal, state, and local governments, the year 2000 also poses a serious challenge to the public infrastructure, key economic sectors, and to other

⁴²Year 2000 Computing Crisis: Progress Made at Department of Labor, But Key Systems at Risk (GAO/T-AIMD-98-303, September 17, 1998).

⁴³Year 2000 Computing Challenge: Labor Has Progressed But Selected Systems Remain at Risk (GAO/T-AIMD-99-179, May 12, 1999).

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.⁴⁴ 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 has formed 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.

Our April 1998 report also recommended that the President's Council 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 then planned to issue quarterly public reports summarizing these assessments. The first such report was issued on January 7, 1999.

The Council's second report was issued on April 21, 1999.⁴⁵ The report stated that substantial progress had been made in the prior 6 to 12 months, but that there was still much work to be done. According to the Council, most industries had projected completion target dates between June and September and were in, or would soon be moving into, the critical testing phase. Key points in the Council's April assessment included the following:

- National Year 2000 failures in key U.S. infrastructures such as power, banking, telecommunications, and transportation are unlikely.
- Organizations that are not paying appropriate attention to the Year 2000 problem or that are adopting a "wait and see" strategy—an attitude prevalent among some small businesses and local governments—are putting themselves and those that depend upon them at great risk.
- International Year 2000 activity, although increasing, is lagging and will be the source of the greatest risk.

⁴⁴GAO/AIMD-98-85, April 30, 1998.

⁴⁵Both of the Council's reports are available on its web site, www.y2k.gov. In addition, the Council, in conjunction with the Federal Trade Commission and the General Services Administration, has established a toll-free Year 2000 information line, 1-888-USA-4Y2K. The Federal Trade Commission has also included Year 2000 information of interest to consumers on its web site, www.consumer.gov.

The Council's assessment reports have substantially increased the nation's understanding of the Year 2000 readiness of key industries. However, the picture remained incomplete in certain key areas because the surveys conducted did not have a high response rate, the assessment was general, or the data were old. For example, according to the assessment report, only 13 percent of the nation's 9-1-1 centers had responded to a survey being conducted by the Federal Emergency Management Agency in conjunction with the National Emergency Number Association, calling into question whether the results of the survey accurately portrayed the readiness of the sector. In the case of drinking water, both the January and April reports provided a general assessment but did 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). Finally, in some cases, such as the transit industry, the sector surveys had been conducted months earlier.

The President's Council is to be commended on the strides that it has made to obtain Year 2000 readiness data 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, in testimony this January, we suggested that the Council consider additional actions such as continuing to aggressively pursue readiness information in the areas in which it is lacking.⁴⁶ If the current approach of using associations to voluntarily collect information does not yield the necessary information, we suggested that the Council may wish to consider whether legislative remedies (such as requiring disclosure of Year 2000 readiness data) should be proposed. In response to this suggestion, the Council Chair stated that the Council has focused on collaboration and communication with associations and other groups as a means to get industries to share information on their Year 2000 readiness and that the Council did not believe that legislation would be necessary. The Council's next sector report is expected to be released later this month.

Subsequent to the Council's April report, surveys in key sectors have been issued. In addition, we have issued several products related to several of these sectors. I will now discuss the results of some of these surveys and our reviews.

Energy Sector

In April, we reported that while the electric power industry had concluded that it had made substantial progress in making its systems and equipment ready to continue operations into the year 2000, significant risks remained since many reporting organizations did not expect to be Year 2000 ready within the June 1999 industry target date.⁴⁷ We, therefore, suggested that the Department of Energy (1) work with the Electric Power Working Group to ensure that remediation activities were accelerated for

⁴⁶GAO/T-AIMD-99-50, January 20, 1999.

⁴⁷Year 2000 Computing Crisis: Readiness of the Electric Power Industry (GAO/AIMD-99-114, April 6, 1999).

the utilities that expected to miss the June 1999 deadline for achieving Year 2000 readiness and (2) encourage state regulatory utility commissions to require a full public disclosure of Year 2000 readiness status of entities transmitting and distributing electric power. The Department of Energy generally agreed with our suggestions. We also suggested that the Nuclear Regulatory Commission (1) in cooperation with the Nuclear Energy Institute, work with nuclear power plant licensees to accelerate the Year 2000 remediation efforts among the nuclear power plants that expect to meet the June 1999 deadline for achieving readiness and (2) publicly disclose the Year 2000 readiness of each of the nation's operational nuclear reactors. In response, the Nuclear Regulatory Commission stated that it plans to focus its efforts on nuclear power plants that may miss the July 1, 1999 milestone and that it would release the readiness information on individual plants that same month.

Subsequent to our report, on April 30, 1999, the North American Electric Reliability Council released its third status report on electric power systems. According to the North American Electric Reliability Council, as of March 31, 1999, reporting organizations, on average, had completed 99 percent of the inventory phase, 95 percent of the assessment phase, and 75 percent of the remediation/testing phase.

In May, we reported⁴⁸ that while the domestic oil and gas industries had reported that they had made substantial progress in making their equipment and systems ready to continue operations into the year 2000, risks remained. In particular, a February industrywide survey found that over a quarter of the oil and gas industries reported that they did not expect to be Year 2000 ready until the second half of 1999—leaving little time for resolving unexpected problems. Moreover, although over half of our oil is imported, little was known about the Year 2000 readiness of foreign oil suppliers. Further, while individual domestic companies reported that they were developing Year 2000 contingency plans, there were no plans to perform a national-level risk assessment and develop contingency plans to deal with potential shortages or disruptions in the nation's overall oil and gas supplies. We suggested that the Council's oil and gas working group (1) work with industry associations to perform national-level risk assessments and develop and publish credible, national-level scenarios regarding the impact of potential Year 2000 failures and (2) develop national-level contingency plans. The working group generally agreed with these suggestions.

Water Sector

As I previously mentioned, the Council's January and April assessment reports provided only a general assessment of the drinking water sector and did not contain detailed data. Similarly, in April we reported⁴⁹ that insufficient information was available to assess and

⁴⁸Year 2000 Computing Crisis: Readiness of the Oil and Gas Industries (GAO/AIMD-99-162, May 19, 1999).

⁴⁹Year 2000 Computing Crisis: Status of the Water Industry (GAO/AIMD-99-151, April 21, 1999).

manage Year 2000 efforts in the water sector, and little additional information was expected under the current regulatory approach. While the Council's water sector working group had undertaken an awareness campaign and had urged national water sector associations to continue to survey their memberships, survey response rates had been low. Further, Environmental Protection Agency officials stated that the agency lacked the rules and regulations necessary to require water and wastewater facilities to report on their Year 2000 status.

Our survey of state regulators found that a few states were proactively collecting Year 2000 compliance data from regulated facilities, a much larger group of states was disseminating Year 2000 information, while another group was not actively using either approach. Additionally, only a handful of state regulators believed that they were responsible for ensuring facilities' Year 2000 compliance or overseeing facilities' business continuity and contingency plans. Among our suggested actions was that the Council, the Environmental Protection Agency, and the states determine which regulatory organization should take responsibility for assessing and publicly disclosing the status and outlook of water sector facilities' Year 2000 business continuity and contingency plans. The Environmental Protection Agency generally agreed with our suggestions but one official noted that additional legislation may be needed if the agency is to take responsibility for overseeing facilities' Year 2000 business continuity and contingency plans.

Health Sector

The health sector includes health care providers (such as hospitals and emergency health care services), insurers (such as Medicare and Medicaid), and biomedical equipment. With respect to biomedical equipment, on June 10 we testified⁵⁰ that, in response to our September 1998 recommendation,⁵¹ HHS, in conjunction with the Department of Veterans Affairs, had established a clearinghouse on biomedical equipment. As of June 1, 1999, 4,142 biomedical equipment manufacturers had submitted data to the clearinghouse. About 61 percent of these manufacturers reported having products that do not employ dates and about 8 percent (311 manufacturers) reported having date-related problems such as an incorrect display of date/time. According to the Food and Drug Administration, the 311 manufacturers reported 897 products with date-related problems. However, not all compliance information was available on the clearinghouse because the clearinghouse referred the user to 427 manufacturers' web sites. Accordingly, we reviewed the web sites of these manufacturers and found, as of June 1, 1999, a total of

⁵⁰Year 2000 Computing Challenge: Concerns About Compliance Information on Biomedical Equipment (GAO/T-AIMD-99-209, June 10, 1999).

⁵¹Year 2000 Computing Crisis: Compliance Status of Many Biomedical Equipment Items Still Unknown (GAO/AIMD-98-240, September 18, 1998).

35,446 products.⁵² Of these products, 18,466 were reported as not employing a date, 11,211 were reported as compliant, 4,445 were shown as not compliant, and the compliance status of 1,324 was unknown.

In addition to the establishment of a clearinghouse, our September 1998 report also recommended that HHS and the Department of Veterans Affairs take prudent steps to jointly review manufacturers' test results for critical care/life support biomedical equipment. We were especially concerned that the departments review test results for equipment previously deemed to be noncompliant but now deemed by manufacturers to be compliant, or equipment for which concerns about compliance remained. In May 1999, the Food and Drug Administration, a component agency of HHS, announced that it planned to develop a list of critical care/life support medical devices and the manufacturers of these devices, select a sample of manufacturers for review, and hire a contractor to develop a program to assess manufacturers' activities to identify and correct Year 2000 problems for these medical devices. In addition, if the results of this review indicated a need for further review of manufacturer activities, the contractor would review a portion of the remaining manufacturers not yet reviewed. Moreover, according to the Food and Drug Administration, any manufacturer whose quality assurance system appeared deficient based on the contractors review would be subject to additional reviews to determine what actions would be required to eliminate any risk posed by noncompliant devices.

In April testimony⁵³ we also reported on the results of a Department of Veterans Affairs survey of 384 pharmaceutical firms and 459 medical-surgical firms with whom it does business. Of the 52 percent of pharmaceutical firms that responded to the survey, 32 percent reported that they were compliant. Of the 54 percent of the medical-surgical firms that responded, about two-thirds reported that they were compliant.

Banking and Finance Sector

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 agencies⁵⁴ to ensure that the institutions that they oversee are ready to handle the Year 2000 problem.⁵⁵ We concluded that the

⁵²Because of limitations in many of the manufacturers web sites, our ability to determine the total number of biomedical equipment products reported and their compliance status was impaired. Accordingly, the actual number of products reported by the manufacturers could be significantly higher than the 35,446 products that we counted.

⁵³Year 2000 Computing Crisis: Action Needed to Ensure Continued Delivery of Veterans Benefits and Health Care Services (GAO/T-AIMD-99-136, April 15, 1999).

⁵⁴The 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.

⁵⁵Year 2000 Computing Crisis: Federal Depository Institution Regulators Are Making Progress, But Challenges Remain (GAO/T-AIMD-98-305, September 17, 1998).

regulators had made significant progress in assessing the readiness of member institutions and in 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.

In April, we reported that the Federal Reserve System--which is instrumental to our nation's economic well-being, since it provides depository institutions and government agencies services such as processing checks and transferring funds and securities, has effective controls to help ensure that its Year 2000 progress is reported accurately and reliably.⁵⁶ We also found that it is effectively managing the renovation and testing of its internal systems and the development and planned testing of contingency plans for continuity of business operations. Nevertheless, the Federal Reserve System still had much to accomplish before it is fully ready for January 1, 2000, such as completing validation and implementation of all of its internal systems and completing its contingency plans.

In addition to the domestic banking and finance sector, large U.S. financial institutions have financial exposures and relationships with international financial institutions and markets that may be at risk if these international organizations are not ready for the date change occurring on January 1, 2000. In April, we reported⁵⁷ that foreign financial institutions had reportedly lagged behind their U.S. counterparts in preparing for the Year 2000 date change. Officials from four of the seven large foreign financial institutions we visited said they had scheduled completion of their Year 2000 preparations about 3 to 6 months after their U.S. counterparts, but they planned to complete their efforts by mid-1999 at the latest. Moreover, key international market supporters, such as those that transmit financial messages and provide clearing and settlement services, told us that their systems were ready for the date change and that they had begun testing with the financial organizations that depended on these systems. Further, we found that seven large U.S. banks and securities firms we visited were taking actions to address their international risks. In addition, U.S. banking and securities regulators were also addressing the international Year 2000 risks of the institutions that they oversee.

With respect to the insurance industry, in March, we concluded that insurance regulator presence regarding the Year 2000 area was not as strong as that exhibited by the banking and securities industry.⁵⁸ State insurance regulators we contacted were late in raising industry awareness of potential Year 2000 problems, provided little guidance to regulated

⁵⁶Year 2000 Computing Crisis: Federal Reserve Has Established Effective Year 2000 Management Controls for Internal Systems Conversion (GAO/AIMD-99-78, April 9, 1999).

⁵⁷Year 2000: Financial Institution and Regulatory Efforts to Address International Risks (GAO/GGD-99-62, April 27, 1999).

⁵⁸Insurance Industry: Regulators Are Less Active in Encouraging and Validating Year 2000 Preparedness (GAO/T-GGD-99-56, March 11, 1999).

institutions, and failed to convey clear regulatory expectations to companies about Year 2000 preparations and milestones. Nevertheless, the insurance industry is reported by both its regulators and by other outside observers to be generally on track to being ready for 2000. However, most of these reports are based on self-reported information and, compared to other financial regulators, insurance regulators' efforts to validate this information generally began late and were more limited.

In a related report in April,⁵⁹ we stated that variations in oversight approaches by state insurance regulators also made it difficult to ascertain the overall status of the insurance industry's Year 2000 readiness. We reported that the magnitude of insurers' Year 2000-related liability exposures could not be estimated at that time but that costs associated with these exposures could be substantial for some property-casualty insurers, particularly those concentrated in commercial-market sectors. In addition, despite efforts to mitigate potential exposures, the Year 2000-related costs that may be incurred by insurers would remain uncertain until key legal issues and actions on pending legislation were resolved.

Transportation Sector

A key component to the nation's transportation sector are airports. This January we reported on our survey of 413 airports.⁶⁰ We found that while the nation's airports are making progress in preparing for the year 2000, such progress varied. Of the 334 airports responding to our survey, about one-third reported that they would complete their Year 2000 preparations by June 30, 1999. The other two-thirds either planned on a later date or failed to estimate any completion date, and half of these airports did not have contingency plans for any of 14 core airport functions. Although most of those not expecting to be ready by June 30 are small airports, 26 of them are among the nation's largest 50 airports.

On June 18, the Federal Aviation Administration issued an air industry Year 2000 status report that included information on airports and airline carriers. Table 3 provides the assessment, renovation, validation, and implementation information contained in this report.

⁵⁹Year 2000: State Insurance Regulators Face Challenges in Determining Industry Readiness (GAO/GGD-99-87, April 30, 1999).

⁶⁰Year 2000 Computing Crisis: Status of Airports' Efforts to Deal With Date Change Problem (GAO/RCED/AIMD-99-57, January 29, 1999).

Table 3: Industry Segment Percentage Completion of Year 2000 Remediation Phases

Industry Segment	Assessment	Renovation	Validation	Implementation
Large hub airports	98%	63%	31%	26%
Medium hub airports	100%	70%	43%	37%
Small hub airports	94%	61%	55%	48%
Non-hub airports	93%	67%	67%	70%
Major carriers	100%	75%	50%	^a
Low-cost carriers	73%	38%	19%	18%

^aImplementation was occurring as validation and testing were completed.

Note: Airport information was based on data as of March 15, 1999 from the American Association of Airport Executives and the Airports Council International/North America. The major carrier information based on data as of February 22, 1999 from the Air Transport Association of America, and the low-cost carrier information was based on data as of November 30, 1998 from the National Air Carriers Association, Inc.

Source: Federal Aviation Administration.

Manufacturing and Small Business Sector

The manufacturing and small business sector includes the entities that produce or sell a myriad of products such as chemicals, electronics, heavy equipment, food, textiles, and automobiles. With respect to the chemical industry, table 4 contains the latest survey data by Chemical Manufacturers Association--which represents over 190 primarily large chemical companies--and shows that while some companies' systems are Year 2000 ready, others are in varying stages of completion. This survey provided information on the Year 2000 readiness stage of 123 respondents with respect to their business systems, manufacturing, inventory, and distribution systems, embedded systems, and supply chain as of May 12, 1999.

Table 4: Results of May 12, 1999 Survey of Chemical Manufacturers Association⁶¹

Function	Year 2000 Ready	Planning	Inventory/ Assessment	Remediation	Validation
Business systems	26	1	5	51	27
Manufacturing, inventory, and distribution systems	18	2	7	53	28
Embedded systems	15	2	26	52	13
Supply chain	10	4	51	22	21

*Some respondents did not provide information to all questions or stated that the question was not applicable.

Source: Chemical Manufacturers Association statement before the Senate Special Committee on the Year 2000 Technology Problem, May 14, 1999.

Since the Chemical Manufacturers Association represented mainly large companies, a survey of small and mid-sized chemical companies was sponsored by several industry associations⁶¹ to assist the Congress, the administration, and the U.S. Chemical Safety and Hazard Investigation Board by obtaining information on the preparedness of this segment of the industry. Table 5 contains the results of the survey, which was conducted between March and May 1999.

⁶¹The sponsors of the survey were the American Crop Protection Association, Chemical Producers & Distributors Association, Chemical Specialties Manufacturers Association, International Sanitary Supply Association, National Association of Chemical Distributors, Responsible Industry for a Sound Environment, and the Synthetic Organic Chemical Manufacturers Association.

Table 5: Readiness Stage of Small and Medium-Sized Chemical Companies^a

Function	Year 2000 Ready	Planning	Inventory/ Assessment	Remediation	Validation
Business systems	147	8	4	24	12
Manufacturing, inventory, and distribution systems	133	8	3	21	13
Embedded systems	83	3	7	13	6
Supply chain	80	17	29	17	25

^aSome respondents did not provide information to all questions or stated that the question was not applicable.

Source: Year 2000 Readiness Disclosure Survey of Small & Mid-Sized Chemical Companies, June 9, 1999.

Another key segment of the economy are small businesses. The National Federation of Independent Business and Wells Fargo sponsored a third survey of the Year 2000 preparedness of small businesses between mid-April and mid-May 1999. This survey found that 84 percent of small businesses are directly exposed to a possible Year 2000 problem. Of the small businesses directly exposed to the Year 2000 problem, 59 percent had taken action, 12 percent planned to take action, and 28 percent did not plan to take action (the other 1 percent responded that the question was not applicable). In addition, 43 percent of the small businesses that were aware of the Year 2000 problem had made contingency plans to minimize the impact of potential problems.

In summary, while improvement has been shown, much work remains at the national, federal, state, and local levels to ensure that major service disruptions do not occur. Specifically, remediation must be completed, end-to-end testing performed, and business continuity and contingency plans developed. Similar actions remain to be completed by the nation's key sectors. Accordingly, whether the United States successfully confronts the Year 2000 challenge will largely depend on the success of federal, state, and local governments, as well as the private sector working separately and together to complete these actions. Accordingly, strong leadership and partnerships must be maintained to ensure that the needs of the public are met at the turn of the century.

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

APPENDIX I

APPENDIX I

Federal High-Impact Programs and Lead Agencies

Agency	Program
Department of Agriculture	Child Nutrition Programs
Department of Agriculture	Food Safety Inspection
Department of Agriculture	Food Stamps
Department of Agriculture	Special Supplemental Nutrition Program for Women, Infants, and Children
Department of Commerce	Patent and trademark processing
Department of Commerce	Weather Service
Department of Defense	Military Hospitals
Department of Defense	Military Retirement
Department of Education	Student Aid
Department of Energy	Federal electric power generation and delivery
Department of Health and Human Services	Child Care
Department of Health and Human Services	Child Support Enforcement
Department of Health and Human Services	Child Welfare
Department of Health and Human Services	Disease monitoring and the ability to issue warnings
Department of Health and Human Services	Indian Health Service
Department of Health and Human Services	Low Income Home Energy Assistance Program
Department of Health and Human Services	Medicaid
Department of Health and Human Services	Medicare
Department of Health and Human Services	Organ Transplants
Department of Health and Human Services	Temporary Assistance for Needy Families
Department of Housing and Urban Development	Housing loans (Government National Mortgage Association)

Department of Housing and Urban Development	Section 8 Rental Assistance
Department of Housing and Urban Development	Public Housing
Department of Housing and Urban Development	FHA Mortgage Insurance
Department of Housing and Urban Development	Community Development Block Grants
Department of the Interior	Bureau of Indians Affairs programs
Department of Justice	Federal Prisons
Department of Justice	Immigration
Department of Justice	National Crime Information Center
Department of Labor	Unemployment Insurance
Department of State	Passport Applications and Processing
Department of Transportation	Air Traffic Control System
Department of Transportation	Maritime Safety Program
Department of the Treasury	Cross-border Inspection Services
Department of Veterans Affairs	Veterans' Benefits
Department of Veterans Affairs	Veterans' Health Care
Federal Emergency Management Agency	Disaster Relief
Office of Personnel Management	Federal Employee Health Benefits
Office of Personnel Management	Federal Employee Life Insurance
Office of Personnel Management	Federal Employee Retirement Benefits
Railroad Retirement Board	Retired Rail Workers Benefits
Social Security Administration	Social Security Benefits
U.S. Postal Service	Mail Service

GAO REPORTS AND TESTIMONY ADDRESSING THE YEAR 2000 CRISIS

Defense Computers: Management Controls Are Critical To Effective Year 2000 Testing (GAO/AIMD-99-172, June 30, 1999)

Year 2000 Computing Crisis: Customs is Making Good Progress (GAO/T-AIMD-99-225, June 29, 1999)

Year 2000 Computing Challenge: Delivery of Key Benefits Hinges on States' Achieving Compliance (GAO/T-AIMD/GGD-99-221, June 23, 1999)

Year 2000 Computing Challenge: Estimated Costs, Planned Uses of Emergency Funding, and Future Implications (GAO/T-AIMD-99-214, June 22, 1999)

GSA's Effort to Develop Year 2000 Business Continuity and Contingency Plans for Telecommunications Systems (GAO/AIMD-99-201R, June 16, 1999)

Year 2000 Computing Crisis: Actions Needed to Ensure Continued Delivery of Veterans Benefits and Health Care Services (GAO/AIMD-99-190R, June 11, 1999)

Year 2000 Computing Challenge: Concerns About Compliance Information on Biomedical Equipment (GAO/T-AIMD-99-209, June 10, 1999)

Year 2000 Computing Challenge: Much Biomedical Equipment Status Information Available. Yet Concerns Remain (GAO/T-AIMD-99-197, May 25, 1999)

Year 2000 Computing Challenge: OPM Has Made Progress on Business Continuity Planning (GAO/GGD-99-66, May 24, 1999)

VA Y2K Challenges: Responses to Post-Testimony Questions (GAO/AIMD-99-199R, May 24, 1999)

Year 2000 Computing Crisis: USDA Needs to Accelerate Time Frames for Completing Contingency Planning (GAO/AIMD-99-178, May 21, 1999)

Year 2000 Computing Crisis: Readiness of the Oil and Gas Industries (GAO/AIMD-99-162, May 19, 1999)

Year 2000 Computing Challenge: Time Issues Affecting the Global Positioning System (GAO/T-AIMD-99-187, May 12, 1999)

Year 2000 Computing Challenge: Education Taking Needed Actions But Work Remains (GAO/T-AIMD-99-180, May 12, 1999)

Year 2000 Computing Challenge: Labor Has Progressed But Selected Systems Remain at Risk (GAO/T-AIMD-99-179, May 12, 1999)

Year 2000: State Insurance Regulators Face Challenges in Determining Industry Readiness (GAO/GGD-99-87, April 30, 1999)

Year 2000 Computing Challenge: Status of Emergency and State and Local Law Enforcement Systems Is Still Unknown (GAO/T-AIMD-99-163, April 29, 1999)

Year 2000 Computing Crisis: Costs and Planned Use of Emergency Funds (GAO/AIMD-99-154, April 28, 1999)

Year 2000: Financial Institution and Regulatory Efforts to Address International Risks (GAO/GGD-99-62, April 27, 1999)

Year 2000 Computing Crisis: Readiness of Medicare and the Health Care Sector (GAO/T-AIMD-99-160, April 27, 1999)

U.S. Postal Service: Subcommittee Questions Concerning Year 2000 Challenges Facing the Service (GAO/AIMD-99-150R, April 23, 1999)

Year 2000 Computing Crisis: Status of the Water Industry (GAO/AIMD-99-151, April 21, 1999)

Year 2000 Computing Crisis: Key Actions Remain to Ensure Delivery of Veterans Benefits and Health Services (GAO/T-AIMD-99-152, April 20, 1999)

Year 2000 Computing Crisis: Readiness Improving But Much Work Remains To Ensure Delivery of Critical Services (GAO/T-AIMD-99-149, April 19, 1999)

Year 2000 Computing Crisis: Action Needed to Ensure Continued Delivery of Veterans Benefits and Health Care Services (GAO/T-AIMD-99-136, April 15, 1999)

Year 2000 Computing Challenge: Federal Government Making Progress But Critical Issues Must Still Be Addressed to Minimize Disruptions (GAO/T-AIMD-99-114, April 14, 1999)

Year 2000 Computing Crisis: Additional Work Remains to Ensure Delivery of Critical Services (GAO/T-AIMD-99-143, April 13, 1999)

Tax Administration: IRS' Fiscal Year 2000 Budget Request and 1999 Tax Filing Season (GAO/T-GGD/AIMD-99-140, April 13, 1999).

Year 2000 Computing Crisis: Federal Reserve Has Established Effective Year 2000 Management Controls for Internal Systems Conversion (GAO/AIMD-99-78, April 9, 1999)

Year 2000 Computing Crisis: Readiness of the Electric Power Industry (GAO/AIMD-99-114, April 6, 1999)

Year 2000 Computing Crisis: Customs Has Established Effective Year 2000 Program Controls (GAO/AIMD-99-37, March 29, 1999)

Year 2000 Computing Crisis: FAA Is Making Progress But Important Challenges Remain (GAO/T-AIMD/RCED-99-118, March 15, 1999)

Insurance Industry: Regulators Are Less Active in Encouraging and Validating Year 2000 Preparedness (GAO/T-GGD-99-56, March 11, 1999)

Year 2000 Computing Crisis: Defense Has Made Progress, But Additional Management Controls Are Needed (GAO/T-AIMD-99-101, March 2, 1999)

Year 2000 Computing Crisis: Readiness Status of the Department of Health and Human Services (GAO/T-AIMD-99-92, February 26, 1999)

Defense Information Management: Continuing Implementation Challenges Highlight the Need for Improvement (GAO/T-AIMD-99-93, February 25, 1999)

IRS' Year 2000 Efforts: Status and Remaining Challenges (GAO/T-GGD-99-35, February 24, 1999)

Department of Commerce: National Weather Service Modernization and NOAA Fleet Issues (GAO/T-AIMD/GGD-99-97, February 24, 1999)

Year 2000 Computing Crisis: Medicare and the Delivery of Health Services Are at Risk (GAO/T-AIMD-99-89, February 24, 1999)

Year 2000 Computing Crisis: Readiness of State Automated Systems That Support Federal Human Services Programs (GAO/T-AIMD-99-91, February 24, 1999)

Year 2000 Computing Crisis: Customs Is Effectively Managing Its Year 2000 Program (GAO/T-AIMD-99-85, February 24, 1999)

Year 2000 Computing Crisis: Update on the Readiness of the Social Security Administration (GAO/T-AIMD-99-90, February 24, 1999)

Year 2000 Computing Crisis: Challenges Still Facing the U.S. Postal Service (GAO/T-AIMD-99-86, February 23, 1999)

Year 2000 Computing Crisis: The District of Columbia Remains Behind Schedule (GAO/T-AIMD-99-84, February 19, 1999)

High-Risk Series: An Update (GAO/HR-99-1, January 1999)

Year 2000 Computing Crisis: Status of Airports' Efforts to Deal With Date Change Problem (GAO/RCED/AIMD-99-57, January 29, 1999)

Defense Computers: DOD's Plan for Execution of Simulated Year 2000 Exercises (GAO/AIMD-99-52R, January 29, 1999)

Year 2000 Computing Crisis: Status of Bureau of Prisons' Year 2000 Efforts (GAO/AIMD-99-23, January 27, 1999)

Year 2000 Computing Crisis: Readiness Improving, But Much Work Remains to Avoid Major Disruptions (GAO/T-AIMD-99-50, January 20, 1999)

Year 2000 Computing Challenge: Readiness Improving, But Critical Risks Remain (GAO/T-AIMD-99-49, January 20, 1999)

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)

(511774)

Mrs. BIGGERT. Thank you. Ms. Reynolds.

Ms. REYNOLDS. Thank you very much. Congressman Horn, welcome to Illinois. And Congresswoman Biggert, it is great to see you again. Thank you for inviting me to share where the State of Illinois is in its preparation for Y2K.

Governor Ryan has made Y2K a priority in his administration and has taken very aggressive steps to make sure that every agency of State government has in fact done all of the reasonable steps to become Y2K ready. In the first weeks of his administration, Governor Ryan created the Illinois Technology Office. Included in my duties as the head of that organization, I oversee the Y2K efforts of State government.

This spring we've designed and implemented a new monthly reporting system by State agencies that adopts a unique approach to definitions and public reporting. I am not aware of any other State in the Nation that is publicly reporting the amount and depth of information Illinois is providing in regard to the Y2K readiness of State agencies.

While many organizations have chosen to remediate computer systems, our focus has been to ensure that the functions of government are Y2K ready and operational. We ask each agency to report the functions and services that it is required to perform and then list each of those systems or components that support the function.

Agencies are asked about the detailed readiness of all the components to support those functions of government. The supporting components include all types of computer systems: Mid-range, PCs, desktop, mainframes as well as the electronic data interfaces, embedded systems, and supplier customer dependency chains.

We do not consider a system as Y2K ready until all the supporting systems and components that support that are in fact ready. That is a very difficult definition to meet.

Within the monthly report, we ask each agency to rank the tiers by functions. Programs, services, or functions included in tier 1 could not be interrupted for more than 24 hours without endangering the public health, welfare, or safety of the citizens of Illinois or seriously impacting the State's revenue streams. Tier 2 functions are those that cannot be interrupted for more than a week, and tier 3 functions are everything else.

A new monthly report will be released next week, but according to our latest report as of May 31st, State agencies have completed 85 percent of the effort to be Y2K ready.

Our current focus among the agencies is now on contingency planning. We're doing this on two levels statewide. The Illinois Emergency Management Organization is coordinating our statewide consequence management plan while the individual agencies are preparing contingency plans for their own functions of government. Overall, I'm coordinating these plans to make sure we integrate the functions of government and are able to employ the resources where they are needed.

Governor Ryan is also emphasizing the need for State government to work with other levels of government as well as the private sector to prepare for Y2K. Over the past several months we've worked closely with Federal agencies as well as local governments

and private industries to coordinate efforts and assist each other in preparations.

Overall, under Governor Ryan's leadership, the State of Illinois is doing everything it reasonably can to prepare for Y2K. We must now make sure that citizens are aware of our efforts and take a reasonable approach to their own preparations. Later this summer and fall, we'll be conducting community forums throughout Illinois at many of our community colleges. We'll also be distributing literature and pursuing public awareness campaigns, and we will continue to update our new enhanced Y2K Web page to make sure the latest information is also available electronically.

We believe the best way to relieve and ease public concern and apprehension over Y2K is by communicating openly and frequently about the status of our Y2K efforts. We appreciate your attention to this matter and at the appropriate time I'll be happy to answer any questions.

Mrs. BIGGERT. Thank you very much.

[The prepared statement of Ms. Reynolds follows:]

**Y2K Congressional Hearing
House Subcommittee on Government Management, Information and Technology**

**Testimony by Mary Barber Reynolds
Chief Technology Officer
Office of Governor George H. Ryan
July 8, 1999**

Good morning. Thank you for the opportunity to participate in this hearing and share a status report of where the State of Illinois is at in its preparation for the Year 2000.

Governor Ryan has made "Y2K" a priority and has taken very aggressive steps to prepare this state for the rollover from 1999 to 2000. In the first weeks of his Administration, Governor Ryan created the Illinois Technology Office. Included in my duties as the head of this office, I oversee the Y2K efforts of state government.

This Spring, we have designed and implemented a monthly reporting system by state agencies that adopts a unique approach to definitions and public reporting. I know of no other state government in the country that is publicly reporting the amount and depth of information Illinois is providing with regards to the Y2K readiness of state agencies.

While many organizations have chosen to remediate computer systems, our focus has been to ensure that the functions of government are Y2K ready and operational. We ask each agency to report the functions and services that it is required to perform and then list all of those systems or components that support the function. Agencies are then asked about the detailed Y2K readiness of all of the components that support each function. These supporting components include: all types of computer systems, electronic data interfaces, embedded systems, and supplier-to-customer dependency chains. We do not consider a function as "Y2K ready" until all of the supporting components are ready.

Within the monthly report, we ask each agency to rank the functions by tiers. Programs, services or functions included in Tier 1, could not be interrupted for more than 24 hours without endangering the public health, welfare or safety of the citizens of Illinois or seriously impact the State's revenue streams. Tier 2 functions are those that could not be interrupted for more than one week, and Tier 3 functions are all others.

Page 2
Reynolds Testimony
Y2K Congressional Hearing
July 8, 1999

A new monthly report will be released next week. According to our latest report, as of May 31 state agencies have completed 85 percent of the effort to be Y2K ready. Our current focus among the agencies is now on contingency planning. We are doing this on two levels statewide: the Illinois Emergency Management Agency is coordinating our statewide consequence management plan while agencies are preparing contingency plans for their own functions. Overall, I am coordinating these plans to ensure that we integrate the functions of government and are able to deploy resources to where they are needed.

Governor Ryan has also emphasized the need for state government to work with other levels of government as well as the private sector to prepare for Y2K. Over the past several months, we have worked closely with federal agencies as well as local governments to coordinate efforts and assist each other in preparations.

Overall, under Governor Ryan's leadership, the State of Illinois is doing everything it reasonably can to prepare for Y2K. We now must make sure that citizens are aware of our efforts and take a reasonable approach to their own preparations. Later this summer and fall, we will be conducting community forums throughout Illinois at many of our community colleges. We will also be distributing literature and pursuing public awareness campaigns. And, we will continue to update our new enhanced Y2K webpage to make sure that the latest information is available electronically. We believe the best way to relieve and ease public concern and apprehension over Y2K is by communicating openly and frequently about the status of Y2K efforts.

Thank you for your attention to this matter. At the appropriate time, I would be happy to answer any questions.

This is a Year 2000 Readiness Disclosure document.

Mrs. BIGGERT. Next is Mr. Carlsen.

Mr. CARLSEN. Congressman Horn, Congresswoman Biggert, thank you for allowing me to testify today. I think the city welcomes this kind of a hearing because we have really done a lot of work in this area and really feel confident that we're working toward compliance.

To date, the city, the computer systems in the city, are 96 percent compliant. We expect to be 100 percent compliant by September. I think the State has adopted some great compliance guidelines that I think we may look into as well. There's some really nice definitions as far as the linkages between the systems. It's something we're going to look at.

The systems that we're looking at that we feel that citizens need to know more about that may be affected in our area really come under four main areas. Those would be the 911 system, the utilities, mainly electric and wastewater.

We own the electric utility in Naperville, which is not common in Illinois. It may be more common in California, Texas, those types of places, but we buy power wholesale from ComEd so we have some linkages there: Traffic signals and heat for residents, which really fall under Nicor, and natural gas as well as ComEd.

As far as the 911 system goes, the city does operate a public safety answering point in the police department, and we have conducted rigorous tests on the software, hardware, and phone interfaces, radio interfaces with those systems, and to date they have all proven to be compliant, and we have done some upgrading of those systems to make—some of them were not compliant originally. We have made them compliant at this time. Really a lot of work went into that. We actually had to travel to some test sites to do some work and really did a lot of work with our software vendor in that area.

Within the utility arena, as I mentioned, the city owns and operates the electric distribution, water distribution, wastewater collection, and reclamation systems. We've tested a lot of our computerized and embedded systems within those plants and we are close to compliance on a number of those systems.

Like many cities, we receive electricity and water from outside source. I mentioned ComEd, DuPage Water Commission, and we're pleased to note that both ComEd and DuPage Water Commission have worked closely with us to assure us of compliance and we're really—we're happy that they've done a lot of work in that area.

Traffic signals present an interesting concern for residents not only in Naperville but a lot of different communities. The city is responsible for 118 signals within our jurisdiction. All of our signals have been tested, and we have found no problems with any of our systems. There is an issue with electricity if they do go out. The contingency plan is to use the full-length stop signs which would obviously cause a little bit of trouble in traffic but hopefully it wouldn't be a longstanding problem.

As far as heat goes, living in the Chicago area we're obviously concerned that the weather may be bad, that there may be some problems with heating, with electricity or natural gas and, as I mentioned, we're working with Nicor and with ComEd to make sure that's not a problem.

As far as contingency planning goes, we met actually yesterday, with all the department directors, representatives from different departments, to discuss contingency planning, and what we've really done is moved from the focus on computer systems to the focus on public safety, those types of areas. And that is being headed by our Emergency Management Agency, and I think within the next couple of months we'll have some contingency plans set so we can handle any kind of public safety situations, those types of things that may occur.

In conclusion, I'd like to say we're cautiously optimistic that there will only be minor interruptions and no show-stoppers relative to Y2K within the city of Naperville. As Congresswoman Biggert stated, we're adopting the statement philosophy. We're urging residents prepare as they would for a snowstorm. Our biggest problem that we feel may be out there may be the overreaction to any problems that occur on or around the new year.

I look forward to answering any questions. Thank you.

Mrs. BIGGERT. Thank you very much.

[The prepared statement of Mr. Carlsen follows:]

Testimony of Donald J. Carlsen, Information Systems Director, City of Naperville, IL

The City has been working on Y2K compliance since 1997. Currently, all mission critical computer systems are 96% compliant. We anticipate being 100% compliant by September, 1999.

How the public might see services affected?

911 System: The City operates a Public Safety Answering Point (PSAP) function at the Police Department. This operation is responsible for the dispatch of Police, Fire and other City vehicles. The dispatching system is computerized, and the software and hardware have been tested and are compliant. There is a generator at the Police Department to handle power outages. There is a back-up computer system located in the Emergency Operations Center (EOC). In the event that there is a massive failure, PSAP can dispatch manually using the radio system. The radio system has been certified as compliant. One area of concern with the 911 system is that the phone system must be operational for people to call for help. Our research indicates that Ameritech is ready for Y2K, and we will not have any problems. The City will be developing contingency plans in the next few weeks to address this issue. In the event that the phone system fails, one answer might be to deploy Police, or Fire vehicles at strategic locations so that people could report emergencies.

Utilities - Electric and Water and Wastewater: The City owns and operates the electric distribution, and water distribution, wastewater collection, and reclamation systems. We have tested computerized, and embedded systems in the electric and water and wastewater utilities, and we anticipate no problems with those systems. Like many Cities, Naperville receives electricity and water from outside sources. Even though the City's systems may be compliant, we are dependent on outside suppliers for electricity (Commonwealth Edison), and water (DuPage Water Commission). We have received information from our suppliers, and we are pleased to note that they have been working hard on the problem, and expect no major service delivery problems.

Traffic Signals: The City is responsible 118 traffic signals within our jurisdiction. All signals have been tested by the City, or the State, and we have found no compliance issues. If the signals failed, they would all turn to flashing red, and as a back-up we have folding stop signs at all signalized intersections.

Heat: Because there is a good chance that it will be cold in the Chicago area on, and around January 1, 2000, there would be a major problem if there was no heat due to natural gas, or electric outages. As part of our contingency planning we will be discussing this issue within the next few weeks.

Contingency Plans:

As mentioned: We are in the process of developing plans for Police, Fire, and all other City services. We anticipate having these plans ready and communicating those plans to the public within the next few months. As always, we will have up-to-date information on the City's web site at www.Naperville.IL.US, the City's cable channels, and in our newsletter.

Conclusion:

We are cautiously optimistic that there will only be minor interruptions, but no show stoppers relative to Y2K. We urge residents to prepare as they would for a snow storm. Our biggest problem may be overreaction to any problems that occur on, or around the new year.

Mrs. BIGGERT. Mr. Mefferd.

Mr. MEFFERD. Thank you, Vice Chairman Biggert, Chairman Horn. I would like to address real quickly the issues relative to DuPage County's preparedness as we look at the overall picture. One of the things that we need to look at is DuPage County's response in two fronts.

First of all, internally, DuPage County is a facility much like everybody else's facility in big business. What we've tried to do is look internally at our computer systems. We've looked at our life safety systems. As of the end of June, we had been advised by our Management Information Department that we are 99.4 percent complete in upgrading for our computer systems and should reach 100 percent compliance by the end of July.

Relative to our life safety systems, we've looked at things such as our ability to generate backup power if that was necessary. Heat and cooling capabilities for the county jail, for example, the convalescent centers and our other facilities, and we feel we are in good shape relative to those issues.

Externally there are three major areas we looked at from the county's perspective. One of the biggest issues that we addressed externally was the issue of utility reliability. I'm not going to address that in great detail as you'll hear from them, not only with Mr. Martin directly following myself, but in the second panel. But with the assurances we have received, we feel pretty comfortable that utility reliability will be there, which allows us to move on to other areas.

Second, as we looked at external issues, we looked at the issue of emergency communications, 911, our emergency radio transmitter sites around the county, that we've been assured that those systems are in good working shape. There's been a significant amount of work done with the countywide computer-aided dispatch system to ensure that it, in fact, is reliable. There's been some hardware changes made in that area which assures that it will be up and running.

Also, the issue of traffic control is something we looked at. The county has looked at five of its different type of controller systems which are common to all of our 100-plus intersections that we control. Every one of those five different types of controllers that the county uses has been tested by allowing the clock and the system to run from 10 minutes prior to midnight to 10 minutes after midnight into the year 2000. There's not been one glitch in any one of those traffic control devices, and that information has been shared with all of our municipalities to ensure the reliability of their systems which are using the same type of controllers.

As we move on to the area of public safety, and that's really where I want to focus today, a lot of questions routinely get asked around the country as we talk about emergency planning. Will do DuPage County develop a specific Y2K emergency planning? The answer to that question is no. The reason for that is that DuPage County, like every other county in the State of Illinois as well as around the country, is required by the State law as well as by the Federal Emergency Management Association to maintain an all hazard emergency plan. That plan must address everything from

tornadoes and floods to utility failures or any type of other incident.

The county emergency operations plan 2 years ago was reformatted, if you will, to be in concert with the Federal response plan. Specifically with the thought of the fact that if we have a disaster of large proportion that would be large enough to implement our entire emergency plan, it would definitely be big enough to bring in the Federal Government. And we wanted to ensure that we were all signing off of the same sheet of music, if you will. So our emergency plan that is currently in place is currently undergoing a revision at this time to make sure that it is compliant. That is required, by the way, by State and Federal requirements on a biannual basis. That will be completed by October 1st.

Under that system, not only DuPage County but all of our municipalities operate under something called the Incident Management System or IMS. Under that system, there is one technical lead agency that assumes responsibility for any type of hazard that may occur, again whether it is a tornado or a flood or a civil disturbance or, in this case, the Y2K issue.

As we have looked at our primary threats relative to Y2K, the major areas of concern as we look at this issue are law-enforcement-related, so we have addressed that. The sheriff's office as well as local law enforcement are the technical lead in dealing with the Y2K-related problems that we anticipate. This Y2K response not only involves the sheriff's office but will involve a variety of other areas, such as the Department of Human Services and others.

The County Emergency Operating Center, located in Wheaton, will be staffed prior to December 31st and through the rollover of the millennium, to make sure the county is available and is prepared to deal with any type of emergency.

Let me real quickly close with two other areas that we feel are important. One is the importance of community preparedness, individual family preparedness. We realize, as you've indicated, Vice Chairman Biggert, that every person has a responsibility in this issue, not just government, and we are urging through a program called the Family Disaster Preparedness Program that individuals develop emergency plans on their own, that they have emergency supplies that will be available not only for a rollover in a Y2K scenario but any type of major emergency or disaster.

Also, public information. We're working very hard at the county level to make sure every public information officer that represents any level of government within the county has the same information, has up-to-date information so that as they receive informational requests, we can address them.

To close, let me bring up one very important point to ponder. We need to remember that the rollover will occur on January 1st. January 1st, 1999 saw this county as well as much of northern Illinois suffer through a major blizzard, a blizzard that was so large that the President of the United States declared us a Federal emer-

gency area. We need to remember that Y2K does not create snowstorms. And if in fact, as you've indicated before, we prepare for a snowstorm because again this is occurring in the middle of winter, then we ought to be prepared for Y2K.

Mrs. BIGGERT. Thank you very much.

[The prepared statement of Mr. Mefferd follows:]

DuPage County, Illinois Y2K Preparedness Briefing



Testimony Before The Congress of the United States House of Representatives Committee on Government Reform

July 8, 1999

Presented By
Thomas O. Mefferd, Coordinator
DuPage County
Office of Emergency Management

**DuPage County, Illinois
Y2K Preparedness Briefing**

July 8, 1999

DuPage County, with a population of 943,000, is located west of the City of Chicago and Cook County. The County is composed of 34 municipalities and 9 townships. Emergency services are provided to the county's residents by 39 fire departments and fire protection districts, 37 law enforcement agencies, and 10 hospitals. Located within the County are 2 federal energy research laboratories; Argonne National Laboratory and Fermi National Accelerator Laboratory, hundreds of facilities owned or operated by business and industry and a host of multi-national corporations.

The Y2K issue within the County must be addressed on two fronts. First, the County government itself is much like its corporate neighbors. County facilities must continue to function effectively through the change in the millennium. Secondly, the County and its municipalities must be able to continue to provide for the public safety of its residents regardless of what might transpire at the stroke of midnight or other dates involved in the Y2K scenario.

This presentation will address three major issues: internal, external, and public safety issues.

Internally, the county has and continues to conduct reviews of its critical systems. Government, much as in big business, relies on computer systems to process data, generate invoices, manage vital statistics, and ensure continued public safety. Current reviews and upgrades to computer systems and software have resulted in a 99.4% compliance level as of June 30, 1999. Additional life safety systems, including the ability to generate backup power, heat, and cooling, the ability to ensure the safety of detainees in our jail and residents at our Convalescent Center, as well as our ability to produce potable water and dispose of sewage have all been researched. County department heads have reviewed their department operating systems to ensure that they will remain in operation and

services will not be interrupted.

Externally, three major areas were researched. The first major area of concern was to ensure the viability of the utilities within the County. As of June 30th assurances have been received from ComEd - the electric utility, Nicor - the natural gas supplier throughout the County, and Ameritech - the primary land line telephone company that services will be available to consumers. Additionally, the majority of the water used throughout DuPage County is transported by the DuPage County Water Commission. This water is acquired from Lake Michigan, by the City of Chicago, and piped to the DuPage water system. Assurances have been received from the DuPage Water Commission, of whom you will hear from as part of today's hearing, that any valves and other control systems can be manually overridden in the event of a failure. The City of Chicago has assured the State of Illinois that they will be able to pump and purify water for distribution, not only to the City, but to surrounding counties that make use of Lake Michigan water. Additionally the DuPage County Department of Public Works, which operates a small distribution system in the eastern portions of the County, have indicated that their system will continue to function.

The second area of external concerns was the reliability of the County's emergency communications systems used to dispatch law enforcement, fire, and EMS. Assurances have been received from our communications vendors that equipment will not fail. The County however has prepared for failure as described later.

The final external system of concern was the traffic control systems through the County. The County utilizes computerized traffic control systems to operate its many traffic lights. A total of five different makes and models of controllers are used in this application. To date the County, in cooperation with our traffic signal vendor, have field tested each of these five types of controllers. This test involved setting the operating clock to 2350 hours on December 31, 1999 and running the clock until 0010 hours of January 1, 2000. In all cases no interruption of the signals occurred.

The data collected as part of these tests was shared with each of our municipalities to assist them in

assessing their municipal control systems.

Issues related to public safety will address contingency plans, community education efforts, and issues of public information.

The question has been raised. Will the County develop a Y2K emergency plan? The answer is no. DuPage County, like most counties currently has in place an emergency management plan designed to address "all hazards" as required by FEMA. The Y2K issue as one of those hazards. The plan, which mirrors the Federal Response Plan, is currently undergoing a review and update process which will be completed by October 1st. In the event an emergency does arise, the plan will serve as the foundation for County response and coordination of municipal operations. The County and its municipalities operate under the "Incident Management System". Under this system one agency is designated as the "lead agency" and all other agencies support operations. It is the feeling that the major of the demands which will impact public safety under Y2K will be law enforcement related. As such the Sheriff's Office and municipal law enforcement agencies will serve as this technical lead. Other agencies that will be tasked in the event of a Y2K related problem include: the Office of Emergency Management, Department of Human Services, Fire Service, States Attorney's Office, Court System, and area hospitals.

To ensure the County is prepared to respond to any eventuality, the County's Emergency Operating Center (EOC) will be staffed on a daily basis from December 27, 1999 through January 1, 2000. Throughout the week leading up to New Years Eve the EOC will serve as a law enforcement "hot spot command center" where County and municipal law enforcement response can be coordinated if necessary. On December 31st, the EOC will be formally staffed at 1200 hours and will remain staffed until at least 0300 hours January 1, 2000. Staffing will include representatives from law enforcement, public information, human services, the fire service, emergency management, resource management, and the states attorney's office.

In addition to the staffing of the EOC, two field deliverable systems will be staffed. First, in the unlikely event of a failure of the telephone system, four communications vans will be deployed to

strategic locations across the County. These vans will be supported by a variety of radio equipped vehicles that can serve as a point of contact between residents in need of communications and the emergency response community. This emergency communications system was first developed in 1988 as a result of a fire in the telephone switching center in the Village of Hinsdale in southeast DuPage County. During that emergency more than 100,000 residential and business customers had no phone service for almost 30 days. The emergency communications system worked effectively around the clock during that outage. Secondly, the County has developed a trailer carrying cots, blankets, and other supplies necessary to support a 100 person shelter. In the event a shelter needs to be opened this equipment can be deployed immediately to that location. The County and its municipalities are currently re-surveying identified mass care shelters. The primary focus of this survey is to determine if the shelters are equipped with a generator and if so does the generator power the heating, ventilation, and air conditioning system.

Community education is a vital part of Y2K preparedness. Based on a program developed by FEMA, the County is actively endorsing two training programs to educate residents about disaster preparedness. The first, the Family Disaster Preparedness Program, is designed to help residents develop family emergency plans and disaster kits so that they can be self sufficient for a period of 72 hours. This planning is useful for any type of disaster, not just Y2K. The second, the Community Emergency Response Team Program, is designed to educate small residential groups such as homeowner associations, neighborhood watch groups, condo associations, etc., to band together and help one another in the period of time before emergency services can arrive. A Train-the-Trainer program was conducted jointly by the Illinois Emergency Management Agency and the County Office of Emergency Management in June for participants representing emergency agencies throughout the County. Field deployment of these programs will begin shortly.

Effective and adequate public information is also a key area being addressed. At the County level, it has been agreed that all information released to the media would be managed from a single point. This will insure accuracy and continuity. A training / briefing session is currently being planned for all of the public information officers (PIOs) throughout the county including municipal, state, and

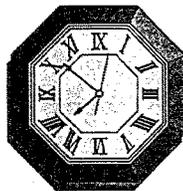
county PIOs. This training session is designed to ensure that all PIOs have the same level of information regarding the Y2K issue and current levels of preparedness.

In summary, DuPage County has been actively planning for Y2K for the better part of a year. As the year marches on, we plan to continue that effort as well as maintaining a close working relationship with municipal, township, and state agencies who partner with us in emergency response efforts.

DuPage County, Illinois
Y2K Preparedness Briefing



DuPage County
Y2K Preparedness Briefing



- Internal Issues
- External Issues and Infrastructure
- Public Safety Issues

Internal Issues



- Review currently ongoing within County structure
- MIS GROUP - computer systems / software
- OEM GROUP - infrastructure items

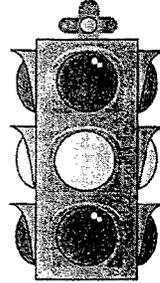
External Issues and Infrastructure



- Utility Reliability
- Public Safety Communications Systems (9-1-1 and Radio Towers)
- Traffic Control Systems

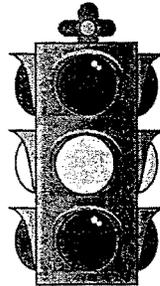
Public Safety Issues

Ensuring public safety requires a joint effort on the part of the government, the private sector, and community residents.



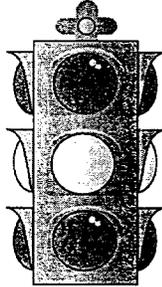
Public Safety Issues

- Contingency Plans
- Community Education
- Public Information



Public Safety Issues ***Contingency Plans***

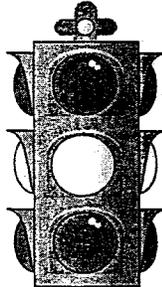
- Existing emergency management structure followed
- Incident Management System utilized
- Sheriff is lead due to potential demand on law enforcement



Public Safety Issues ***Contingency Plans***

Components of current Emergency Plan

- Communications failure - OEM
- Shelter - Dept of Human Services
- Law enforcement and response - Sheriff
- Critical power - OEM



Mrs. BIGGERT. And now Mr. Martin.

Mr. MARTIN. Thank you. Just on a little bit of a background. The DuPage Water Commission purchases water from the city of Chicago for resale to utilities in DuPage County. The commission has water purchase agreements with 25 municipal utilities, Argonne National Laboratory, and one private utility with six service areas. It is estimated that the commission's utility customers provide service to approximately 700,000 people.

The commission has been working on the year 2000 compliance issue for close to 2 years. The two main information systems that the commission has are a supervisory control and data acquisition, known as a SCADA system, and a local area network. The SCADA system is the instrumentation that the commission uses to monitor and control water operations. The local area network serves as the administrative system used for word processing, payroll, accounting, purchasing, and preventative maintenance.

The commission has contacted its hardware and software vendors, and with our testing we feel that our hardware and software is year 2000 compliant.

The commission's operations rely heavily on the Chicago Water Department, Commonwealth Edison and Northern Illinois Gas. The commission has sent Y2K compliance letters to these supporting utilities, and the following are the responses received from these utilities.

The Chicago Water Department has retained a consulting firm to work with city staff to evaluate the issue. Fortunately, the Jardine Water Purification Plant which is the plant that treats our water is in the process of installing a SCADA system and it would appear that their water treatment equipment is not vulnerable to Y2K.

Commonwealth Edison has responded to the commission's inquiry stating that their goal is to finish a companywide year 2000 compliance by the third quarter of 1999. In addition, Commonwealth Edison's Y2K program Website indicates that January 1, 2000 falls on a weekend when electrical demand is relatively low and ComEd expects and plans to have excess generating capacity available at that time.

Northern Illinois Gas has indicated that they have the necessary contingency plans.

The commission is performing the necessary activities to minimize service disruptions due to Y2K problems. The one significant concern for the commission is if there were minor electrical outages at midnight on January 1, 2000. In this event the commission would not be able to close the discharge valves at the 74 delivery points to prevent the distribution system pressure from dropping below the Illinois Environmental Protection Agency required minimum pressure of 20 pounds per square inch. If the distribution system pressure did drop below 20 psi, it would be necessary to issue a countywide boil order. To reduce this possibility, the customer utilities have been directed to have all their reservoirs and storage facilities filled by 11:45 p.m. on December 31st. At this time the outlet valves on the connection points will be closed. The commission will continue pumping at a reduced rate during this period. If there is no interruption in electrical service by 12:30 a.m. on January 1st, water service will resume. This temporary interruption in

service should have no effect on water users because of the requirement for the customer utilities to maintain 2 times average day storage. The water usage during winter months is generally 90 percent of average water usages.

If you have any questions, I would be glad to answer them.

Mrs. BIGGERT. Thank you very much.

[The prepared statement of Mr. Martin follows:]



DuPage Water Commission

600 East Butterfield Road

Elmhurst, Illinois 60126

Phone: 630-834-0100

Fax: 630-834-0120

From: Robert L. Martin, P.E.
Manager of Water Operations

Date: July 8, 1999

Location: Naperville City Hall
400 S. Eagle Street
Naperville, Illinois

Subject: Y2K Congressional Hearing

Year 2000 Readiness Disclosure
Under the Year 2000 Information and
Readiness Disclosure Act, Public Law 105-271

Background

DuPage County is one of the fastest growing counties in the United States. The DuPage Water Commission operates under the 1985 Illinois Water Commission Act, which empowered the Commission to finance, construct, acquire and operate a water supply system to serve municipal and private water utilities in DuPage County.

In 1984, the Commission entered into an agreement with the City of Chicago to purchase treated Lake Michigan water for resale to utilities in DuPage County. The Commission has water purchase agreements with 25 municipal utilities, Argonne National Laboratory and one private utility with six service areas. It is estimated that the Commission's utility customers provide service to approximately 700,000 people. Prior to construction of the Commission's system, utilities within DuPage County obtained their water from deep and shallow wells.

The Commission went into full operation on May 1, 1992. Its present average day demand is 83 million gallons per day (MGD).

Commission Computer Facilities

The Commission has been working on the Year 2000 Compliance issue for close to two years. The two main information systems the Commission has are the Supervisory Control and Data Acquisition (SCADA) and the Local Area Network (LAN). The SCADA system is the instrumentation that the Commission uses to monitor and control water operations. The LAN serves the administrative system used for word processing, payroll, accounting, purchasing and preventative maintenance.

The Commission has taken the following three steps in addressing the Y2K problem:

Inventory – The first process was to identify all systems, software and equipment with computer chips.

Assessment – Determine which of those chips and programs may be Y2K sensitive and test those systems.

Remediation – Replace and repair chips and software, or develop and implement an alternative process that works around the problem.

Commission staff prepares a monthly Year 2000 Compliance Status report. The following is a synopsis of the Y2K compliance to date:

Hardware: At the present time the Commission's vendors have advised that the hardware is Y2K compliant with the exception of some older LAN workstations which will not automatically reflect the proper date on January 1, 2000. Because of the age of these workstations it is our intention to replace them and if they are not replaced by January 1, 2000 we will reset the date.

Software: The Commission's vendors have advised that most of the Commission's software is Y2K compliant except the payroll system. The Y2K compliant payroll system software has been received, but requires Windows NT rather than the Novell 3.12 operating system software presently installed on the LAN. Staff is in the process of converting the LAN to Windows NT.

There are some small miscellaneous software programs that will be corrected for Y2K or replaced. This work should be completed by the third quarter of 1999.

Supporting Utilities

The Commission's operations rely heavily on Chicago Water Department, Commonwealth Edison and Northern Illinois Gas. The Commission has sent Y2K compliance letters to these supporting utilities. The following are responses received from these utilities:

Chicago Water Department (CWD) has retained a consulting firm to work with City staff to evaluate the issue. Fortunately, the Jardine Water Purification Plant is in the process of installing a SCADA system and it would appear that their water treatment equipment is not vulnerable to Y2K.

Commonwealth Edison (ComEd) has responded to the Commission's inquiry stating they their "goal is to finish Company-wide year 2000 compliance by the third quarter in 1999."¹ In addition, the ComEd's Y2K Program Website indicates that January 1, 2000 falls on a weekend when electrical demand is relatively low. ComEd expects and plans to have excess generating capacity available on that date.

Northern Illinois Gas (NICOR) indicated they have the necessary contingency plans in place.

Commission Financial Institutions

The Commission has also sent Y2K compliance letters to financial institutions that we deal with. We are in the process of receiving responses from these institutions. In addition to these letters, the Commission also maintains computer and paper records of its investments to verify information from these institutions.

Backup Generators

There have been inquiries regarding the installation of backup generators at the DuPage Pump Station to provide electrical service in the event there is a loss of service as a result of the Y2K issue. This would be a benefit to the Commission only if the Lexington Pump Station, which supplies water to the Commission and is operated by the City of Chicago, has backup generators. If there was a major loss of power, and only the DuPage Pumping Station had backup generators, the Commission would only be able to pump until the ground storage reservoirs at the DuPage Pumping Station were depleted.

¹ Commonwealth Edison letter dated December 1, 1998

Proposed Action

The Commission is performing the necessary activities to minimize service disruptions due Y2K problems. The one significant concern for the Commission is if there were minor electrical outages at midnight on January 1, 2000. In this event, the Commission would not be able to close the discharge valves at the 74 metering stations to prevent the distribution system pressure from dropping below the Illinois Environmental Protection Agency required minimum pressure of 20 pounds per square inch (psi). If the distribution system pressure did drop below 20 psi, it will be necessary to issue a countywide boil order.

To reduce this possibility, the customer utilities have been directed to have all their reservoirs and storage facilities filled by 11:45 PM on December 31, 1999. At this time the outlet valves on the connection points will be closed. The Commission will continue pumping at a reduced rate during this period. If there is no interruption in electrical service by 12:30 AM on January 1, 2000, water service will be resumed.

This temporary interruption in service should have no effect on the customer utilities because of the requirement that the customer utilities have storage in the amount of two times average day demand. The water usage during the winter months is generally 90% of the average day demand.

Mrs. BIGGERT. That brings us to the questions from the subcommittee and then we will—if you have questions and have not turned them in yet for this panel, can you pass them over and somebody will pick them up.

First of all, I'll ask a couple of questions. Mr. Mefferd, you mentioned about the traffic signs and how many there are. Is it a contingency plan—let's assume the traffic lights all went out. Is it a contingency plan to have all of those lights, or do they already have the type of stop signs that drop down so that you could have a stop sign there or what would happen?

Mr. MEFFERD. The plan is on the county intersections that those stop signs would be installed.

Mrs. BIGGERT. But they have not been now?

Mr. MEFFERD. That is the plan for later this year.

Mrs. BIGGERT. That would be beneficial not only for Y2K but for—

Mr. MEFFERD. Absolutely; any power outage that occurs.

Mrs. BIGGERT. Saturday, I attended a cardboard boat regatta and I thought it was just little cardboard boats that they raced across this lake, but it turned out that they would have as many as 10 people in these boats and the first—one of the first boats was named Y2K Bug, and I have to say it was the first boat that sank. So I hope we have sunk the bug and taken care of all of our problems. But it was a nice bright yellow boat, but it didn't make it even out of the starting box, as I recall. I think maybe we have solved all the problems.

Ms. Reynolds, what are you doing, in the message at the public forums, are you recommending that people take precautionary steps?

Ms. REYNOLDS. The public forums are really intended to get a sense of what's going on around the State so we have asked the community colleges around the State of Illinois to in fact host their community leaders and we will bring a State team in then to help moderate, to provide information, and to really organize and structure the events. But our message really is to what the State is doing, and then to find out how the communities are in fact preparing, and it really involves a panel such as you've organized today.

But it also is, I think, incredibly important to make sure that the public knows how their own community leaders are preparing and then to offer suggestions as we would again with any winter storm. This is in the middle of winter. It is Illinois. Just make sure you are taking precautions as you would for the spring tornado season as well.

So it really isn't a message of make sure you've got your basement full of food. It really is a message of take reasonable approaches to your own preparations, but we want to make sure that you know where your local governments are. It is also a way for us to assess where we need some State resources or some State attention in regional areas of the State or in specific communities that may need additional help.

Mrs. BIGGERT. Thank you.

Mr. Carlsen, what are you doing to communicate your message to the residents?

Mr. CARLSEN. We've started what our community relations people have termed a 3-pronged approach on using newsletters that are sent out to all residents. We've already sent one out. We have a copy of the original newsletter that was sent out as one of the handouts. Our Website is really a big focus. Naperville has a lot of people who have computers or have access to the Web, and that's where we've pointed them.

Newspaper articles through the press. They've been really good with us as far as talking to us about what's going on and there's been a lot of really good articles done that way. I think those are the three main areas that we've used but we also communicate at each council meeting through an FYI device to the council to let them know where it is at and also that those agendas are available to the public as well.

Mrs. BIGGERT. Do you have a budget for what's been spent on the Y2K?

Mr. CARLSEN. Yeah, we do. We've spent about \$600,000 to date. That's actually kind of low for a city our size, but the reason that is, is because a lot of our normal replacement programs have funded a lot of the replacement of computers that would not have been compliant but they weren't done for compliance sake. So \$600,000 was spent strictly as a result of things that were not compliant.

Mrs. BIGGERT. Thank you.

Mr. Martin, have you recommended contingency planning for municipalities in case there is an interruption in your services?

Mr. MARTIN. We have not. We don't feel there will be a problem and if there is, as I've indicated, a minor electrical problem because of the 2 times average day storage that they're required to have, that problem should be resolved before the water is used up in storage.

Mrs. BIGGERT. So you are really putting your percentage at 100 percent that there's not going to be—

Mr. MARTIN. Yes.

Mrs. BIGGERT. Good. Positive thinking.

Mr. Willemsen, you have kind of the overview of the whole situation and have done so much with the Federal agencies. Do you think that maybe just people here would like to know if you think that all the Federal agencies will be compliant by our next deadline? As you know, Mr. Horn gives pretty tough report cards to the agencies, and I think that's based on your work.

Mr. WILLEMSSEN. I would say overall I'm much more optimistic today on where Federal agencies stand compared to a year ago and much more optimistic compared to 2 years ago, in large part because of the oversight done by Chairman Horn and his subcommittee. There has been much more urgency on the part of top Federal leaders to address Y2K that, frankly, we didn't see 2 years ago. I can remember hearing in July 1997 with the Office of Management and Budget indicating that they didn't think this was a major issue. Shortly thereafter they changed their tune and so has senior Federal leadership, so I'm more optimistic today than I was at that time.

Nevertheless, as I mentioned earlier, there are some major risk areas among Federal programs that have to be addressed. As Chairman Horn indicated in his most recent grading session of the

43 high-impact programs, the data supplied to the subcommittee only indicated that 2 were ready and 41 were not, and it is July 1999. So there is still a lot of work to be done, and I don't think Federal agencies can rest easy until it is done.

Mrs. BIGGERT. Thank you. Those are my questions.

Chairman Horn.

Mr. HORN. I'm going to ask a couple for the panel in general, and just if anybody is willing to respond to this. If you had to do this over again, what have you learned that you should have done first after you've gone through this exercise—not that we'll go through it again, maybe? I would like to get your wisdom after you've dealt with this for months or even years. Any thoughts? Let's just go right down the line.

Mr. WILLEMSSEN. I'll offer a couple of comments. I think if we're starting over again, one thing we've learned is where the emphasis needs to be. While systems are important and we have to address the computer systems and address the 2-digit problem for the year in those systems, we probably should have earlier on had more of an emphasis on providing programs, functions, and services to the public. Because the bottom line to the public is they don't really care if the system works. What they care about is that they get their benefit or their service that is expected. That kind of emphasis, at least from a Federal agency perspective, didn't occur until this year so that was a little late.

Second, I think the other thing that's been learned is when many went into this Y2K issue early on, they thought of it primarily as a mainframe problem and as they started peeling the onion, they found out it was much bigger than that. There was little discussion a few years ago about drinking water and wastewater, little discussion on telecommunications, electric utilities. It was predominantly talking about old IBM mainframes and COBOL. As more work was done on Y2K, we quickly understood that it was a much broader problem in scope and that's something that I think if we could have done that earlier would have been beneficial.

Ms. REYNOLDS. My only regret is not having started on this earlier. We only took office 6 months ago, so I wish we would have been in office last year to be able to address this a little earlier. But at this point I really have no regrets. We have done exactly what he suggested of taking a functional approach to government and services.

I didn't feel like I honestly could have gone to the Governor and said three critical systems may not be compliant, Governor. He would have said, "What does that mean? I want to make sure the services of State government can in fact be delivered. Period." So that's what our approach has been. I really have no regrets to this point.

Mr. HORN. Mr. Carlsen.

Mr. CARLSEN. I would echo that sentiment. We started in 1997 and involved about 20 or 30 employees over the term of what we've done. I think we didn't take a functional approach at the beginning. I think that might be something I would say that I wish we would have done and we've done more of that now. I think that's because we focused on systems. That's what we're trained to do. When we moved on those things and got some of those things out

of the way, we were able to move on and start taking a higher level approach as far as functionality. That would have been nice to start that way.

Mr. HORN. Mr. Mefferd.

Mr. MEFFERD. I think in the same light, one of things we're fortunate about in this county is we have a good working relationship between the county government and our municipalities. One of the real benefits we have reaped from this, and I can't say we want to go back and do it over again, but we have opened some doors relative to closer cooperation not only with the government agencies but more with the private agencies, and we've found ways to better coordinate and better cooperate not only for this emergency but others.

And I guess we can always say if we had more time to do more of it, we could come up with a perfect world. I think the more time we are in preparation for any disaster or a major emergency event, the better off we can be prepared and better ensured of public safety. That's our ultimate goal.

Mr. HORN. Mr. Martin.

Mr. MARTIN. We have with our water system a pretty sophisticated instrumentation system, but we've always taken the approach that at some time the system might not operate. So we've always tried to prepare ourselves with contingency plans in the event that we don't have a working control system and so we really had—it was just modifying our systems for the year 2000, but we had already come up with contingency plans and we just modified them.

We're a newer agency so we have the advantage there in that we were able to include this in the original design but we really haven't—I don't think there would be anything that we would really do differently.

Mr. HORN. Ms. Reynolds, since you are the chief technology officer for the State of Illinois, let me ask you to what degree has the various Federal programs that the State administered and Federal agencies been in touch with you and are the interconnections being made that have to be made once they give you the money you administer it? What's happening on that front?

Ms. REYNOLDS. We have had several teams of Federal auditors in Illinois that I have met with as a State perspective, and then they have been going over individual agencies' programs. Just this week I have spent another day with a second team from HCFA to go over, in fact, the Medicaid programs with our Department of Public Aid and our Department of Human Services. So they have been very thorough and they have been very supportive of our efforts and there's been a nice coordination.

About a month ago I spent a day with the FEMA regional meeting of 6 States and that was a very productive day as well, and they had all the Federal agencies represented there as well. And about 2 months ago I was invited by the Chicago Federal Executive Board, which is a conglomerate of all the Federal agencies in this region, to work with them on Y2K efforts. So there's been extremely good cooperation both among the Federal agencies and the State government as well as, I might add, the city and municipal governments.

The one in particular that I'm working with on a weekly or monthly basis is the city of Chicago. And we are working with them very closely and I would echo really this has been—Y2K is an opportunity to strengthen those types of relationships. And it's also been a great opportunity to get a better sense of inventory, I think, than certainly government and probably private industry has ever had in terms of technology. So I really look at it as an opportunity to work with the Federal agencies on a day-to-day basis in the future beyond January, hopefully.

Mr. HORN. I think that's very well said. You are absolutely right. If nothing else comes out of this and we get improved Federal, State, and local cooperation, I think it's been an exercise worth having done.

Let me ask you, what is the major mistake that you think people have made in this area and you'd try to remedy that again? So you don't have to confess yourself, but just from what you hear and see in terms of other governmental entities and other States. You are all parts of States' associations.

Ms. REYNOLDS. The biggest mistake, I think, is people aren't communicating the full ramification of both their efforts or their remediation plans, and I think the general public is just scared. I mean, they're generally skeptical of the government "I'm from government, I'm here, you can trust me" kind of attitude. So I think people are generally skeptical and they want to see details.

Whether they use that detail I think is immaterial. It is important to me that we communicate very openly about where we're at. I've told the agencies I don't want you to lie. If the truth is bad, I want to know the truth. It doesn't matter to me whether you'll be done December 31st or July 1st. To me, I want to know the truth in where you're at. Because I think that's critical to how the public reacts to that preparation. So I think the biggest mistake people have made is not communicating the full truth or the full story.

My other sense is that people haven't taken it seriously in all areas or all levels of government or public utilities. I think the larger facilities and the larger companies and the larger municipalities have certainly done an admiral job of addressing the issue. But I think there are some smaller communities, smaller companies, smaller businesses, that have in fact not taken it seriously and may not have the staff or the resources to do much about it, and those are probably the links in the chain that I'm most concerned about.

Mr. HORN. That's well said. Does anybody have another point they'd like to make before I get into the audience questions?

Let me start on the audience questions, and it comes at a very good time. Mr. Martin, you are the manager of water operations for DuPage County Water Commission. The first question here is, Will the toilets flush? This is by, obviously, a practical person in the audience here who is in touch with reality.

Mr. MARTIN. Yes, they should. I know one of the concerns that people have with the fact that we're going to stop providing service to our municipal customers, but they have again—and that's the reason you have water storage is so you can operate during interruptions in electrical power service.

I don't anticipate anything going wrong with the water system because we've been told by the electric utility that we should have electrical service. Things can happen and that's why we maintain the 2 times average day storage so we can survive periods of time without electricity. So I think you can flush your toilets.

Mr. HORN. Well, that's helpful. I take it the water I'm drinking is under your commission's jurisdiction?

Mr. MARTIN. Yes. Isn't it good?

Mr. HORN. I must say, it is a great pleasure for all of us to get out of Washington where we have to use bottled water. And yesterday in Topeka, and now Naperville, we've got great water. I keep drinking it all the time. But back there we have wonderful reservoirs and everything that the Corps of Engineers built in 1859, but the city of Washington hasn't upgraded our distribution system since 1859. And we decided, I guess when x rays started showing metal in our bodies, that we would get private water, although the L.A. Times series says there isn't much difference. I envy you with decent water out in the hinterlands, so keep it coming.

Mr. Willemsen of GAO, maybe you can explain to an individual in the audience, What's the difference between Y2K OK, Y2K ready, and Y2K compliant?

Mr. WILLEMSSEN. Those terms have been thrown around loosely by many different organizations and you really have to rip away the detail behind the definitions to clearly understand what they are. I think, for example, the State of Illinois testified that their definition of compliance includes making sure that all the exchanges have been thoroughly addressed. Other organizations do not do that before deeming their systems compliant. Other organizations just simply look at the application code and once that's fixed, they view their system as compliant, irrespective of whether the supporting hardware and operating system are compliant.

So I think it is a valid question. It is one of the issues that in the guides that we initially put out in draft form in February 1997, we said an organization, one of the first things you need to decide is defining what you mean by Y2K compliant and making that definition clear to all, because there continues to be a wide variety of definitions used by differing organizations.

Mr. HORN. The next one I think is also directed at you. Since there's a vast quantity of items that are imported along with the crude oil and some foods, how will Y2K affect these supplies after January 1, 2000, the foreign countries being much further behind and transport being suspect?

Well, you are absolutely right on both refinery and oil and other liquid resources. There are problems with microchips on a lot of the tankers, and there's also a lot of them on the pipelines. Let's take Russia, for example. Mrs. Biggert mentioned the snows in January here. Russia provides most of the natural gas for eastern Europe and parts of central Europe, and if their pipelines go down because of malfunctions due to the particular microchips they have in either diverting it in certain pipes and in certain methods and the particular refinery ships, they will have some real problems in central Europe in freezing at that point in the year. Now, this was what happens afterwards. Hopefully things will get back to normal afterwards.

Mr. Willemsen.

Mr. WILLEMSSEN. I think that's a very valid issue, one that we've done some work on, and one that we've made some suggestions to John Koskinen, the chairman of the President's Y2K Council. In particular, the oil issue was one of concern to us.

Because of the many unknowns surrounding other countries' readiness on their oil production and distribution system and because of our heavy reliance on imported oil, we had recommended to one of the working groups of Mr. Koskinen that they put together some credible national-level risk assessments and develop national-level scenarios and contingency plans in the event that there was a disruption with oil imports, and put those contingency plans together so that they can be ready if that disruption occurred. They agreed with those suggestions. They are in the process of putting together those contingency plans so that in the event the disruption occurs, that there will be some backup plans in place.

Mr. HORN. Next question is directed to county officials and some local officials. It says: I called the DuPage emergency group and the Kane County to request a representative to speak to a local government group. Both said they weren't getting involved till the end of August. Why?

Mr. MEFFERD. I think we have in fact been speaking on a regular basis to various groups. I'm not aware of any specific request that came in. I would be more than happy to respond to that.

Mr. HORN. We'll point that anonymous person and push them in the direction of Mr. Mefferd. I think we all agree that the sooner we get information out, the less rumor and panic and the rest of that nonsense, and people wanting to make a living on misery, writing books; and now you mentioned the movie that I guess is starting in "Melrose Place" or something, Beverly Hills—what's the difference? OK.

Mr. Willemsen, State contingency programs at National and State levels must go on through testing. I understand testing is considered 60 percent of the work. If so, we're in trouble. What do you think on that?

Mr. WILLEMSSEN. I think there is reason for concern on some of those State administered Federal programs, especially where we see completion dates targeted for the fourth quarter of 1999. And what we've seen to date, at least Federal agencies, is very typically underestimation of the amount of testing that's required. And cutting that a little finer, it's the amount of effort involved in resolving the problems that result from the testing. So when we see those fourth quarter 1999 completion dates, it is cutting it very tight.

And in some cases the fail date is not January 1, 2000. In some cases it will be October 1, 1999. In the case of State unemployment insurance agencies, we had a fail date of early January 1999 and four States and territories actually didn't have their systems done in time and had to implement a contingency plan. So I think there is a reason for concern in that area.

Mr. HORN. The last question from the audience—the others will go over to panel 2 where they're more pertinent. Ms. Reynolds states that Illinois provides more information on Y2K compliance

than any other State. Where does this information go? I haven't seen much.

And no matter how many times we always can say something in any agency, Congress, executive branch, States, we don't reach everybody; and one person wisely said, When you are tired of saying it about the 100th time, that's just when you begin sinking through. So what's the State of Illinois doing to do this? And when bills are sent out by city, county utilities, I would think that's one good way to get the message out.

Ms. REYNOLDS. I hadn't thought about it till now. Property tax notices are due all over the State right now. We probably should have sent it out with the property tax notices.

In terms of public information, we've certainly put out press releases this spring and the beginning of the monthly reports, once we got the report redone and enhanced in the way that I have suggested. But it is all available. The monthly reports are downloadable on our Website which is www.state.il.us/y2k. It is available off the State home page. It is also available in printed format through our office, the Governor's office. We'd be glad to supply that to anybody who requested it.

It's also been made available to the media throughout the State and there simply has not been a lot of coverage on it. My suspicion is this fall when people begin to get back to school and focus on the end of the year, I think there will be more public attention to the matter, but we have in fact tried to provide it. It is a fairly lengthy report in terms of our monthly report. This summer we'll be doing a pamphlet and we'll be providing more, smaller packets of information available to people in terms of a very public way statewide.

Mr. HORN. Your suggestion on the schools is fine. How about the libraries throughout the State?

Ms. REYNOLDS. Anybody can get access to the Internet and access to the home page through their libraries. That is one way to access the Web page, certainly. The libraries, in terms of their preparation—is that your question?

Mr. HORN. Yes. People ought to know—I think you were wise if we could have gotten it on that property tax. That's a good idea.

Ms. REYNOLDS. I just thought of it right now. People probably wouldn't have been appreciative of State information in their tax bills. That's not always one of their favorite pieces of mail they receive. But at any rate, we will try it this fall and try through public service announcements and through other avenues. Our intention is to try to get information out through numerous avenues this fall.

Mr. HORN. I think you've got to remember that most of the citizenry do not know how to work a computer. Not everybody is going to get into the Worldwide Web so we've got to reach them another way.

Thank you very much. Appreciate it.

Mrs. BIGGERT. I would like to thank the entire panel. I think that your testimony and your comments were very helpful to us, and we really appreciate your taking time out of your busy schedules to come. So I will excuse this panel and we will call the second panel up. Thank you very much.

If you'd all like to stand, I'll administer the oath.

[Witnesses sworn.]

Mrs. BIGGERT. I think for this panel I'll introduce you one at a time so that the audience will be able to have a better background as you start.

Our first panelist of the second panel is Alan Ho from Commonwealth Edison. He's going to review how Commonwealth Edison is becoming or is Y2K compliant. Thank you very much.

STATEMENTS OF ALAN D. HO, Y2K CORPORATE MANAGER, COMMONWEALTH EDISON; DALE JENSEN, DIRECTOR, Y2K CUSTOMER COMMUNICATIONS, AMERITECH; CRAIG WHYTE, DIRECTOR, REGIONAL COMMUNITY RELATIONS, NICOR GAS; PHILIP PAGANO, EXECUTIVE DIRECTOR, METRA; AND GARY MIELAK, VICE PRESIDENT AND CHIEF TECHNICAL OFFICER, EDWARD HOSPITAL

Mr. HO. Good morning. Thank you for the opportunity to testify here today. I had testified last September and stated a few things. I would just like to go back to that, just to provide some continuity.

We at Unicom and ComEd recognize the important role that we play in this whole Y2K issue, and indeed last September I stated that if we are unsuccessful in our readiness efforts, why then the readiness efforts on the part of others would really go unnoticed. I'm glad and pleased to state today that as of June 30th, Unicom and the ComEd company is Y2K ready.

And so what do I mean when I say that? That includes all Unicom companies, ComEd's nuclear stations, ComEd's fossil generating systems, our transmission and distribution system, our enterprise wide mainframe computer systems and applications. It includes our distributed computer operations, our local area and wide area networks, our office facilities, and our supply chain.

Some of the activities that we've undertaken this year to increase the certainty of our readiness and strengthen our readiness include independent verification and validation activities where we've hired third-party reviewers to come in and review our management process as well as dig into the computer code that's been renovated and remediated as well as the embedded systems work.

We've also had peer reviews by other utilities come in and review our work and we've reciprocated by going to those other locations as well to provide lessons learned and share information.

Another activity we undertook this year to further demonstrate our readiness is performed numerous integration tests. This year alone we've performed over 90 integration tests on our electric operating system. That includes our generating stations as well as our transmission distribution system and our computer systems. These are date rollover tests that we've conducted with dates including this year, the year 2000, and into the year 2001. Again, these tests are tests that were performed on our actual systems, not computer simulations, actual tests at our plants and our facilities.

Third, the fact that we are today Y2K ready, we need to maintain a vigilant position. We have instituted a Y2K moratorium starting on July 1st to manage the risk and maintain our readiness. We've implemented a clean management program and a program that requires senior officer approval to make any changes to

our computer systems and our embedded systems. So there's very tight control. Because we've worked so hard to make our systems Y2K ready, we want to keep it that way through the rollover period.

Last, we have prepared numerous contingency plans and have developed what I call an operating plan, which I will use to run our Y2K command center on New Year's Eve. Basically, it will be our playbook that will guide us through the various scenarios that we've developed. And between now and then, we will be practicing monthly exercising and practicing getting ready for our September nationwide drill that will be coordinated through NERC, and there's also a drill that we're helping with the NRC in October, all in preparation for New Year's Eve.

Last, I would like to offer a practical tip for our 3.4 million customers. I would just ask that our customers keep to their normal electrical usage pattern. The reason for that is having a predictable load pattern will allow us to avoid any additional challenge that may come up on New Year's Eve.

I would be glad to answer any questions that you might have. Thank you.

Mrs. BIGGERT. Thank you very much for your testimony.

[The prepared statement of Mr. Ho follows:]



Briefing Package for
Year 2000 Public Meeting
&
Tour of Braidwood Nuclear Plant

212

for
Rep. Judy Biggert (R-IL), Rep. Stephen Horn (R-CA)
and NRC Commissioner Diaz

July 8, 1999

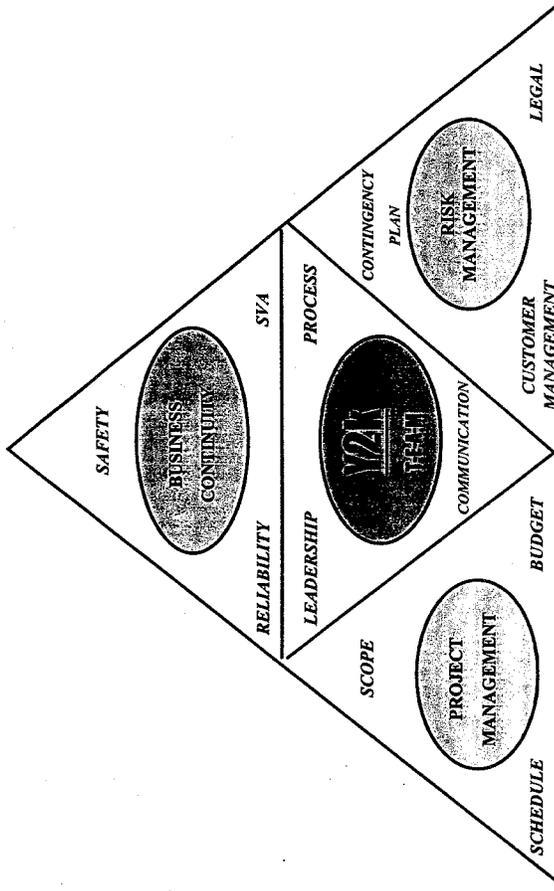


PROJECT STATEMENT

The Year 2000 Project will plan, manage, and coordinate the activities to ensure Unicom's computer systems and related processes will continue to function correctly when processing dates within and between the 20th and 21st centuries.



UNICOM Y2k PROJECT STRUCTURE





SUMMARY OF ASSETS / PROJECT HIGHLIGHTS

UNICOM ASSETS

Generation Resources:		9,407	10 Units	50%
Nuclear				
Fossil	8,324	24 Units	43%	
Peakers	1,407	73 Units	7%	
TOTAL	19,138 MW	Net	100%	

T & D System Make-Up:

765 kV	90 miles
345 kV	2,468 miles
138 kV	2,708 miles
69 kV	185 miles
* Utility Interconnections	- 8

Customer Statistics:

3.4 million customers		
Northern 20% of Illinois - 11,525 square miles		
Peak Load Records		
Winter	14,222	1.5,99
Summer	19,212	8.14,95

Y2K PROJECT HIGHLIGHTS

- Project began in mid-1996
- At its peak, the Year 2000 Team was comprised of over 300 employees
- 15 million lines of code analyzed
- 30,000 embedded systems / only 5% required replacement throughout the Company
- Types of computer systems included in the project:
 - Mainframe & distributed systems
 - Custom developed applications
 - Vendor supplied systems
 - Network & telephone systems
 - Control systems and instrumentation
 - Building services & facilities management
- Contingency Planning was a part of the project as Year 2000 scenarios were incorporated into existing Company contingency plans
- Communications outreach in place since March, 1997

NGG SUMMARY OF ASSETS / PROJECT HIGHLIGHTS

NGG ASSETS

Generation Resources:

Braidwood	2240 MW	2 Units	24%
Byron	2240 MW	2 Units	24%
Dresden	1588 MW	2 Units	17%
LaSalle	2156 MW	2 Units	23%
Quad Cities	1183 MW	2 Units	12%
TOTAL	9407 MW	10 Units	

Embedded Assets:

Site	Total Assets (Excluding Software Apps)	Leave As-Is	Requiring Detailed Assessment	Assets Requiring Remediation
Braidwood	2,181	2,066	715	109
Byron	2,179	6,995	281	70
Dresden	4,443	3,051	326	60
LaSalle	2,115	1,317	1,205	19
Quad	1,722	1,497	315	34
TOTAL	26,175	16,083	4,092	102

Software Applications:

Facility	Total Assets	Leave As-Is	Retire	Remediate	Replace
Braidwood	152	70	54	24	14
Byron	312	13	17	34	3
CTEAM	67	152	495	64	29
Downers Grove	174	84	22	56	12
Dresden	179	73	36	37	13
LaSalle	52	15	11	24	2
PTC	199	72	44	68	15
Quad Cities	156	42	60	47	7
Zion	1934	585	763	480	106
TOTALS					

Y2K PROJECT HIGHLIGHTS

- Five-Phase Project began in mid-1997
 - 1) Inventory
 - 2) Assessment
 - 3) Remediation
 - 4) Test
 - 5) Notification
- Status ~
 - ~20,000 embedded assets reviewed / 400 affected
 - ~1,900 software programs and assets were inventoried / 200 unique applications representing 586 users required Remediation/Replacement

Significant Embedded Assets Requiring Remediation

- Radiation Monitors
- Process Computer
- Diesel Generators (non-safety related)
- Sequence of Events Recorders
- Security Computer

Significant Software Applications Requiring Remediation

- Radiation Area Protection System
- Emergency Response Data System
- Power Flex
- Safety Display System
- A-Model Dose Project



KEY PROJECT DATES

June 8	NRC Pre-walkdown of Braidwood with Regional Administrator
June 23	NEI Conference
June 29	NERC Honor Roll announced
June 30	Unicom Declared Y2k Ready / Press Conference
July 7	5th Key Customer Forum
July 8	Congressional Testimony/Field Hearing Commissioner Diaz visit to Braidwood
July 31	IEMA State-wide Drill
September 8 -9	2nd NERC drill / 6th Key Customer Forum / Y2k critical date (9.9.99)
October 1	Unicom Y2k Operating Plan Finalized
October 15	NRC Desktop Exercise
November 11	7th Key Customer Forum
Dec. 31 - Jan. 1, 2000	Key roll-over weekend
February 29, 2000	Y2k critical Date

Year 2000 Public Meeting: July 7 & 8, 1999

Year 2000 Readiness Disclosure

Unicom



KEY ACCOMPLISHMENTS & 1999 INITIATIVES

KEY ACCOMPLISHMENTS

- All Nuclear Stations are Y2k ready
- All Fossil Stations are Y2k ready
- Transmission & Distribution systems and computers are Y2k ready
- Enterprise-wide Mainframe applications and systems are Y2k ready
- Distributed Operations (LAN, WAN & related systems) are Y2k ready
- All office facilities are Y2k ready
- Mission critical products and services of our supply chain are Y2k ready
- Completed Independent Verification & Validation by 6.29.99
- The NRC conducted a Year 2000 readiness audit of the Braidwood Nuclear Plant and reviewed the Nuclear Generation Group's contingency plans
- Contingency Plan / Operating Plan is Y2k ready - submitted the company's Contingency Plans to the North American Electric Reliability Council and Mid-America Interconnected Network
- Implemented "Clean Management" procedures to ensure newly renovated applications & inventory remain Year 2000 Ready

CUSTOMER MANAGEMENT

- Established a Corporate-wide communications program in March of 1997 to share information with all of our customer segments:
 - > Conducted four Year 2000 Forums for business customers and municipalities
 - > Conducted Media Briefing for local and national media
 - > Completed Year 2000 training with our Energy Services Account Managers and Public Affairs Directors so they can provide project information to customers
 - > Y2k Communications staff receive regular project updates and periodic training
- Disseminated project information to customers via the Unicom web site and "The Source" bill inserts
- Provided interviews to the Chicago Tribune, Chicago Sun-Times, Daily Herald, WNNB, WTTW, Business Week, WLS, New York Times and numerous other local media outlets
- Provided project updates to the City of Chicago, Illinois Commerce Commission, Illinois Energy Association, Securities and Exchange Commission, North American Electric Reliability Council, Nuclear Energy Institute and the Nuclear Regulatory Commission
- Provided testimony to the Congressional Subcommittee on Year 2000 in September of 1998

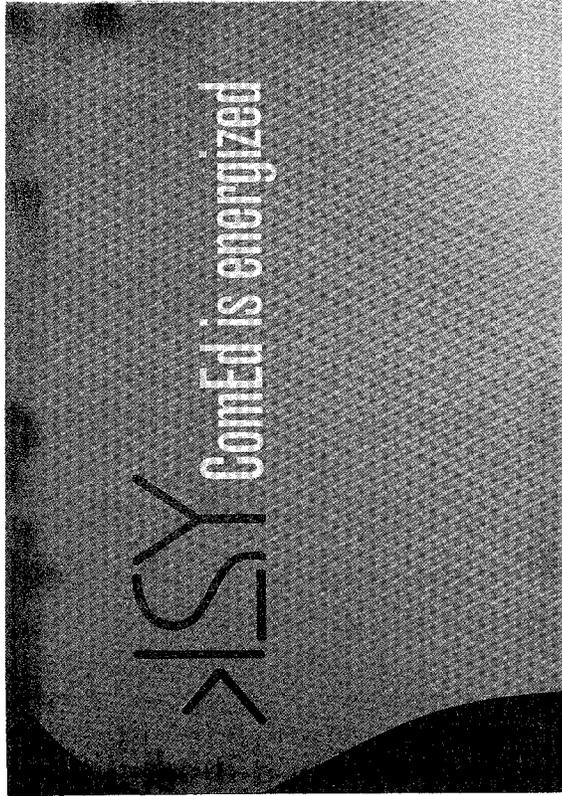
1999 INITIATIVES

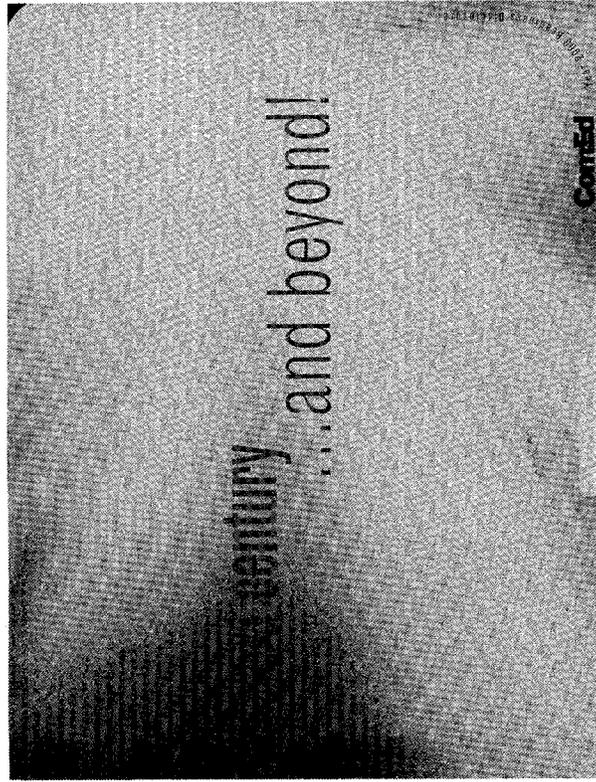
- Complete remediation efforts
- Finalize contingency planning efforts (complete company operational plans and internal drills / participation in two industry-wide readiness drills)
- Perform integration testing to ensure systems are Year 2000 ready
- Increase information sharing efforts with all customer segments

Increase Certainty, Strengthen Readiness → Demonstration

Unicom







How good is a factory electric service?

Most of us take electricity for granted. We rarely think about it, with the exception of a power outage. In fact, there are hundreds of thousands of software programs that must be checked for bugs. There are also millions of individual computer chips within the various equipment used to generate, transmit, and receive information. It is not, as you might think, a simple matter to ensure that the information that we are known as "unbuffered data"

What is the Y2K problem?

When the first computer programs were written in the 1960s and 1970s, years were represented by two digits (99) instead of four (1999) in the computers' coding. Next year, some computers and their applications may not be able to process the date change from December 31, 1999 to January 1, 2000. In other words, certain computers, software programs and other types of electronic equipment might mistakenly recognize the year 2000 as the year 1900. This potential problem is what is known as the Millennium Bug or... Y2K.

Millennium Bug?

and must also be checked. The challenge for electric companies and ConEd's 150,000 customers is to ensure that the information that we are known as "unbuffered data" is not lost or corrupted. At ConEd, we have been aggressive in our identification of which computers, systems and equipment have potential Y2K problems. And, we fully expect that all systems will be ready for the year 2000. Our work is not done, however. We are continuing to identify and address any potential Y2K problems and the implications for ensure that all of our systems will be able to accurately process dates from this century... and beyond.



EC-338-302

n your side
you'll be ready for the new millennium.

Electricity is a critical part of our lives. It powers our homes, businesses, and industries. It's the lifeblood of our modern society. As we move into the new millennium, we need to ensure that our power systems are reliable and secure. That's why we're working together with other industries to help maintain the stability of the electric grid during the transition to the year 2000. Through utility information-sharing programs, such as the Electric Power Research Institute (EPRI) and the North American Electric Reliability Council (NERC), we are able to learn from each other, identify potential problems, and develop solutions to avoid any pitfalls. Along with the rest of the utility industry, we've been working hard to identify and correct any potential Y2K concerns. And we are confident that our customers will have a smooth and safe New Year's Day 2000. Electric companies spend every day planning for the unexpected: storms, high winds, tornadoes, excessive temperatures, ice and snow

can all affect the supply of electricity. Our past experiences, combined with our long-term planning, have allowed us to develop an expertise for aggressively identifying and correcting any potential failures. We fully expect to have a plan in place to continue our efforts to effectively anticipate problems and address them as they arise.

And remember, it's a team effort. One of the challenges facing the electric industry requires cooperation between the industry, government agencies and customers. It's critical that utilities and customers communicate with each other about their Y2K plans and programs. For instance, severe disruptions could result if too many customers suddenly shut off equipment at 11:59 p.m. on December 31, 1999 (without having their local utility shut them all back on again at 12:01 a.m. on January 1, 2000).

The best thing to remember is not to suddenly change your habits and routines. The way we'll all be able to safely and effectively prepare for the Year 2000.



With ComEd o

we'll get down to business for the Year 2000.

We take great care in providing our business customers with innovative products and services that add value to their assets. That's why meeting the challenge of the Y2K has become a top priority as far back as 1996.

Our Year 2000 project is just one of many initiatives that will enable us to continue delivering our business customers' services and products into the next millennium and contribute to the mission of becoming a leading provider of services.

For example, we have created an outreach program to communicate Year 2000 project information to all of our customers. In September of 1998, we began hosting a series of Year 2000 forums to provide regular status updates on ComEd's Year 2000 readiness and give our business customers an opportunity to ask questions relevant to our Y2K program.

Meeting the Y2K challenge also requires a team effort from utilities both large and small, as well as from the customers and suppliers of each. That's why ComEd has taken a strong partnership approach in helping to ensure that our suppliers achieve Year 2000 compliance for their own internal programs.

All of our most critical suppliers have been contacted regarding Y2K certification of products and services. Our

over all supplier approach involves risk analysis, product review & testing as well as contingency planning. This team approach is designed to ensure that none of us experience any interruption of product or service to our customers, and we are well on our way to making the transition to Year 2000 a smooth one.

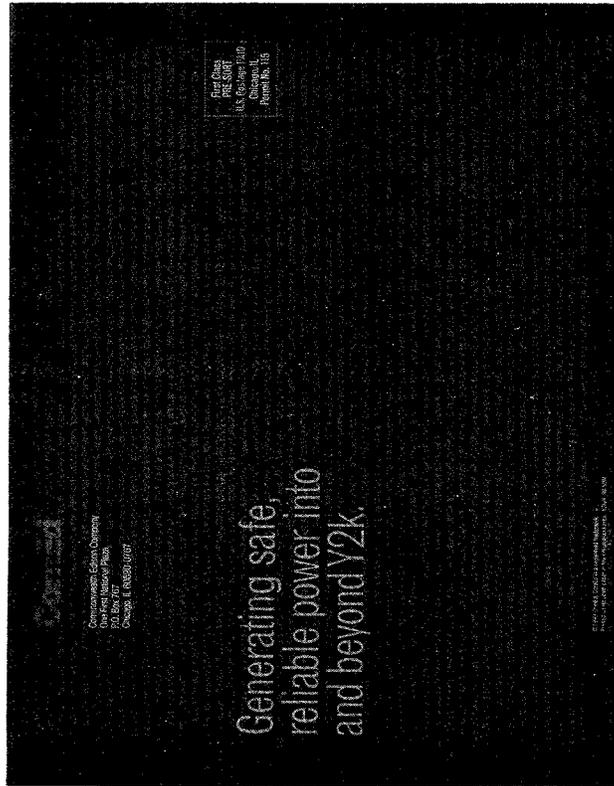
60-939 3C3

At ComEd, we answer to our customers.

How widespread is the V2X problem?
 V2X is not just a recent industry problem. Major incidents in past years and the growth that have been working to address V2X concerns. The utility industry is working with other entities, such as, time communications and data providers, to work to improve the reliability of their systems. This includes increasing the number of vehicles that are equipped with V2X capabilities. The following are some steps that can be taken to address problems that are due to a V2X problem that is identified.

Will ComEd have an impact on the industry?
 Yes. The industry is working to address the problem by increasing the number of vehicles that are equipped with V2X capabilities. ComEd will be continuing to prepare and carry out its policy plans and participate in NERC efforts throughout the remainder of the year.

00-333 305



Compassionate. Edson Company
500 West Lawrence Plaza
Chicago, IL 60680-2077

Generating safe,
reliable power into
and beyond Y2k.

Page One
Chicago, IL
Chicago, IL
Page No. 15

PHOTO COURTESY OF EDSON COMPANY. DATE 10/99

6C-939 3C9

Mrs. BIGGERT. And now we have Dale Jensen, Ameritech director, year 2000 customer communications. Thank you.

Mr. JENSEN. Good morning, Vice Chair Biggert, Chairman Horn. Thank you for inviting me to present testimony on Ameritech's activities to address year 2000 issues within our company. In the interest of time, I propose to direct my testimony to the following five areas: The scope of our initiatives; the identification and status of key areas of the initiative; additional readiness activities underway at Ameritech; our participation in industry year 2000 readiness activities; and some tips for consumers, courtesy of the Federal Communications Commission.

We began our year 2000 initiative at Ameritech in 1996. Throughout our efforts, our overriding goal has been to make the year 2000 event transparent to our customers by working to ensure that the products and services we provide avoid material problems associated with the year 2000.

Our year 2000 initiative includes reviewing more than 2,500 products and services; remediating an IS portfolio of approximately 1,000 applications; upgrading 1,400 host and remote switches; analyzing and preparing thousands of desktop and office components; and preparing the access and security systems, heating and cooling plants, alarms and elevators in over 12,000 buildings and equipment vaults.

A major component of Ameritech's year 2000 initiative is ensuring that we address and resolve any year 2000 issues within three critical areas of our business.

The first area was our network infrastructure; which includes our local exchange, cellular paging, advance data services, video and long distance networks.

The second area is our information services infrastructure, which includes the information services hardware; applications, and operating systems that enable us to conduct the day-to-day operations of our business.

And the third area was our operating infrastructure; which includes items such as real estate properties that we occupy as well as employee support tools such as desktop personal computers.

Having broadly defined the critical areas of our initiative, I would like now to discuss the status of each of those areas as of March 31, 1999. While I recognize that this hearing is taking place in July 1999, at Ameritech we report our results to our customers on a quarterly basis, and we're still in the process of compiling our data for the second quarter of 1999. We expect to post those results on our Internet Website in mid-July.

For Ameritech's network infrastructure, as of March 31st, all identified mission-critical network components of Ameritech's local telecommunications services, dedicated voice and data transport services are year 2000 ready. Similarly, as of March 31st, all identified mission-critical network components for Ameritech cellular, paging, and long distance service networks are year 2000 ready.

Corrective activities are also far along for our cable television service infrastructure and those mission-critical network components are expected to be made year 2000 ready well in advance of the turn of the century.

As of March 31st, Ameritech had completed its year 2000 remediation activity on all of the mission-critical information services systems and applications in its IS infrastructure, and they are now year 2000 ready.

And, finally, as of March 31st our operating infrastructure was over 95 percent year 2000 ready.

As I mentioned, at Ameritech we've made significant progress to address and resolve the year 2000 issue, and we believe that we'll have all Ameritech systems essential to maintain customer service completely year 2000 ready well before the turn of the century, perhaps even as early as July 31st.

In addition, although we are confident that we have taken appropriate steps to assure that we do not encounter year 2000 issues within our company, we are also developing business recovery and continuity plans designed to quickly address and resolve any significant potential problems that may arise.

In addition to internal company activities focused on addressing year 2000 within Ameritech, we were also participants in several industry forums that focused on addressing and resolving year 2000 issues within the telecommunications industry. As a member of the Telco Year 2000 Forum, a nationwide group of the largest telecommunications companies, Ameritech participated in intranetwork tests covering voice, high-speed data and 911 emergency services. Almost 2,000 tests produced only 6 anomalies, a 99.9 percent success rate, and each anomaly was corrected.

Before I conclude, I would like to share several consumer tips that were published by the FCC in its recently released Y2K communications sector report wire line telecommunications sector. In that report the FCC suggests some tips for consumers, including try to place some important telephone calls, particularly those overseas, before or after New Year's Day; minimize phone use on New Year's Day. Heightened traffic volume could overtax the network. And have at least a phone available that doesn't rely on electric power to operate. Cordless phones normally do not work without a separate power source.

I would like to conclude my testimony just by saying, as the subcommittee has recognized, the year 2000 issue represents a significant challenge to Ameritech's business and residential customers as well as to the government. As had been noticed, it is a worldwide concern which has been declared by many industry experts as the largest single project many companies will have to face. Resolving the issue requires strong project management, timely and informative communication, and cooperation across industry boundaries. At Ameritech, we're confident that we've addressed those challenges. I thank you for the opportunity to share these thoughts with you today.

Mrs. BIGGERT. Thank you very much.

[The prepared statement of Mr. Jensen follows:]

Testimony of Dale Jensen,
Ameritech Director - Year 2000 Customer Communications, Before a Field Hearing of
the Government Reform Committee to Examine Efforts of Local Governments and
Private Organizations to Address the Year 2000 Computer Problem

Naperville, Illinois
July 8, 1999

This document and the information contained herein is intended, and for
all purposes shall be deemed, a *Year 2000 statement* and a *Year 2000
readiness disclosure* as those terms are defined under United States federal law.

Opening Statement

Congresswoman Biggert and members of the Subcommittee, I am pleased to present testimony on Ameritech's activities to address Year 2000 issues within our company and I want to commend the subcommittee for its efforts to raise public awareness on the Year 2000 issue.

In the interests of time, I propose to direct my testimony to the following five areas:

1. The scope of our initiative;
2. The identification and status of key areas of the initiative;
3. Additional readiness activities underway at Ameritech;
4. Ameritech's participation in Industry Year 2000 readiness activities; and,
5. Tips for consumers courtesy of the Federal Communications Commission

I would then invite you and the other members of the subcommittee to explore in greater depth any area that may be of interest to you during the question and answer period following this panel's testimony.

In addition to my testimony, I have also provided the committee with copies of "Ameritech's Year 2000 Initiative - 1st Quarter 1999 Program Summary and Progress Report" and there are additional copies of that document at the back of the room. This report, which we update quarterly and make available to our customers through our internet web site (www.ameritech.com/y2k) or directly from an Ameritech customer service representative, provides additional detail on our efforts to meet the challenges presented by the Year 2000.

Ameritech's Year 2000 Initiative

We began our Year 2000 Initiative at Ameritech in 1996. Throughout our efforts, our overriding goal has been to make the Year 2000 event "transparent" to our customers by working to ensure that the products and services we provide to our customers avoid material problems associated with the Year 2000.

Our Year 2000 initiative includes:

- Reviewing more than 2,500 products and services for Year 2000 issues;
- Remediating an IS portfolio of approximately 1,000 applications;
- Upgrading 1,400 host and remote switches that handle telephone calls;

- Analyzing and preparing thousands of desktop and office components such as telephones, computers and fax machines; and
- Preparing the access and security systems, heating and cooling plants, alarms and elevators in over 12,000 buildings and equipment vaults.

Critical Areas of Ameritech's Year 2000 Initiative

A major component of Ameritech's Year 2000 Initiative is ensuring that we address and resolve any Year 2000 issues within three critical areas of our business:

The first area is our network infrastructure which includes our local exchange, cellular, paging, advanced data services, video and long distance networks.

The second area is our information services infrastructure which includes the information services hardware, applications and operating systems that enable us to conduct the day-to-day operations of our business.

And, the third area is our operating infrastructure which includes items such as the real estate properties that we occupy, for example, office buildings and central office locations, as well as employee support tools such as desktop personal computers and internal communications networks.

March 31, 1999 Status of the Key Areas of our Initiative

Having broadly defined the critical areas of our initiative, I would now like to discuss the status of each of those areas as of March 31, 1999. While I recognize that this hearing is taking place in July, 1999 – at Ameritech we report our results to our customers on a quarterly basis and we are still in the process of compiling our data for the second quarter of 1999. We expect to post our 2nd quarter results on our internet web site in mid-July .

Network Infrastructure Status

For Ameritech's network infrastructure, as of March 31, 1999, all identified mission-critical network components of Ameritech's local telecommunications services and dedicated voice and data transport services are Year 2000 ready. Similarly, as of March 31, 1999, all identified mission-critical network components for Ameritech's cellular, paging and long distance service networks are Year 2000 ready. Corrective activities are

also far along for Ameritech's cable television service infrastructure and those mission-critical network components are expected to be made Year 2000 ready well in advance of the turn of the century.

Information Services Infrastructure Status

As of March 31, 1999, Ameritech has completed its Year 2000 remediation activity on all of the mission-critical information systems and applications in its information services infrastructure and they are now Year 2000 ready. The majority of such systems have already been deployed back into production.

Operating Infrastructure Status

Finally, as of March 31, 1999, Ameritech's operating infrastructure was over 95% Year 2000 ready. As I mentioned earlier, for purposes of this testimony, the term operating infrastructure includes Ameritech's buildings and other facilities, internal communications networks and desktop PCs.

Other Ameritech Year 2000 Readiness Activities

As you have now heard, at Ameritech we have made significant progress to address and resolve the Year 2000 issue and we believe that we will have all Ameritech systems essential to maintain customer services completely Year 2000 ready well before the turn of the turn of the century – perhaps even as early as July 31st. In addition, although we are confident that we have taken the appropriate steps to assure that we do not encounter Year 2000 issues within our company, we are also developing business recovery and continuity plans designed to quickly address and resolve any significant potential problems that may arise.

Industry Year 2000 Initiatives

In addition to internal company activities focused on addressing Year 2000 within Ameritech, we are also participants in several industry forums that are focused on addressing and resolving Year 2000 issues within the telecommunications industry.

As a member of the Telco Year 2000 Forum ("Forum"), a nationwide group of the largest local telecommunications companies, Ameritech participated in intra-network tests

covering voice, high-speed data and 911 emergency services. Almost 2,000 tests produced only six anomalies; a 99.99% success rate. Each anomaly was corrected.

Ameritech is also a member of the Alliance of Telecommunications Industry Solutions ("ATIS"), a longstanding organization that includes both local and long-distance telecommunications companies and participated in their recent inter-network testing effort. These tests revealed no Year 2000 anomalies and verified that the public network can handle the expected high calling volume.

Consumer Tips Courtesy of the FCC

Before I conclude my testimony, I would like to share several consumer tips published by the FCC in its recently released *Y2K Communications Sector Report, Wireline Telecommunications Sector*. In that report, the FCC suggests that consumers:

- "Try to place important phone calls, particularly those overseas, before or after New Year's Day."
- "Minimize phone use on New Year's day (including modems). Heightened traffic volume could overtax the network"
- "Have at least one phone available that does not rely on electric power to operate. Cordless phones normally do not work without a separate power source."

Conclusion

As the subcommittee has recognized, the Year 2000 issue represents a significant challenge to Ameritech's business and residential customers, as well as to the government. As has been noted, it is a worldwide concern, which has been declared by many industry experts as the largest single project that many companies will have to face.

Resolving the Year 2000 issue requires strong project management within a company, timely and informative communication between companies and their customers and cooperation within industry and across industry boundaries. At Ameritech, we are confident that we are addressing those challenges.

I thank you for the opportunity to share these thoughts with you today.

Mrs. BIGGERT. Next is Craig Whyte from Nicor Gas. He says that gas service will not be interrupted.

Mr. WHYTE. Yes, you will have gas. Of course. Thank you again, Congresswoman Biggert and Congressman Horn.

On behalf of Nicor, we're very pleased to be here. We've been working on this project since 1996. We've had a committee established of 40 people and have made tremendous progress. As Alan mentioned, we believe we're Y2K ready as well. However, we'll continue to do testing throughout the end of the year.

In order to make my testimony more concise—which I'm sure you appreciate—as well as informative, we've put it on a video, and the video will be made part of the testimony when we're done. So in lieu of any more time, I think we'll just roll the video and if time permits, I'll wrap up afterwards.

Mrs. BIGGERT. That will be included in the testimony, without objection.

Mr. WHYTE. Additional copies will also be made if needed.

[Videotape played.]

Mr. WHYTE. We've made that tape available to all of the local municipalities that we currently service, over 400. A majority of them have used it on their cable access channel to put the word out. We've also distributed it to all of the local television, newspapers, and so forth. So the word is out there. We started our presentations early in January. We've been very successful with local and civic organizations and so forth. With that, I would be happy to answer any questions you might have.

Mrs. BIGGERT. Thank you very much. That was a different type of testimony than we're used to.

Mr. WHYTE. It's a lot easier for me, that's for sure.

Mrs. BIGGERT. Next we have Gary Mielak, vice president and chief executive officer at Edward Hospital.

Mr. MIELAK. Thank you, Vice Chairwoman Biggert and Chairman Horn.

In 1992, Edward Hospital launched an orchestrated attack on the millennium bug. As the community's health care provider, we have invested more than \$4¼ million on the project. We have also invested labor that's equivalent to four full-time employees. As a result of this 7 year Y2K project, Edward has made provisions to enter the new year with adequate power, supplies, staffing, communications and fuel, along with Y2K compliant medical devices.

Edward Hospital has deep roots in Naperville, having served as the community's health care provider for decades. Edward Hospital today is a medical center providing a broad spectrum of health care services to Naperville and a widening area of surrounding communities.

Like other hospitals, Edward maintains a posture of readiness for emergencies and disaster response. Because of this orientation, Edward is among those at the head of the pack. According to a Chicago based consulting firm, Edward is among the Nation's top 25 percent of hospitals in Y2K preparedness. The bottom line for us is anything with the potential to affect our patient's health and welfare is a high priority.

Let's look at the Y2K problem in the context of health care delivery. While Edward and other hospitals have a history of emergency

readiness, the Y2K bug is a unique animal for us. In the worst case scenario, many of the interdependent services could be cut at one time, requiring hospitals to survive on emergency backup systems and processes which were really never meant to sustain a hospital for an extended period of time. Failure in the chain of major utilities supply distribution, communications, and financial services would cripple a hospital's ability to serve its community, and this is a serious threat.

Y2K presents an incredibly complex planning job and challenge for the hospitals. The sheer number of areas that must be addressed is vast. The issues involve interdependency among patients, doctors, suppliers, payors, and agencies.

In addition to care delivery and office management issues, we're also dealing with potential supply chain problems beyond our control. For example, manufacturers and vendors are not always aware of their products' Y2K readiness because some of the components come from yet another supply chain. However, many areas remain that we can affect and minimize the impact of Y2K.

And here are some of the things that Edward has done: First, medical monitoring equipment with microprocessors and embedded chips. These are devices that are critical to life support in a lot of cases. These include infusion pumps, glucose monitors, ventilators, dialysis machines, heart machines, defibrillators and others. So far, of the date sensitive equipment that is high priority, we have found that less than 3 percent of the devices have required repair or replacement.

Next, the hospital has emergency power from its routine backup generators as well as a large extra generator leased for additional power during this period of time that will sustain us during any kind of an emergency. Information systems, of course, affect everything from patient scheduling to clinical records and inventory management.

To date, close to 100 percent of the computer software and hardware products the hospital uses are compliant. A new control computer for the heating and ventilating system had to be replaced because it was not compliant. The hospital has made provisions for bulk delivery of water and fuel oil, for heating and electricity generation, as necessary. And Edward will keep an additional 7 day patient food supply on hand during critical Y2K periods.

Security systems have been checked and made compliant. Elevators will operate. The telephone system is being tested, as we speak today, for compliance at the manufacturer's site. A radio station is working with the hospital to provide emergency communications for calling in staff. A network of CB radio users will be formed for communication if necessary.

Internal and external communications to the staff and public are an integral part of the preparation. We will continue to inform the public about what we are going to do in case of an emergency. Planning is underway to ensure appropriate staffing levels. Inter-hospital planning has just begun and we're working with our colleagues to make sure plans and ideas are shared.

In conclusion, behind all of the devices, processes, and plans are

people. Our health care professionals' ingenuity, integrity, and pride in providing quality health care will drive us all regarding Y2K preparedness. Thank you for the opportunity to make our presentation today.

Mrs. BIGGERT. Thank you very much for being here.

[The prepared statement of Mr. Mielak follows:]

The Y2K Project

Edward Hospital, Naperville IL

July 1999 Congressional Testimony

In 1992 Edward Hospital launched an orchestrated attack on the Millennium Bug. As the community's health care provider, we have invested more than \$4.25 million dollars on the project, as well as labor equivalent to four full-time employees. As a result of this seven-year Y2K project, Edward has made provisions to enter the New Year with adequate power, supplies, staffing, communications and fuel along with Y2K compliant medical devices.

Edward Hospital has deep roots in Naperville, having served as the community's healthcare provider for decades. Originally a tuberculosis sanitarium, today's Edward is a medical center providing a broad spectrum of health care services not only to Naperville but also to a widening area of surrounding communities.

Like other hospitals Edward maintains a posture of readiness for emergency and disaster response. Because of this orientation, Edward is particularly primed for staying on top of the Millennium Bug threat. And Edward is among those at the head of the pack even compared to other hospitals. According to a Chicago-based consulting firm, Edward is among the top 25 percent of the nation's hospitals in Y2K preparedness. The bottom line is anything with the potential to affect our patients' health and welfare is a high priority.

Let's look at the Y2K problem in the context of healthcare delivery. While Edward and other hospitals have a history of emergency readiness, the Y2K bug is a unique animal. In some ways it's easier to grapple with the specter of a tornado or other natural disaster. "Typical" disasters are usually more limited in their disruption of the complex infrastructure that healthcare delivery depends on. Natural disasters temporarily cut or slow down some of the region's supply chain of services. The Y2K challenge, however, is unusual. In the worst case scenario, it could cut many, if not all, of the interdependent services at one time and require many hospitals to survive on emergency back-up systems beyond their capacity to operate. Failure of major utilities, supply distribution, communications and financial services would cripple a hospital's ability to serve its community.

Edward's preparations in 1992 began with formation of a technical team representing many hospital departments and skills. The first order of business was to inventory the entire stock of equipment and systems that could be affected by Y2K issues. Tasks were prioritized and assigned and schedules were set for accomplishing the corrections. Our management team and board, who were kept informed throughout these activities, provided unwavering financial and moral support.

Y2K poses an incredibly complex planning challenge. The sheer number of areas that must be addressed is vast and the related issues involve interdependence among patients, doctors, suppliers, payors and agencies. In addition to care delivery and office

management issues, we're also dealing with potential supply chain problems beyond our control. For example, manufacturers and vendors are not always aware of their products' Y2K readiness because some of their components come from yet another supply chain. Other suppliers make vague statements regarding their intentions to be compliant. Some even are going out of business.

However, many areas remain that we *can* control to minimize the impact of Y2K. Here are some of those areas and what we have done at Edward to address them:

- First, medical monitoring equipment with microprocessors or embedded chips. Those devices that are critical to life support are Y2K ready. These include infusion pumps, blood glucose monitors, ventilators, dialysis machines, heart machines and defibrillators and others are ready. Of the more than 4000 pieces of medical equipment checked, over 2000 featured date sensitivity. About 1800 of these were determined to be "high priority" based on their potential impact. Approximately 60 percent of this latter group have now been deemed compliant and the rest are on a tight schedule for checking and compliance by the fall of 1999. So far less than 3 percent of the devices have required replacement.
- Next, emergency power. The generator software for our emergency power had to be replaced or it would not have operated properly when 1999 became 2000. Now the hospital will have emergency power from its routine back-up generators, as well as a special trailer-mounted emergency generator that is connected as a standby unit. Power will be available for the duration of any emergency.

- Information systems. These affect everything from patient scheduling to clinical records and inventory management. Testing is taking place on a separate testing system. To date close to 100 percent of the computer software and hardware products the hospital uses are compliant.
- Environmental control equipment. A new control system computer for the heating, ventilation and air conditioning had to be installed because the system was non-compliant.
- Water and fuel. The hospital has made provisions for bulk deliveries of water and fuel oil for heating and electricity generation as necessary.
- Food. The Joint Commission on Accreditation of Healthcare Organizations requires hospitals to keep a seven-day supply of food on hand for patients. Edward will keep an additional seven-day patient food supply on hand during the critical Y2K period.
- Security. All security systems have been checked and made compliant.
- Elevators. These will be operational in our multi-story hospital.
- Phone services. The telephone and data communications network is being tested for compliance at the manufacturer's site. This will entail a complete test of our exact configuration of equipment and operations software. Modifications will be made as required once the testing is complete at the end of July 1999.
- Emergency communications. A radio station is working with the hospital to provide emergency communication regarding services and staffing call-ins. Security regarding these services will be very tight. A potential group of CB radio users will be formed for building to building communication, if there is a need.

- Internal and external communications. Communications to the staff and public are an ongoing part of the preparation. We have distributed press releases on the hospital's preparation and will continue to inform the public during the coming months about what they can expect from the hospital if a Y2K emergency should occur.
- Planning is underway to ensure appropriate hospital staffing levels and processes during the Y2K period.
- Inter-hospital planning has just begun. We are working with our colleagues to plan and share ideas about preparation for Y2K issues in our communities.

Behind all of the devices, processes and plans are people. Our health care professionals' ingenuity, integrity and pride in providing quality health care will drive us all regarding Y2K preparedness.

Based on our study of the issues we strongly recommend the public consider the following tips:

- Don't postpone refilling your prescriptions until January 1, 2000. If you do need prescriptions filled during or just after the millennium change, review the instructions and information on the containers and sheets carefully to make sure all information is correct.
- If you, family members or significant others use life-sustaining equipment, make sure that it will operate properly going into and beyond January 1, 2000.
- Check with your physician if you have acute or chronic respiratory illnesses, heart disease, diabetes, epilepsy, or other serious ailments. Ask your doctor if he or she

will be available during the holiday period and whether they have special instructions should complications occur during this time.

- Be prepared for minor emergencies by maintaining a well-equipped first-aid kit, along with an easy-to-use instruction booklet.
- Have a portable radio with a fresh spare battery ready for use.
- Have flashlights with fresh batteries handy and maybe a candle or two.
- Have drinking water available in a place where it will not freeze.
- Be prepared for extreme weather conditions.

Edward will remain ready to serve regardless of the environment. Prudent precautions on everyone's part can and will allay fears about the future surrounding Y2K. We feel confident about our Y2K provisions to date. At the same time our team will continue to review and refine Edward's contingency plans and to address Y2 issues right to the end of the year.

Mrs. BIGGERT. Now, Mr. Pagano.

Mr. PAGANO. Thank you for inviting us here today. For the benefit of those not familiar with Metra, let me start with a brief summary of what we do. You'll quickly see why we took this very seriously and aggressive approach to the Y2K readiness situation.

In terms of ridership, Metra is the second largest commuter rail system in the United States. Last year we carried 77 million people, which was our highest ridership since 1984. This year we are ahead of that mark and intend to set another record.

In terms of our network, however, we are the largest commuter rail system in the United States. We operate over 11 lines, have 500 route miles, have 130 locomotives, 900 passenger cars. We service an area the size of Connecticut and carry nearly 300,000 passengers weekly.

Finally, we operate this network with a great deal of reliability and it is recognized as the leading commuter rail agency in the United States.

If some computer glitch forced those riders out into Chicago's expressway system, we'd have instant regional gridlock. I'm happy to say that we don't think that will happen. We've been working on the Y2K compliance since 1996. We have found no Y2K problems in our computers, facilities, or equipment that would cause a disruption to our computer rail service.

Looking for possible Y2K bugs, we first focused on large mainframe legacy financial administrative systems. We then broadened our focus to include all areas of computer use and established an internal Y2K task force.

That group surveyed and assessed support computers and embedded computers in equipment and facilities. They also evaluated the readiness of key suppliers, service providers, and other railroads that interact with Metra.

For all areas of computer use, we employed a methodology of awareness, inventory, assessment, testing, and implementation. During the assessment phase, we measured each computer system for Y2K processing issues and classified each as mission-critical or not. We gave remediation priority to systems that are mission-critical to safety reliability of train operations, revenue collection, and compliance with government regulations.

Throughout this process, Metra's Board of Directors, senior management and auditors, along with the Federal Transit Administration and the Federal Railroad Administration, have received regular reports. Specific areas of investigation include mainframe and administrative computer systems, locomotive and passenger cars, track and signal stations, so on and so forth.

Of course, we can't guarantee that nothing will fail or that our service is totally immune to disruption from a third-party problem. We are prepared to respond to any such situation with the same dedicated manner as during other unexpected or winter-related disruptions to service. We rely on established procedures within our operating rules and contingency plans for power losses or problems caused by bad weather. We also rely on federally required manual backup systems and procedures for components or equipment failures.

We're confident that we won't have to do this. As I said earlier, we really don't see any Y2K problems. So far, to date, we have spent about \$750,000, and again we have found very few of our systems that had to be tinkered with or modified. With that, we'll answer any of your questions.

Mrs. BIGGERT. Thank you very much.

[The prepared statement of Mr. Pagano follows:]

Remarks of Phil Pagano, Metra Executive Director, U.S. House Subcommittee on Government Management, Information, and Technology, Naperville, Illinois, July 8, 1999

Good morning. Thank you for inviting me.

For the benefit of those of you who may not be familiar with Metra, let me start with a brief summary of what we do. You will quickly see why we took a very serious and aggressive approach to Y2K readiness.

In terms of *ridership*, Metra is the second largest commuter railroad in the United States. Last year, we provided over 77 million passenger trips. That was the most since 1984, our first full year of operation. This year, with a steady growth of almost 3 percent we seem headed for another record.

In terms of *network*, Metra is the largest commuter railroad. We operate over 11 lines with a total of about 500 route miles. We own and directly operate four of those lines. We contract with two major freight railroads for service on four other lines.

And through trackage agreements, we directly provide service on three more lines. Finally, we operate this network with a great degree of reliability and are recognized as one of the leading commuter rail systems in the United States.

We are a true *regional passenger railroad*, serving the six-county Northeast Illinois Region, about the size of Connecticut. We cover that network with a fleet of 130 locomotives and more than 900 passenger cars. We now provide nearly 300,000 passenger trips each weekday.

If some computer glitch forced those riders out onto Chicago's expressway system, we'd have instant regional gridlock.

I'm happy to say that we don't think that will happen. We've been working on Y2K compliance since 1996. We have found no Y2K problems in our computers, facilities or equipment that would cause a disruption of commuter rail service. We look forward to the new millennium with the utmost confidence in our Y2K readiness.

- Continued ...

Looking for possible "Y2K bugs," we first focused on large mainframe legacy financial and administrative systems. We then broadened our focus to include all areas of computer use and established an internal Y2K task force.

That group surveyed and assessed support computers and embedded computers in equipment and facilities. They also evaluated the readiness of key suppliers, service providers, and other railroads that interact with Metra in any way, especially those that operate our service under contract.

For all areas of computer usage, we employed a methodology of awareness, inventory, assessment, remediation, testing, and implementation. During the assessment phase, we measured each computer system for Y2K processing issues and classified each as mission-critical or not. We gave remediation priority to systems that are mission-critical to the safety and reliability of train operations, revenue collection, and compliance with government regulations.

Specific areas of investigation included mainframe and administrative computer systems; locomotives and passenger cars; track and signals; stations, offices, yards and shops; communications, suppliers, and other railroads and agencies.

Throughout this process, Metra's board of directors, senior management, and auditors, along with the Federal Transit Administration and the Federal Railroad Administration, have received regular reports.

Of course, we can't guarantee that nothing will fail or that our service is totally immune to disruption from a third-party problem. We are prepared to respond to any such situation in the same dedicated manner as during other unexpected or weather-related disruptions of service. We will rely on established procedures within our operating rules and

- Continued . . .

contingency plans for power losses or problems caused by bad weather. We'll also rely on federally-required manual backup systems and procedures for component or equipment failures.

I'm confident that we won't have to do that. As I said earlier, we really don't foresee any Y2K problems. We simply have found nothing that would prevent our trains from operating normally throughout the year 2000.

Again, thank you for this opportunity to talk about Metra's Y2K readiness. Now, if you have any questions, I'll be happy to answer them.

###

Mrs. BIGGERT. That concludes the testimony for this panel, so I think I'll ask Chairman Horn to ask questions.

Mr. HORN. Let me ask you generally the same question I asked the last panel. And that is if you had to do it over again, what have you learned that you should have done first? Let's just go down the row with Mr. Ho.

Mr. HO. There isn't much I think that we would do different. I do believe there is significant value gained now on a go-forward basis beyond these Y2K rollover dates, and that comes from the additional configuration of control that we have over our computer systems. We have inventoried everything. We have also retired non-standard applications, so we've taken an opportunity to standardize work so that—standardized applications as well as systems. And so that has value both internally and across our supply chain.

Mr. HORN. The next gentleman, Mr. Jensen.

Mr. JENSEN. I would agree with Alan. I think at Ameritech, we have a strong program in place. I don't—in retrospect, I don't think we would have done anything different. Certainly, probably everyone would have started earlier but—and I suspect in the future if we run into a situation like this, we probably will start earlier.

But overall inventory, the benefits are numerous going forward from an inventory control, supplier management and supplier relationship and so I don't think we would have changed very much, if anything, in our program.

Mr. HORN. Mr. Whyte, Nicor Gas.

Mr. WHYTE. I would have to agree with the comments made. We started in 1996, which is really a 4-year tenure, which gives us a lot of time to prepare. We started our informational process up early, which has been very beneficial. So I really can't say that we would have changed anything drastic.

Mr. HORN. Mr. Pagano, Metra.

Mr. PAGANO. I think what we learned was, as a benefit, we had many of the people that had put in the systems for us on staff so that they were able to quickly make an assessment. I think in the future what we've learned is that there needs to be more documentation of procedures so that recordkeeping is there in case you don't have the old heads around to followup.

Mr. HORN. Mr. Gary Mielak, the vice president and chief technical officer for the Edward Hospital.

Mr. MIELAK. I think the two issues that we learned more about than anything going through this process was that interaction with our professional colleagues, other hospitals and agencies. I wish we would have had more time to do that, because everybody was so busy focusing on their own areas of expertise within their own facilities and hospitals that people just didn't have time to look around. Even having started in 1992, we only found the time recently to start looking outward from our facility.

Mr. HORN. Did you start in 1992?

Mr. MIELAK. We started in 1992.

Mr. HORN. I congratulate you, because you were 6 years ahead of the executive branch of the Federal Government, and it took us 3 years to prod them into doing anything, and they didn't do it until 1998.

Mr. MIELAK. Thank you.

Some of the supply chain concentration also is another thing that I think that we could have spent and should spend more time on between now and the end of the year. But it is very difficult for a lot of the suppliers to even know their situation for us to appropriately interact with them.

Mr. HORN. Perhaps you can answer the question that was filed with the first panel, but we really didn't have an expert on this: What is the situation with the drug manufacturers? As a pharmacist in the community, says the writer, a common question is, How much of a supply should I keep in store and on hand that's extra? What we have been told is a 90-day period we ought to prepare for.

Can any of you comment on a contingency plan regarding the situation?

Well, I guess, Mr. Mielak, you have the same problem they face?

Mr. MIELAK. I think we probably do. However, hospitals, of course, having always an emergency preparedness plan, even for pharmaceuticals and other items that patients use, we really do keep several days' and sometimes a week or more worth of supplies on hand, and one can usually tell from your inventory turnover how fast that supply will deplete in each one of the drugs. It is not our intention to hoard supplies or to bring weeks' worth of supplies in, but to be prudent about what we think maybe an inventory shortage might be, and work with our suppliers to have an adequate supply on hand for a week or so.

Mr. HORN. OK. Do we have any more questions here from the audience?

With concern in it being a leap year—I guess it means about a leap year and turning—I really—staff is going to have to put it into English I can read. I can't read it.

Mrs. BIGGERT. I'll read it. With concern with it being a leap year and the turn of the century, will there be any problems on February 29th? Will this affect us?

Mr. HORN. I guess I'll answer that first. The leap day, February 28th, 29th, and March 1st have been dates that have been included in our overall test program so our electric systems and our computer systems can handle that date in the year 2000 and beyond.

Mr. MIELAK. There are several applications also in the hospital area where we have started testing software a few months ago for date changes that might be applicable all the way until the year 2004. So there are several dates along the way that I know in our applications we have to be mindful of.

Mr. HORN. Next question is, Where and when can a citizen obtain the summary of this hearing?

The hearing transcripts will be printed shortly, but the testimony that the members before you have given in three panels—we have two panels so far—they will be put on our Website and the Website is www.house.gov/reform/gmit. It stands for Government Management, Information, and Technology. So right now they can put this testimony on when they get back tomorrow.

Mr. Ho of Consolidated Edison, what are the ComEd staffing plans for December 31st to ensure delivery of power and as a contingency if the power fails?

Mr. HO. We have normal staffing every day around the clock. For New Year's Eve and for the other rollover dates, we have planned additional staffing to be at the ready. So we will be in a ready posture, with staff physically located throughout our northern Illinois territory so as to monitor the system as well as respond, should there be any outage occurrences, whether Y2K related or otherwise. And so we look to have a rapid response to any occurrence.

Mr. HORN. Mr. Whyte of Nicor—gas is supplied through a network of pipelines with gas moved along by pumps operated by turbines and generators. Is there a problem if electrical power is disrupted?

Mr. WHYTE. We currently have 8 major pipelines coming into our area, all independently operated. To have all 8 of those pipelines go down, I think, would be very remote. But should that happen, it is important to know that a majority of the natural gas industry is run on mechanical, by nature, so most of the valves can be overridden. If not overridden, they can certainly be hand-manipulated open or shut. That night we will also have a full staff on, as well as people at these locations should the power fail. We do have generators to rate our own electricity, so to speak, if we need to. And should that fail, for whatever reason, we have a manual override. Should that fail, we physically can put someone out there and crank open valves if necessary.

Mr. HORN. Mr. Mielak, representing the Edward Hospital, and you partially answered the pharmaceutical question, but another one along that line puts a little different wrinkle on it. As a major percentage of prescription medicines are imported, what contingencies are being made to ensure adequate availability? It should be noted that insurance only allows monthly purchases. Is that correct? Or do you have a pharmacy in the hospital?

Mr. MIELAK. We have an internal pharmacy at the hospital and there are the Naperville pharmacies who are independent of the hospital. I really don't have an exact answer to that question. It is very difficult for me to look out into that supply chain and make comments on it.

Mr. HORN. Well, I would think the Pharmaceutical Association for the State of Illinois would be working on that problem and since every pharmacist probably pays dues to that agency, get them to work if they haven't answered that question.

Now, on the utilities in general, with respect to the utilities, do you rely on what they tell you, or do you audit their statements? What type of independent verification efforts has each utility undertaken?

In other words, we face the same problem with the Federal Government. We ask the inspector generals in each agency that are really one step apart—they don't report to the Secretary. They're independent people, and the General Accounting Office that Mr. Willemsen represents and is here, they're part of the legislative branch. To look at the financial and programmatic aspect of the executive branch, and so they're asking the same now of utilities. Have you gotten outside independent verification, or is this simply your own people verifying it and should we trust them?

Mr. HO. We've had several levels of independent review. We've had third-party consultants come in, assess our management proc-

ess as well as the cogeneration embedded systems renovation work and those reports have been given to the senior officers of the corporation as well as our Board of Directors.

Second, the NRC has come in, the Nuclear Regulatory Commission has come in and audited our Braidwood Station and indeed our entire nuclear fleet, our corporate IS, our supply chain activities, and given us high praise in their January report. They've since followed up and reviewed our contingency planning activities and there will be a report coming out later this month.

We've also had peer reviews where we've had other utilities come and look at our process, look at our results, and we've shared and exchanged resources and information to that point. So we think there's a very solid basis for the results that we've achieved and reported.

Mr. HORN. Was that the Nuclear Regulatory Commission, the Federal Commission?

Mr. HO. Yes.

Mr. HORN. How many different facilities of yours did they look at? Just one?

Mr. HO. They looked at all of our nuclear facilities. There was a very strong focus at our Braidwood Nuclear Station. They asked to look at the results across our nuclear fleet.

Mr. HORN. So the answer would be they have looked at every single facility in your company's jurisdiction that has nuclear reactors?

Mr. HO. That's correct.

Mr. HORN. I'm glad to hear it because when they started out, they said we're only going to audit 10 percent, and we argued with them on that and we said we wanted to see 100 percent. They've never given us an answer to our letter on why they were doing just 10 percent. So at least in your situation, you got 100 percent audit from them.

Mr. HO. That's right.

Mr. HORN. Thank you very much on that.

Mr. Willemsen is still here, I'm sure. There's a chair right down here at the end, Joel. From the audience, despite all the optimism stated by your committee—I guess he's referring to us—the consensus in the technical computer world is that no one really knows what really will happen. A worst-case situation may be a lack of power and utilities for several months. Are you even considering a worst-case situation?

Mr. WILLEMSSEN. I think even in those Federal agencies who are far ahead of the game, such as the Social Security Administration, they have also been on the forefront of doing business continuity and contingency planning, recognizing that they, along with other organizations, cannot provide an absolute guarantee that there won't be some Y2K problems at the turn of the century or at other critical dates. And therefore they have put a lot of emphasis on contingency plans to have them available in the event of disruptions and have them available to trigger at appropriate points in time.

I think a scenario that was laid out in the question of widespread electric power disruption over a couple months, I don't think any reasonable organizations have thought that far out in terms of

worst-case scenario. Worst-case scenarios for the contingency plans that I've reviewed, and I have reviewed several, do not go beyond a few weeks in terms of electric power outage. Frankly, if we did have that situation, and we don't have any evidence to suggest that would be the case, we would be looking at an entirely different scenario than the one we've talked about today.

Mr. HORN. Thank you very much for that.

Mrs. BIGGERT. Thank you, Chairman Horn. I have just two more questions from the audience. The first one is addressed to Mr. Ho. Can Commonwealth Edison isolate themselves from the power grid to continue to service their customers if the power grid is in trouble?

Mr. HO. The simple answer to that is yes, but the Eastern Interconnection in the grid, as everyone refers to it, is really designed to be a robust system and reliable because everyone shares in that pool. And so our plans are not to island or isolate ourselves should there be a problem. The real benefit to the grid is that ComEd can help support, and the surrounding utilities can support one another should there be a stability problem on the system. And so we look to not implement a sort of islanding or isolation-type of approach. The grid is very robust and we look to maintain that.

Mrs. BIGGERT. Thank you.

And then the last question is for all of you. Should glitches occur in service, how will they be communicated to the public? Will there be additional staff on board to handle these calls? And third, will we call the same service numbers that we currently call or will hotlines be set up? I think we can start with Mr. Ho and just go down the line.

Mr. HO. On New Year's Eve, we will start our staffing of our command center early in the morning, 6 o'clock New Year's Eve morning, and we'll have an eye on the globe. We will be providing press releases and system status reports three times throughout that business day. By 8 o'clock that evening, we will be fully manned at our command center, at which time we will start hourly system status reports. Those status reports will go out across the normal channels through our account managers for those commercial industrial customers, through our public affairs directors, to the various municipalities, such as here in Naperville. We'll have media briefing and, in fact, media will be with us at our command center.

So we look to have constant reporting and increased frequency of reporting as the day goes on. So there will be additional staff, like I said, across our territory; and our communications staff will certainly be right in the thick of it with us.

Mr. JENSEN. Like Alan, Ameritech will also have a command center in place and we'll be undergoing many of the same activities and preparation.

I think that what I would like to address here is on the other side of the coin: What would we ask our customers to do in the event that they encounter a problem? And we're asking customers to do the same thing that they do today; call the same trouble reporting number, follow the same procedures. We don't want to confuse the issue by putting anything different in place. We expect, just like probably Alan and everyone else, to have additional staff-

ing on hand to take care of any additional calls that we may get. So keep it simple is kind of our watch word. Our customers just call the same number that they would call today if they encounter a problem.

Mrs. BIGGERT. Thank you.

Mr. Whyte.

Mr. WHYTE. Real briefly, the service numbers they call right now will certainly be the same numbers they will use then. As far as staffing, it'll definitely be beefed up. I know I will be there, as well as all of our representatives, they will be there. We'll have our labor staff available.

As far as communications are concerned, we are in the process now of developing a list of all key contacts through all of our municipalities that we serve so that on that night, should they have any issues or questions, they'll know who to call as well as when we have updates throughout the day and night, we have someone to contact as well.

Mrs. BIGGERT. Mr. Pagano.

Mr. PAGANO. Yes, they'll be using the same hotline phone numbers. We'll have additional staff there to take care of any problems.

Mrs. BIGGERT. Thank you.

Mr. MIELAK. Assuming normal communications, telephone, pagers, cell phones stay in operation, we don't have any problems in those areas. All of our normal service lines will be open, and there will be staff there to answer any telephone calls or concerns by patients in the communities or others looking for information.

Should that not be the case, our fallback readiness position, of course, in an emergency is always to go to the radio systems that the emergency folks have both in Naperville and the hospital. Ambulance services are all equipped with these standby emergency systems. Of course, we can't get out and talk to the general public about what's going on under those conditions, but we certainly can try to get out to the radio station and get out the word otherwise through some means that we have yet to talk about.

Mrs. BIGGERT. Thank you.

Mr. WILLEMSEN. The Federal Government right now is in the process of setting up a command center that will be led by retired General Peter Kind, and they're putting their procedures together right now. They intend to get contacts and links set up with all the major Federal agencies and also with States so that the reporting process will occur as the rollover happens. In addition, they will be monitoring the activities through the State Department of all other countries. As you know, obviously we have a tremendous built-in advantage in our country. We will have lead time to see what happens in other countries as the clock switches there before it does in our country.

Mrs. BIGGERT. Thank you. Again, this is all part of being prepared, and I hope that none of these hotlines have to be called or none of these phone numbers—they won't be busy if somebody does call, because there won't be the problems. But I think as long as everybody is ready and have those contingency plans, that things will go smoothly.

So I thank you all on this panel for coming. I think it's been very enlightening. And to hear what our utilities are doing, what our

hospitals, transportation, is all very important to all the citizens of this area and to the State and to the country. So thank you very much for coming.

We'll then call up the next panel.

Mr. Skarr, if you want to come up and join the panel. We will have to do a little switching of mics, but I think there's almost room.

If you all want to stand.

[Witnesses sworn.]

Mrs. BIGGERT. Thank you again. This is the third panel of the hearing this morning, and I think again I will start by just introducing you as each of you speak and if you can limit that to 5 minutes, particularly since we have a larger panel this time, it would be appreciated.

The first member of the panel is Clint Swift who is director of Banking Technology, the Bank Administration Institute of Chicago. Thank you very much for coming, Mr. Swift. You may proceed.

STATEMENTS OF CLINT SWIFT, DIRECTOR OF BANK TECHNOLOGY, BANK ADMINISTRATION INSTITUTE; DELORES CROFT, SENIORS POLICY ADVISOR, ILLINOIS ATTORNEY GENERAL'S OFFICE; LEONARD HARRIS, PRESIDENT, CHATHAM FOOD CENTER; RON CLARK, TREASURER, ILLINOIS AYERS OIL CO.; MONTY JOHNSON, COMMUNICATIONS COORDINATOR, CITGO GAS; MIKE SKARR, PRESIDENT AND CEO, NAPERVILLE AREA CHAMBER OF COMMERCE; AND ED PAULSON, AUTHOR OF YEAR 2000 CRISIS SURVIVAL IN 10 MINUTES, PROFESSIONAL ENGINEER, FINANCIAL EXPERT

Mr. SWIFT. Mr. Chairman and Madam Vice Chairman, thank you for providing a public forum on the year 2000. Just a week ago, the banking industry passed the last of the major federally mandated milestones for year 2000. The bankers are intensely aware that the challenge has shifted from a technological one to a psychological one. It is crucially important that people understand the lengths to which banks have gone to ensure that it will be business as usual before, during, and after January 1, 2000.

As one independent observer after another has told you, the reality is that financial services are in good shape. Banks, thrifts, credit unions will be spending much of the next 6 months ensuring that the key energy, telecommunications, and other providers they rely on are ready as well.

I can state this for the record. First, your bank will be ready for the century date change. Many of them are ready now. The rollover is going to be a non-event for almost all bank customers. Your bank is the safest place for your money. Your money is insured there up to \$100,000, but there are at least two other significant issues. Your bank will have accurate records of your accounts and you'll be able to get the cash you need when you need it.

How can I say these things? First, for the last 2 years I've been working day to day with 50 of the Nation's largest banks. Institutions that represent about two-thirds of this Nation's banking assets. I know personally the quality of their planning, their systems inventories, their code repairs and their testing. These institutions have verified that the systems that support checking, savings, cer-

tificates of deposits, loans, and other products and services, process dates accurately before, during, and after January 1, 2000. Now they're monitoring Y2K progress at the suppliers and service providers they rely on.

Second, banking is a highly regulated industry. As part of Y2K preparation, Federal examiners have visited each bank in this Nation at least three times. At the end of May, more than 98 percent of the Nation's 10,000 federally insured depository institutions had received the highest ranking. During the next 6 months I can promise you that the handful that didn't can look forward to a very personal relationship with your examiners.

To ensure that banks have plenty of cash for anyone who needs it, the Federal Reserve has accelerated printing of nearly \$50 billion in currency, and they're placing that at 100 locations, closer to banks than their own Federal vaults are.

In this highly interconnective world, nobody with any sense is going to give you a guarantee that there will be no disruptions at the century date change. For all but a handful of Americans, the lights are going to come on. By the time you get the phone to your ear, there is going to be a dial tone. Where outages do occur, research and testing across industries say they will be localized and of short duration.

In case one of those limited local outages occurs in DuPage or Kane Counties, let me also observe that banks, thrifts, credit unions have always been among the first to reopen after a hurricane, tornado, or other natural disaster. Why? Because they're practiced masters at contingency plans. Banks have always been required to keep multiple backup records of your transactions in case of power outages or computer problems, and fresh backups are made every day. Banks have now supplemented their existing contingency plans with special preparations to cover the glitches that may occur due to the year 2000 date change.

Before I close, I want to address the notion that people need to withdraw a month's worth of cash to get through the rollover period. I live in the next town north of here, Wheaton, with my wife and son. Based on what I know about banking, I'm going to withdraw the same amount of cash that I would for any other holiday weekend. I know that if I need more, I'll be able to get it from an ATM or from a teller. In the meantime I know I'm not going to be contributing to a sudden shortage that could keep my neighbors from getting the cash that they need.

And keeping large amounts of cash outside the bank is not just unnecessary, it is dangerous. Local law enforcement officials are some of the most outspoken opponents of stashing months of cash around your house. Theft is a very real threat. At a recent White House Community Conversation I attended, a police chief said that 90 percent of thefts in his jurisdiction involved people close to the victims, such as family or so-called friends.

You can have confidence in the year 2000 preparations of your

bank. It is going to be business as usual at the bank today, tomorrow, during the year 2000, and after.

If you have questions about the details of bank readiness, I would be pleased to try to address them.

Mrs. BIGGERT. Thank you very much for your testimony.

[The prepared statement of Mr. Swift follows:]

JUNE 8, 1999

TESTIMONY OF

CLINTON R. SWIFT, PH.D.
DIRECTOR, BANKING TECHNOLOGY
BANK ADMINISTRATION INSTITUTE,
CHICAGO

AT Y2K CONGRESSIONAL HEARING (NAPERVILLE, ILLINOIS) ON
GETTING READY FOR THE MILLENNIUM BUG

Good morning, madam vice chair. Thank you for providing this public forum on how business and government in the 13th District are preparing for the century change. Just a week ago, the banking industry passed the last of the major federally mandated deadlines for year 2000 preparations, and bankers are intensely aware that their challenge has shifted from a technological one to a psychological one. It is crucially important that people understand the lengths to which banks have gone to ensure that it will be business as usual before, during and after January 1, 2000.

The reality is that the financial services sector is in good shape, and banks, thrifts and credit unions will be spending much of the next six months ensuring that the key energy and telecommunications providers they rely on are ready as well.

I can state this for the record:

- First, your bank will be ready for the century date change, and the rollover will be a non-event for almost all bank customers.
- Second, your bank is the safest place for your money. Your money is insured there up to \$100,000, but it's more than a security issue. It means two specific things – your bank will have accurate records of your accounts, and you'll be able to get the cash you need when you need it.

How can I say those things? First, for the last two years, I have been working day to day with 50 of the nation's largest banks, institutions that represent about two-thirds of this nation's banking assets. I know personally the quality of their planning, their systems inventories, their code repairs and their testing.

Banks, thrifts and credit unions have tested and re-tested their computers, watching the date roll over into the next century and across Leap Day, 2000. They have verified that the systems that support checking, savings, certificates of deposit and loans process dates accurately before, during and after January 1, 2000. And we're not talking about just mainframe and personal computers. Your bank is checking the ATMs, the security systems, the clocks, the elevators, and the heating and air conditioning systems. And they are monitoring Y2K progress at the suppliers and service providers they rely on.

Second, banking is a highly regulated industry. As part of Y2K preparation, federal examiners have visited every bank in the nation at least three times. At the end of May, more than 98% of the nation's 10,000 federally insured depository institutions had received the highest rating. And during the next six months, I can promise you that the handful that didn't can look forward to a having a very personal relationship with their examiners.

Third, to ensure that banks have plenty of cash for anyone who needs it, the Federal Reserve has accelerated printing of nearly \$50 billion in currency. To ensure that transportation doesn't create local shortages, the Fed is placing up to \$100 million at each of more than 100 locations closer to banks than the Fed's own vaults are.

Fourth, don't forget about those other forms of payment that you use every day. They're still going to work. At a Washington news briefing recently, a representative of the Retail Federation laughed at the notion that you'll go into Wal-Mart or Dominick's in January and be told you can't pay with anything but cash. "After those millions spent on advertising?" she said. Your check, debit card and credit card will be accepted with a smile – business as usual.

In this highly interconnected world, nobody with any sense will guarantee you that there will be no disruptions when the century date changes. But for all but a handful of Americans, the lights will come on, and by the time you get the phone to your ear, there will be dial tone. Where outages do occur, research and testing across industries say they will be localized and short-term.

But in case one of those limited, local outages occurs in DuPage or Kane County, let me also observe that banks, thrifts and credit unions have always been among the first businesses to re-open after a hurricane or tornado. Why? Because they are masters of contingency planning. Banks have always kept multiple back-up records of your transactions and accounts in case of power outages or computer problems, and fresh back-ups are made every day. Now, banks have supplemented existing contingency plans with special preparations to cover the glitches that may occur due to the year 2000 date change.

The notion that people need to withdraw months worth of cash to get through the rollover period is troubling. If everyone withdrew months worth of cash on little or no notice, a branch's ability to meet demand could be stretched to the limit until it was resupplied. I live in the next town north of here with my wife and son, and based on what I know about banking, I will be withdrawing the same amount of cash that I would for any other holiday weekend. I know that if I need more at any point, I will be able to get it from an ATM or a teller. And I know I won't be contributing to a sudden shortage that could keep my neighbors from getting the cash they need for the weekend.

But keeping large amounts of cash outside the bank is not just unnecessary; it's dangerous. Local law enforcement officials are some of the most outspoken opponents of

stashing months of cash around the home. Theft is a very real threat. At a recent White House Community Conversation, a police chief said that 90% of thefts in his jurisdiction involved people close to the victim, such as family or so-called friends.

During the greatest banking crisis this country has faced, President Franklin D. Roosevelt said: "There is an element in . . . our financial system more important than currency, more important than gold, and that is the confidence of the people." You can have confidence in the year 2000 preparations of your bank. It will be business as usual at the bank today, tomorrow, during the year 2000, and beyond.

Thank you.

A year 2000 checklist for financial services

How can you prepare for the year 2000? You're already taking the sensible first step -- educating yourself by attending a forum such as this. Here are a couple of other tips:

- Your bank is absolutely committed to making it business as usual for you before, during and after the century date change. But business as usual means that you continue to *keep your bank receipts and statements*, as you always do. In a bank, the word "balance" has nearly religious significance. There are layers of experienced supervisory staff behind each teller that spring into action in an out-of-balance situation. Coupled with back-up bank records, your receipts and statements are a one-two punch that is the closest thing you can get to a guarantee that you and your bank will knock out any glitch that may occur in the shortest possible time.
- **Balance your checkbook regularly and check your statements** for accuracy.
- **Remember all your payment options** -- checks, credit cards, debit cards, ATMs, and tellers will work.
- **Be skeptical** if someone asks for your account information or tries to sell you a product, service or investment that supposedly is Y2K safe. If it sounds too good to be true, it probably is.
- **Protect your personal information**, including your bank account, credit card, and Social Security numbers. Never give out account information unless you initiated the contact, and never give out your personal identification number (or PIN) for any reason. Banks don't need that to get their job done.
- **Report suspicious requests** or calls to the police and your bank.
- **Check the accuracy of your bank statements** soon after they arrive.
- When you need help sorting fact from fiction, **go to a knowledgeable trusted source** such as the police, your bank or a banking regulator.
- **Review your FDIC deposit insurance coverage** with your banker. The federal government's protection of insured deposits will be in place for Y2K.

Mrs. BIGGERT. Next we have Leonard Harris, president, Chatham Food Center. You may proceed.

Mr. HARRIS. Good morning, Vice Chairman Biggert and Chairman Horn. Thank you for the invitation.

What I hope to do today is three things: Introduce you to FMI and what we do as an association; tell you about what we're doing to give you some assurances that we will be ready for the Y2K; and to voice our concerns.

Food Market Institute has 21,000 members. They do \$220 billion in sales, and we represent more than half of the supermarket sales in the United States. We represent national chains, local chains, and independent operators. I'm happy to say as a member of FMI, as a single store operator in the city of Chicago, that I have been closely intertwined with what's going on with the technology group, which means stores big and small are involved and being communicated to about what's going on in the industry.

What we have done; 2 years ago we issued a year 2000 white paper for the purpose of helping members understand the broad scope of the problem and to develop comprehensive solutions. The first of this year we set up an electronic share group with an Internet-based discussion platform for the purpose of members being able to access the Internet, and not only leave questions on the Internet to be answered but also to see the answers from other members who have had questions and have had their answers left on the Internet.

FMI and the Grocery Manufacturers of America have produced a joint Y2K business contingency plan framework and they've held three joint Y2K contingency planning forums. FMI is working with the Y2K Food Sector Working Group of the USDA and the President's Council on Year 2000 Conversion and Communications Industry Readiness.

There's a lot of talk in the industry about reduction of inventory levels. At one point in time, the average inventory in the pipeline was 120 days. The industry has cut that inventory level down to 60 days and its store level down to 2 weeks. We believe that will be more than sufficient inventory to deal with any contingency. We issue a quarterly newsletter and we've had seminars discussing the issue at our major convention each year in Chicago.

Our concerns are with those industries that are outside of our industry, primarily utilities and the government's food assistance program, the EBT program. Certainly there have been breakdowns in that program on an ongoing basis, and we're concerned that not only the system be running properly January 1, but also that there be no new revisions or conversions of that system before the first of the year.

Certainly I'm happy to be present here. I have been reassured, listening to the conversations and testimony from our utility groups and our transportation groups, and I will be happy to report back to our chairman and our president that this committee is doing an excellent job and we just hope that you stay on top of this. Thank you.

Mrs. BIGGERT. Thank you very much.

[The prepared statement of Mr. Harris follows:]



909 CONNECTICUT AVE., N.W.
WASHINGTON, D.C. 20006-2701
TELEPHONE: 202/452-8444
FAX: 202/429-4519
E-MAIL: FMI@FMI.ORG
WEBSITE: HTTP://WWW.FMI.ORG

**TESTIMONY OF LEONARD HARRIS
PRESIDENT, CHATHAM FOOD CENTER, INC.
CHICAGO, IL
&
CHAIRMAN, INDEPENDENT OPERATORS COMMITTEE
FOOD MARKETING INSTITUTE**

YEAR 2000 ISSUES FACING THE SUPERMARKET INDUSTRY

**BEFORE THE UNITED STATES HOUSE OF
REPRESENTATIVES
COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION AND TECHNOLOGY**

**JULY 8, 1999
NAPERVILLE, IL**



YOUR NEIGHBORHOOD SUPERMARKETS

© 1999 by Food Marketing Institute

Mr. Chairman, Vice Chairwoman Biggert and Distinguished Members of the Committee:

Thank you for the opportunity to testify on Year 2000 issues facing the supermarket industry. The Food Marketing Institute (FMI) very much appreciates the leadership that this Committee has shown to identify potential Y2K problems as well as solutions. With the new millennium now only 176 days away, it is indeed time for industry and government to assess our readiness and ensure that we are prepared to meet this technological challenge.

Food Marketing Institute (FMI) is a nonprofit association that represents food retailers and wholesalers in the United States and around the world. FMI's domestic member companies operate approximately 21,000 retail food stores with a combined annual sales volume of \$220 billion — more than half of all grocery store sales in the United States. FMI's retail membership is composed of large multi-store chains, small regional firms and independent family-owned supermarkets. Its international membership includes over 200 members from 60 countries. In addition to the recognizable names of large food chains, over half of FMI's membership is composed of independent operators. As the Chairman of FMI's Independent Operator Committee, and a member of FMI's Board of Directors, it is that perspective I would like to share today.

The food industry has taken the Year 2000 technology problem very seriously. We have spent extensive time and resources identifying, correcting and testing potential problems. We now must assure the public of our readiness to prevent overreaction or panic. The role of our elected leaders at the federal, state and local levels in disseminating accurate, responsible information cannot be understated. Toward that end, I appreciate your holding this hearing. There are several points I would like to highlight today regarding Y2K preparations.

- First, we want to assure you and the public that the food industry will be ready when January 1, 2000 arrives. Today, the industry is well beyond analyzing the problem. We are now testing our solutions — both within companies and industrywide.

-
- Second, there are Y2K issues beyond the control of our industry; for those we need government's help. Specifically, we need government's help to maintain our nation's power, water, natural gas and communications grids so that food products can be processed and transported and we can provide the refrigeration necessary to safeguard our food.
 - Third, we urge the government also to ensure the viability of our food-assistance programs during the Y2K transition. I see every day how important these programs are to the Americans who depend on them. We believe any major new revisions in the conversion to computer-based electronic benefits programs now underway need to be delayed until after the critical date has passed.
 - Finally, should the Y2K problem cause any disruptions, we want to remind everyone that the supermarket industry — more than any other — is well accustomed to operating in even the most trying circumstances. We have proved this capability again and again under every conceivable hardship (earthquakes, floods, hurricanes, snow and ice storms).

Industry history supports our reassurance. The first grocers marked prices with grease pencils and made change out of cigar boxes. Yes, it is true that the industry has made great advances in applying computer technology since those early days. Like every business, our computers go down from time to time and supermarkets continue to stay open with a full inventory of products using contingency plans that have withstood the test of time. Industry research gives us every reason to believe that any disruptions will be minimal. This is good news for our industry and the public.

Secretary Glickman shared a similar assessment of our industry on February 5, 1999, when he said, "The state of readiness within the food industry is encouraging. The Food Supply Working Group's initial analysis suggests that the American public can be confident that the major domestic companies, which provide most of the key foods, will continue to operate in spite of the Year 2000 problem."

This degree of readiness is not surprising since the industry has been focusing on Y2K issues for several years. In addition to my oral testimony, I would like to provide you with a copy of FMI's Year 2000 white paper, *The Millennium Crisis*. FMI issued this paper more than two years ago to help our members understand the broad scope of the problem and develop comprehensive solutions.

Earlier this year, FMI established an electronic share group, of which I am a member, for the discussion of Year 2000 issues facing our industry. This Internet-based discussion platform allows members -- large and small -- to share solutions to Year 2000 problems. Sharing information is critical and we appreciate Congress' efforts to provide liability protection for information sharing between companies by passing the Year 2000 Information Disclosure Act last year and the broader Year 2000 Readiness and Responsibility Act, just last week.

Obviously, the relationship between retailers and suppliers is critical to ensuring that inventories are replenished and available for customers. We are working closely with our suppliers. FMI and the Grocery Manufacturers of America recently produced a joint Y2K Business Contingency Planning framework and then held three joint Y2K Contingency Planning Forums to discuss issues impacting the supply chain. FMI is also working closely with the Y2K Food Sector Working Group at USDA and the President's Council on Year 2000 Conversion to communicate food industry readiness information to consumers.

I would like to put one more concern to rest for you. You may have heard that the food industry has worked hard to become more efficient over the last several years and that these efforts have included eliminating unnecessary inventory supplies. While this is true, and the results have clearly benefited consumers who now spend a record low percentage of their incomes on food, several weeks of inventory remain in the pipeline between farm and table. The levels of supply on hand throughout the system are more than adequate to take us well into the new year.

Turning now to the industry's need for government support, I would like to point out that the Food Stamp Program along with the Women, Infants and Children program are critical elements to providing a nutritious diet to low-income families. We need government support and assurance that those food-assistance programs have been tested, will be operational and contingency plans are in place well in advance of December 1999. We are working with USDA and ask for your help as well to continue to look at the readiness of the food assistance programs — especially those that now rely on electronic benefits transfer systems. Our request is rather straight forward. Do not put new burdens on retailers in the last months of this year to make computer changes that could affect Y2K readiness of food assistance programs, particularly for new technologies such as "smart cards."

I could list a number of specific concerns that warrant Congress or others stepping in to help reduce the risks of Year 2000 failures. Most relate to the maintenance of the national power grid, including electricity, communications, water and gas. I appreciate hearing the testimony of witnesses from the utilities here today, and just want to reiterate what you have already heard from others: like many other consumer-service businesses, the retail food industry relies extensively on power, and we need the government to ensure that the power grids remain functional as we move into the year 2000.

The work this Committee is doing to ensure that critical systems are operational on January 1, 2000, and beyond is very important and should be commended. I want to reassure consumers that the food distribution industry takes Year 2000 issues very seriously. Stores will be open with an ample supply of food on January 1st. This commitment will be a challenging one, and the entire food industry is responding accordingly.

Again, thank you for the opportunity to testify.

Mrs. BIGGERT. Delores Croft, seniors policy advisor, Office of Attorney General Jim Ryan. Thank you for coming in. You may proceed.

Ms. CROFT. Good morning, Chairman Horn and Vice Chair Biggert. By now you are familiar with the term Y2K. I will attempt to give you a different perspective on how others will use Y2K as a means of exploiting you.

Fraud is a big business in America, taking in about \$100 billion a year according to the U.S. Office of Consumer Affairs. Law enforcement officials believe that seniors are the targeted customers. The FBI estimates that approximately 10 percent of the Nation's 140,000 telemarketing firms are fraudulent and nearly 80 percent of the crooked companies target seniors.

Y2K provides another opportunity for unscrupulous individuals and companies to scam the seniors. This is a time that con artists will choose to prey on the elderly. They will attempt to cash in on fears about the year 2000. Beware of people telling you where to hide your money. Some hiding places being recommended to seniors are wrap your money in aluminum foil and place it in the freezer, wrap it in dirty laundry and hide it in the laundry. Stuff the money in your spare tire in the trunk of your car. Remember, the same people that tell you where to hide it will be the very ones to return and to rob you.

One senior stated to me that she was told, "Your money is safe in the house of the Lord." Beware of these statements where you are told that you should remove your money from the bank and place it elsewhere.

Be especially weary of phone solicitors. Many times they will call and want you to verify certain personal information. They may ask for your bank account number, stating that they're calling from the bank. They may ask you to tell them the last purchase that you charged on your credit card. And because your cards are supposedly insured, they may ask you to verify exactly how many cards you have and at some point during the conversation, they may ask you for your card number. Beware.

Social Security numbers also provide a means for the con artist to claim a new identity—yours. Beware. Con artists prey on seniors all year, not just during the Y2K period. Remember, don't make purchases for your home or auto from unfamiliar companies. Take your time before making a decision, consult others that you trust such as family members or friends. Be suspicious when a salesman or telemarketer tells you that you must make the purchase so that there will be ample opportunity for it to be in place before the new year.

What can you do to be prepared? You should prepare for an emergency that might arise from a Y2K problem as you would prepare for any other emergency situation. Just keep in mind that con artists materialize during emergency situations. Before allowing any stranger into your home, ask for a picture identification first. If in doubt, call the company or agency they work for. This includes employees from the gas company, the light company, and the telephone company. You should not have any difficulty verifying your local policeman or fireman because they should be in a marked car or truck. However, if in doubt call the agency first. If you have any

questions, do not hesitate to call the Attorney General Jim Ryan's Senior Citizen Hotline at 1-800-243-5377.

And Illinois Attorney General Jim Ryan would like to thank you for inviting the office to give testimony on this important issue.

[The prepared statement of Mr. Ryan follows:]

ILLINOIS ATTORNEY GENERAL
JIM RYAN

FRAUD AND THE Y2K

By now, you are familiar with the term Y2K. I will attempt to give you a different perspective on how others will use Y2K as a means of exploiting you.

FRAUD is big business in America, taking in about 100 billion a year according to the U.S. office of Consumer Affairs. Law Enforcement officials believe that seniors are the targeted customers. The FBI estimates that approximately 10% of the nations 140,000 telemarketing firms are fraudulent and nearly 80% of the crooked companies target seniors.

Y2K provides another opportunity for unscrupulous individuals and companies to scam the seniors.

BEWARE OF CON ARTISTS

This is a time that con artists will choose to prey on the elderly. They will attempt to cash in on fears about the year 2000. Beware of people telling you where to hide your money. *Some hiding places being recommended to seniors are:*

- Wrap you money in aluminum foil and place it in the freezer.
- Wrap it in dirty laundry and hide it in the hamper.
- Stuff the money in your spare tire (in the trunk of your auto).

Remember: The same people that tell you where to hide it, will be the very ones to return and rob you.

One senior stated to me that she was told "Your money is safe in the house of the Lord." Beware of these statements where you are told that you should remove your money from the bank and place it elsewhere.

Be especially wary of phone solicitors! Many times they will call and want you to verify certain personal information. They may ask for your bank account number, stating that they are calling from the bank! They may ask you to tell them the last purchase that you charged on your credit card and because your cards are insured they may ask you to verify exactly how many credit cards you currently have. At some point in the conversation, they may ask for your card number. **BEWARE.** Social Security numbers also provide a means for the con artist to claim a new identity.....**YOURS!** **BEWARE!** Con artists prey on Seniors all year, not just during the Y2K period.

Remember:

- Don't make purchases for your home or auto from unfamiliar companies.
- Take your time before making a decision. Consult others that you trust, such as, family members or friends.
- Be suspicious, when a salesman or telemarketer tells you that you must make the purchase, so that there will be ample opportunity for it to be in place before the new year.

WHAT CAN I DO TO BE PREPARED?

You should prepare for an emergency that might arise from a Y2K problem as you would prepare for any other emergency situation. Just keep in mind that con artists materialize during emergency situations.

Illinois Attorney General Jim Ryan would like to thank you for inviting the office to give testimony on this important issue.

Remember:

If you have any questions do not hesitate to call Attorney General Jim Ryan's Senior Citizen Hotline at 1-800-243-5377.

Before allowing any stranger into your home, ask for a picture identification first. If in doubt, call the company or agency they work for first. This includes employees from the gas company, light company and telephone company. You should not have difficulty verifying your local policeman or fireman because they should be in a marked car or truck, however if in doubt call the agency first.

Mr. HORN. I congratulate you on that statement. Yesterday in Topeka, another distinguished resident of Chicago, IL who happens to have her column in the Kansas City paper—and that's Ann Landers—she had a great column yesterday on just the point of the senior citizen fraud by the Y2K bit. They're phoning up saying that we're from the bank, of course; we're checking; we want to move your money from accounts into the bond accounts so they can't be hurting you in any way, and all this nonsense. So you've got a lot of scum out there that are going to take advantage of senior citizens throughout America.

Thank you for making the point. Ann Landers closed her column with saying call your State Attorney General's office.

Ms. CROFT. Good. We'll be there to answer.

Mrs. BIGGERT. Thank you for your testimony.

Next we have Ron Clark, treasurer, Illinois Ayers Oil Co., representing the National Association of Convenience Stores. You may proceed.

Mr. CLARK. Vice Chair Biggert and Chairman Horn, thank you for inviting us here today. Our company in west central Illinois operates 27 convenience stores, doing business as Ayerco Convenience Centers. All of our stores sell convenience goods and 25 of our stores sell gasoline.

We are happy to be able to provide this testimony on how Illinois Ayers Oil Co. and the convenience store and petroleum marketing industry have responded to the year 2000 challenge.

I appear before you representing NACS as you stated, an international trade association representing over 2,100 retail members operating approximately 65,000 convenience stores nationwide. Convenience stores sell 55 percent of all U.S. gasoline. Approximately 2,700 convenience stores are operating within the State of Illinois.

Illinois Ayers began assessing its software and hardware for Y2K compliance in spring of 1998, followed by the upgrade of non-compliance stores, including the installation of new systems and training store employees on those systems. Overall we've budgeted approximately \$350,000 for equipment alone, such as the new personal computers and point-of-sale terminals.

Probably the biggest area of concern for Illinois Ayers was the supply of gasoline and convenience goods to our retail sites. In contacting each of our 12 fuel suppliers, we found that most were either in the midst of, or had already completed, their Y2K readiness. We use one grocery supplier for our entire chain, and they have assured us that they are compliant and we should not experience any disruption in deliveries. At this time our Y2K readiness is approximately 85 percent complete.

The central point Illinois Ayers and NACS wish to make is that unless they are without electricity for extended periods of time, the vast majority of convenience stores should adhere to their normal operating hours on January 1, 2000. NACS has provided industry retailers with information and resources to assist them in achieving Y2K compliance, and through NACS our industry is represented on the President's Council on the Year 2000 Conversion as part of both the Oil and Gas Sector Working Group and the Food Supply Working Group.

According to the results of the NACS year 2000 survey released just this week, these efforts are bearing fruit. The survey found that 95 percent of store owners and petroleum marketers planned to be Y2K ready by November 30, 1999. By November, also, 94 percent of the respondents plan to have a contingency plan in place; that is, a plan of action for dealing with uncertain operational events caused by the Y2K problems.

Sixty-five percent of respondents have been gathering equipment compliance documentation from business partners, while 20 percent have been conducting joint contingency planning. The NACS survey also found that the majority of industry operators, 72 percent, are concerned about the possibility of consumer overreaction to Y2K in the manner of hoarding food, gasoline and/or money. This finding will become more important as we near the close of 1999. Retailers are deservedly skittish about consumer reaction during the last few weeks of 1999 and into the year 2000. Consumer reaction is the wild card in all of our industry Y2K efforts.

While the aforementioned responsible efforts and survey results should help allay any consumer concern, we're also well aware that a minority of consumers will remain concerned. For that small minority, NACS urges that they act responsibly.

Specifically regarding gasoline, we suggest that concerned consumers make sure to keep their gasoline tanks at least half full starting in early December. As for the storing of extra gasoline, NACS urges extreme caution. Consumers should contact their local fire department for more information on the rules and regulations governing gasoline handling and storage. If consumers do not overreact, we do not expect either gasoline rationing or shortages. We also urge all consumers to seek information from responsible parties. The President's Council on Year 2000 Conversion can be reached via phone at 1-888-USA4Y2K or via the Internet at www.y2k.gov.

In addition, the Council's Oil and Gas Sector Working Group and Food Supply Working Group have Web pages offering responsible information on our industry's Y2K readiness as well as consumer information. Through such meetings and hearings as this, as well as retail industry and public education efforts, consumers should begin to feel more confident. NACS and Illinois Ayers stand ready and willing to assist as our means dictate in any efforts to ensure that consumers know that the convenience store and petroleum marketing industry is preparing for Y2K.

Again, I thank you for inviting me to appear today. I would be pleased to answer any questions.

Mrs. BIGGERT. Thank you very much.

[The prepared statement of Mr. Clark follows:]

**TESTIMONY OF RON CLARK
TREASURER, ILLINOIS AYERS OIL COMPANY
ON BEHALF OF
THE NATIONAL ASSOCIATION OF CONVENIENCE STORES
BEFORE THE
HOUSE COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION, AND TECHNOLOGY
FIELD HEARING ON
JULY 8, 1999**

Good morning, Mr. Chairman and Representative Biggert. I am Ron Clark, Treasurer of Illinois Ayers Oil Company of Quincy, Illinois. Our company operates 27 convenience stores doing business as Ayerco Convenience Centers. All of our stores sell convenience goods, and 25 of our stores sell gasoline.

Thank you for inviting me to testify this morning on how Illinois Ayers and the convenience store and petroleum marketing industry have responded to the Year 2000 challenge.

I appear before you representing the National Association of Convenience Stores or "NACS." NACS is an international trade association representing over 2,100 retail members operating approximately 65,000 convenience stores nationwide. Approximately 2,700 convenience stores operate in the State of Illinois. According to a 1996 Gallup poll, 96 percent of Americans shop at convenience stores, with nearly half of those shopping at least twice a week. These retail outlets offer three types of products:

- In-store merchandise, that is, the convenience foods and products used by consumers on a daily basis, such as bread, snack foods, edible and perishable groceries, milk and deli products, frozen foods, batteries, and health and beauty care items;
- Foodservice, including co-branded quick serve restaurants, food prepared on-site, packaged sandwiches, and hot, cold and frozen dispensed beverages; and
- Motor fuel, including gasoline, diesel fuel and other motor fuels. According to NACS, convenience stores sell approximately 55 percent of all gasoline sold in the United States.

In addition to the aforementioned, many convenience stores offer other customer services, such as automated teller machines (ATMs), check cashing, lottery sales, money orders, video rentals, photocopy and facsimile machines, postal services and car washes.

Illinois Ayers began the process of ensuring its software and hardware would successfully interpret the Year 2000 date code in the Spring of 1998. As with most companies and organizations, we began by conducting an audit of all our store and headquarters' equipment and software, dividing responsibilities, and working with business partners—that is vendors, suppliers, service providers and financial institutions—to assess their Y2K readiness.

For convenience stores, the critical areas include scanners, point-of-sale terminals, gasoline dispensers, card readers, back office systems, security systems, refrigeration units, lottery terminals, food preparation equipment, electronic links to home office and vendors, ATMs, energy systems, underground petroleum storage tank monitors and leak detection systems. These are the some of the same areas assessed by Illinois Ayers for Y2K compliance.

Following our assessment of Y2K compliance, we began upgrading our non-compliant stores, including the installation of new systems and training store employees on those systems. Overall, we budgeted \$350,000 for equipment alone such as new personal computers and point

of sale terminals. We still have employee training expenses to account for and the costs of testing to ensure everything is working properly. Testing includes such processes as running sample sales through the cash register, sample transactions through gasoline dispenser card readers, and testing lottery transactions.

Currently, we are upgrading our back office computers and point of sale terminals on a schedule of two per month. That process is nearly half complete, and we expect to have this area fully Y2K compliant by the end of November 1999.

Probably the biggest area of concern for Illinois Ayers was the supply of gasoline and convenience goods to our retail sites. That meant contacting each of our fuel suppliers to assess their level of Y2K readiness. Our company uses 12 different fuel suppliers at 10 different terminals. Not only do the suppliers need to be compliant, but also the terminals through which the product is delivered need to be compliant. In contacting each supplier, we found that most were either already in the midst of their Y2K upgrades or had completed them. We use one grocery supplier for our entire chain, and they have assured us they are compliant and that we should not experience any disruption in deliveries.

At this time, our Y2K readiness is approximately 85 percent complete. I can say with a great deal of certainty that our business should continue its normal business operations on January 1, 2000, barring any unforeseen circumstances.

The central point that both Illinois Ayers and NACS wish to make today is that unless they are without electricity for extended periods of time, the vast majority of convenience stores should adhere to their normal operating hours on January 1, 2000. The convenience store and petroleum marketing industry has and continues to seriously address its obligation to prepare for the Year 2000.

Since 1998, NACS has provided industry retailers, such as Illinois Ayers, with information and resources to assist in achieving Y2K compliance, including a free video and guidebook, compliance and contingency planning manuals, legal advice and workshops at Association conventions.

In addition, through NACS, our industry is represented on the President's Council on Year 2000 Conversion as part of both the Oil and Gas Sector Working Group and the Food Supply Working Group.

Through such efforts, NACS has attempted to ensure that the convenience store and petroleum marketing industry successfully transitions to the Year 2000. According to the results of a NACS Year 2000 Survey, released just this week, these efforts are bearing fruit. The NACS survey found that 95 percent of convenience store owners and petroleum marketers plan to be Y2K ready by November 30, 1999.

In addition to this important finding, the NACS Survey found:

- Industry retailers are actively engaged in contingency planning, that is, developing a plan of action for dealing with uncertain operational events caused by Y2K problems. Thirty percent of respondents said they already have a contingency plan in place and are testing simulations; 11 percent have a completed contingency plan; 46 percent are in the initial stages of developing a plan; and 13 percent have not yet developed a contingency plan. Ninety-four percent of respondents plan to have a contingency plan in place prior to November 30, 1999.
- As part of their Y2K readiness efforts, industry retailers have been working with their business partners to ensure retailers have the necessary Y2K compliance information for store equipment and the continued fulfillment of products and services prior to and after January 1, 2000. Sixty-five percent of survey respondents said they have been gathering Y2K

compliance documentation for their equipment, while 20 percent have been conducting joint contingency planning. Seventy-one percent of industry retailers have been working with their business partners on Y2K compliance issues for at least 6 months.

- Respondents indicated that the following store equipment has been validated as Y2K compliant: motor fuel dispensers (85 percent); credit and debit card readers (85 percent); point-of-sale scanners (77 percent); point-of-sale terminals (86 percent); back office computers (83 percent); ATMs (75 percent); underground storage tank monitors (78 percent); and leak detection systems (72 percent).
- Fifty-three percent of respondents said they have a company employee working on their Y2K readiness; 44 percent have assembled a team; and 20 percent have retained third-party consultants.

Obviously, the NACS Year 2000 Survey found that as an industry we still have some Y2K readiness work to complete in certain areas. But overall, the Survey's findings are evidence of our industry's serious efforts to ensure consumers have regular and continued access to the convenience goods and gasoline they require before and after January 1, 2000.

It is important to note that the NACS Survey also found that the majority of industry operators—72 percent—are concerned about the possibility of consumer overreaction to Y2K, in the manner of hoarding of food, gasoline and/or money.

This finding will become more important as we near the close of 1999. Retailers are deservedly skittish about consumer reaction during the last few weeks of 1999 and into the year 2000. Consumer reaction is the "wild card" in all of our industry's Y2K efforts.

It is the hope of Illinois Ayers and NACS that the aforementioned responsible efforts and Survey results will help allay any consumer concerns that convenience goods and gasoline will not be available come January 1, 2000.

However, we are also well aware that, regardless of all our planning and actions, a minority of consumers will remain concerned about the availability of convenience goods and gasoline as we approach January 1. For that small minority, NACS urges that they act responsibly.

Specifically regarding gasoline, we suggest that concerned consumers make sure to keep their gasoline tank at least half full starting in early December 1999. As for the storing of extra gasoline, NACS urges extreme caution. Gasoline, like any flammable product, can be dangerous if handled or stored improperly. Consumers should contact their local fire department for more information on the rules and regulations governing the handling, storage and disposal of gasoline. If consumers do not overreact, NACS does not expect either gasoline rationing or shortages.

We also urge all consumers to seek information from responsible parties. The President's Council on Year 2000 Conversion can be reached via phone at 1-888-USA-4-Y2K, or via the Internet at www.y2k.gov. In addition, the Council's Oil & Gas Sector Working Group Web page can be accessed at www.ferc.fed.us/y2k/index.html. And the Council's Food Supply Working Group Web page can be accessed at www.usda.gov/aphis/FSWG. Each of these Web pages offers responsible information on our industry's Y2K readiness efforts and status, as well as consumer information.

Through such meetings and hearings as this, as well as retailer and industry public education efforts and the Community Conversations that are part of the President's Council on

Year 2000 Conversion, consumers should begin to feel more confident that, to paraphrase President Clinton, the Year 2000 challenge will be the last great challenge of the 20th century, not the first big challenge of the 21st century.

NACS and Illinois Ayers stand ready and willing to assist, as our means dictate, in any efforts to ensure that consumers know that convenience store and petroleum marketing industry is preparing for January 1, 2000.

Again, I thank you for inviting me to appear today. I would be pleased to answer any questions you may have regarding my testimony.

Ron Clark is Treasurer of the Illinois Ayers Oil Company in Quincy, Illinois. He is a May 1975 graduate of Quincy College (now University) with a Bachelor of Science degree in Accounting, and for 15 years, he has been a member of the Institute of Management Accountants. Prior to joining Illinois Ayers, Mr. Clark served for 15 months as a manager with a national retailer. In November 1976, Mr. Clark was hired as Controller of Illinois Ayers and has remained in the company's employ. In 1989, he was elected to the Illinois Ayers' Board of Directors and was named Treasurer. During his tenure, Mr. Clark has been active in the evolution of the company from the traditional tank wagon service company to today's 27-site chain of convenience stores.

Mrs. BIGGERT. Next is Monty Johnson from Citgo, representing the American Petroleum Institute.

Mr. JOHNSON. Thank you. First of all, I want to thank Mr. Horn and Mrs. Biggert for the opportunity to be here today. I am particularly pleased to be in Naperville. I had a chance to walk around your beautiful city last night, and I plan to come back.

With the help of staff, I'm going to step through a quick slide presentation. I'm here really in my role as chairman of the Public Information Group of the American Petroleum Institute's Y2K Task Force.

Explain the role of the task force: It is approximately 50 of the major oil companies that began in 1997 meeting every 6 to 8 weeks to share information, do benchmarking studies, set up committees on key areas of the Y2K issue and share information with both the government and the public.

Some of the things that we've accomplished so far: We have a very comprehensive Website where we share information not only among the member companies but also with the public. We've established a data base of readiness information on equipment that's common throughout our industry. We've interfaced considerably with other industry organizations.

Mr. Clark's presentation was a good lead-in because NACS is one of the areas that we coordinate with very closely.

We've established a contingency plan framework that all of our member companies are following, just so we have some consistency in exchanging information among ourselves. We've set up an effort to meet with all our supply chain partners because many of us in the petroleum industry deal with the same suppliers and vendors, so rather than 50 of us contacting a pump supplier, for instance, we can contact them once and get the information and share it among our members.

We've also set up standards for testing embedded systems. We're very involved currently on assessing the readiness of some of the international supply areas.

Mr. Horn, you mentioned Russia. A number of our member companies operate around the world. So our companies have a very personal interest in assuring the readiness of the infrastructure of those companies to support their operations. And our task force is also the focal point for the government for the oil industry.

The next slide talks about our role as the focal point of the industry to the President's Council. The President's Council has been mentioned several times today but the API Y2K task force is the focal point for the oil and gas industry. The other segments of that task force are shown there and our reports are given quarterly to FERC as we report the findings of surveys that we've done quarterly to assist the readiness of the overall industry.

Next slide shows members of the task force, which shows it is a pretty broad representation of all the major segments of the oil and gas industry.

Gas Processors Association: We had gas utility reporting on their readiness efforts a little earlier.

The Petroleum Marketers Association of America: We don't have NACS directly in our reporting relationship, but we're certainly sharing information and coordinating a lot of effort, since many of

our member companies market our products through convenience stores.

The current focus of our activities: We have ongoing working groups, and this is representatives from our member companies that are focusing on the specific areas of embedded systems, retail automation, all the dispensing equipment, point-of-sale equipment at our retail operations.

Supply chain, both the vendors and suppliers that provide services and equipment to our companies as well as our customers downstream. We believe a disruption anywhere in that supply chain could have a severe impact on our ability to operate, so we're concerned with not only what's upstream of us but also what's downstream.

International issues as they relate to our domestic operations: Contingency planning is a big focus currently. And public information is the reason I'm here today.

We do benchmarking studies every 6 to 7 weeks among our member companies, and this has been a tremendous help to us in sharing information and helping us all find out if we have common problems. We can come up with solutions that we can share among our members. We feel like this has saved us a tremendous amount of time and effort that we each would have had to do individually had we not had this information sharing operation.

Hot issues for this year. Managing public perception: A number of people have mentioned today that public reaction to the Y2K issue is probably a bigger concern than some of the technology issues, and that's very much our belief.

Cross industry reliance: We're very active in sharing information with both the electric utilities and the telecommunications industry since those are where we feel our greatest vulnerabilities are, and we have a very high confidence that those facilities will be in operation.

Contingency planning is our big focus, and international vulnerability as it relates to our ability to supply products and have gasoline at the pump when you need it.

In summary, our oil and gas companies are focusing on our operations to be reliably able to have the gasoline there when you want it. Our efforts are very comprehensive, all the way from planning the effort to resolving the problem. All of our companies are currently in either their remediation or contingency planning stages and very near resolution, and we feel we're well on the way to Y2K readiness.

And with that, I'll focus your attention on a news release, copies of which are outside, and you have a copy for the record.

These are the results of a survey of 1,250 oil and gas companies that are task force conducted. The results were reported on June 28th after they were presented to FERC and this shows that of these 1,250 companies, 95 percent of them showed that they are going to be Y2K ready by September of this year, and the results

of this survey represent 93 percent of the domestic oil and gas demand in the country. So it is a very high representation of the industry and their ability to provide services.

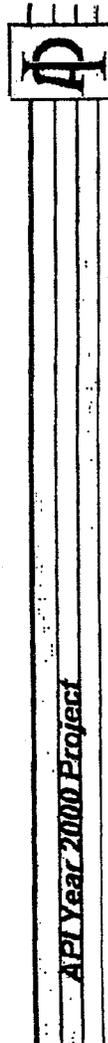
With that, I'll be prepared to answer questions.

Mrs. BIGGERT. Thank you very much.

[The prepared statement of Mr. Johnson follows:]

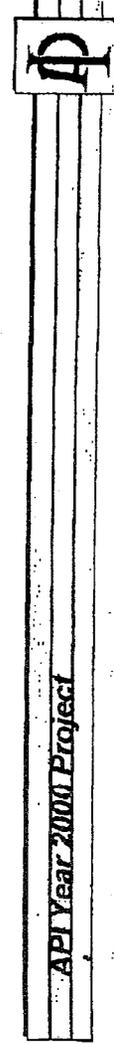
An Industry-Wide Approach to the Year 2000 Challenge

Monty Johnson
Member, API Year 2000 Task Force
Representing CITGO Petroleum Corporation
Tulsa, OK



American Petroleum Institute Year 2000 Task Force

- 50+ Companies - All The Majors
- First activity mid-1997
- Meets Every 6-8 Weeks
- Task Force Objectives:
 - **Benchmarking**
 - **Shared Learnings**
 - **Committees Coordination**
 - **Government & Public Information**



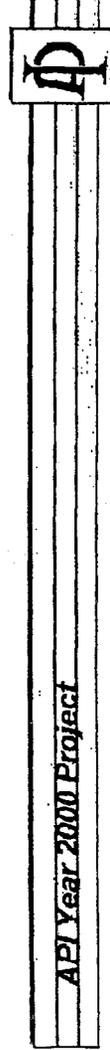
API Y2K Task Force Activities / Accomplishments

- **Comprehensive Web Site Repository**
- **Establish Industry Readiness Database**
- **Interface with Other Industry Associations**
- **Contingency Plan Framework**
- **Supply Chain Trading Partners Liaison**
- **Embedded Systems Test Procedures**
- **International Sub-Team**
- **Government Focal Point for Oil Industry**



President's Council on Y2K Conversion

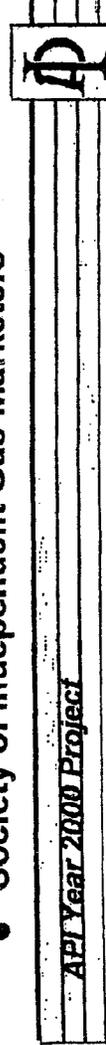
- **34 Agencies Represented, 5 joint sector groups**
 - Financial
 - Telecommunications
 - Workplace Issues
 - Transportation
 - Energy (Electric / Utility + Oil & Gas)
- **API Serving as Oil Industry Focal Point**
- **Industry-wide Surveys; Reports to FERC**



President's Council on Y2K Conversion

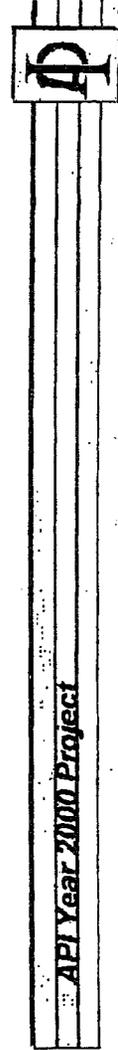
Oil Industry Working Group

- American Petroleum Institute
- Association of Oil Pipe Lines
- Australian Institute of Petroleum
- Canadian Association of Petroleum Producers
- Gas Processors Association
- Independent Petroleum Association of America
- Interstate Oil & Gas Compact Association
- National Petrochemical & Refiners Association
- Petroleum Marketers Association of America
- Petroleum Technology Transfer Council
- Society of Independent Gas Marketers



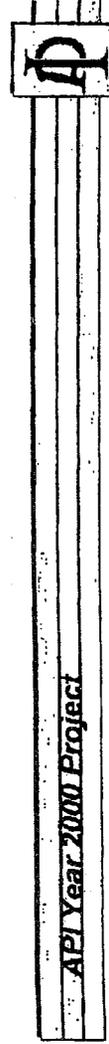
API Y2K Task Force Working Groups

- Embedded Systems
- Retail Automation
- Supply Chain
- International Issues
- Contingency Planning
- Public Information



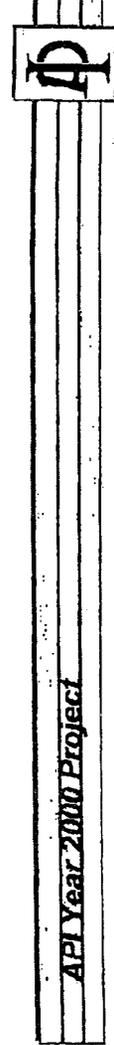
API Y2K Task Force Benchmarking Activities

- Benchmarking survey every 6-7 weeks
- 30-40 Task Force companies
- 70+ questions, 10 categories
 - Communication
 - Program Management
 - Legal
 - Field Systems
 - Supply Chain
 - HW / System Software
 - Telecommunications
 - Contingency Planning
 - Applications (approach)
 - Applications (types)



**API Y2K Task Force
Hot Issues for 1999**

- **Managing Public Perception**
- **Cross Industry Reliance**
- **Contingency Planning**
- **International Vulnerability**



API Y2K Task Force Summary / Conclusions

- **Oil and Gas Industries Focusing on Operations**
- **Y2K Efforts Comprehensive: Planning to Resolution**
- **Y2K Readiness Currently in Remediation & Contingency Planning, Moving Toward Resolution**
- **Industry Well on Way to Year 2000 Readiness**

295



Thank You!

Monty Johnson
Communications Coordinator
Year 2000 Project Team
CITGO Petroleum Corporation
TEL 918.495.5422
FAX 918.495.5407

E-MAIL
mojohns@citgo.com
citgoy2k@citgo.com



Mrs. BIGGERT. I think I'll skip over Mr. Paulson, our author, for just a moment and go to Mike Skarr who is the president and CEO of the Naperville Area Chamber of Commerce to talk about businesses, and then we'll come back to you.

Mr. SKARR. Thank you, first of all, for your flexibility in listening to a few comments I've got. I will be very brief today. First of all, let me thank Congress for the recent passage of legislation dealing with the potential liability issues of the Y2K issue. We lobbied very hard that legislation be passed. We think it brings a sense of sanity, hopefully a sense of sanity into a world of the future that most of us don't know very much about. So we're very appreciative of that.

For those of you who don't know, the Naperville Area Chamber of Commerce is an organization of 1,600 members. We're one of the largest Chambers in the State of Illinois. We have some of the large businesses, many who testified here today are members, down to many small home-based businesses.

We have a very active technology committee that's been in operation for over 3 years and I think ties in to many of the comments that have been made today.

Much of the testimony that's been presented today really focused on government or infrastructure services, and while I found that all very informative, I'm glad I did come. The reality is that the private sector, in my opinion, has an even greater interest in this whole area.

Using stockpiled food and using stockpiled water implies to me that businesses have been forced to shut down. Production stops, services stop, and most importantly paychecks stop. The possible economic consequences of that scenario, in my opinion, are disastrous.

We have been discussing the issue at the Naperville Area Chamber of Commerce for quite some time. There isn't a month that doesn't go by that we either don't hold a seminar or training session or include articles in our newsletter relative to the Y2K issue. I would point out, though, that America's success to a great extent rests on the shoulders of small business. Our organization reflects the composition of business in America. Y2K to a great extent is going to rest on the shoulders of small business rather than big business, ultimately to us in local communities.

As a result of that challenge, we have assembled resources for use by our members. Local resources or local solution providers are really the key issue in the Y2K case as far as we're concerned. Washington will not be solving the problems of many of our local businesses here in our community; fellow business members will.

I will leave copies of the local resources we have assembled here in our local community.

[The information referred to follows:]

The City of Naperville



Bridges

— Keeping The Naperville Community Connected



www.naperville.il.us • Cable TV - Channel 6 • 1610 AM • Naperlink Hotline - 420-6700

Brush Collection Scheduled for May and September



The city provides two brush collection options to meet the needs of all residents. In May and September, city crews collect unbundled tree and shrub trimmings measuring between 3 and 8 feet in length and no larger than 8 inches in diameter. Residents should stack brush on the parkway with the cut-end toward the curb on the Sunday before collection begins. Pick-up lasts one week and corresponds with your trash collection day as follows:

If your garbage collection day is:	Then your brush collection weeks are:
Monday	May 3 & Sept. 6
Tuesday	May 10 & Sept. 13
Wednesday or Friday	May 17 & Sept. 20
Thursday	May 24 & Sept. 27

In addition, the city offers a weekly brush pick-up option with the yard waste program. From April 1 through mid-December, small bundles of brush and bagged yard waste will be picked up on your normal trash collection day. Yard waste stickers must be placed on each item put out for collection. Stickers can be purchased at many Naperville stores or at the Municipal Center Finance Department. After November 1, bags containing only leaves are collected at no charge.

Grass, weeds, twigs and leaves should be placed in 33 gallon Kraft paper bags. Branches up to 3 inches in diameter should be bundled and secured with twine. Bundles may be as large as 4 feet in length, 2 feet in width and weigh up to 60 pounds.

For more information, visit our website at www.naperville.il.us or call 420-4190 to have a detailed brochure mailed to your home.

About This Newsletter

Welcome to *Bridges*, the City of Naperville's new resident newsletter. *Bridges* will appear with your utility bill six times each year, providing you and your family another way to keep up to date with municipal programs, services, public safety tips and events.

Along with the city's other communication vehicles listed on the front and back pages, *Bridges* connects you with important municipal information. We hope *Bridges* adds convenience and serves your information needs. We welcome your comments to continually improve the newsletter and make it a quality source of information.

May/June 1999 • Volume 1 Issue 1

What's In This Issue...

- Where to Find Us..... 1
- Community..... 1
- Home Improvement..... 1
- Noteworthy..... 1
- Municipal Calendar..... 1
- Memorial Day..... 1
- Severe Weather Communications..... 1
- Vacation Tips..... 1

Y2K Preparedness is on Track

Naperville uses high-tech software to run everything from the 911 response system to traffic lights, so before the Y2K buzz started, Naperville began working to avoid any problems in the year 2000. In fact, a team of 20 city employees representing every facet of city government has been working on it since 1997.

In 1998, the Y2K team completed an inventory of all computer applications and embedded systems. The city immediately took steps to upgrade systems that vendors indicated might fail in the year 2000. At this time, 87 percent of

our mission-critical systems meet year 2000 standards.

Naperville continues to test mission-critical systems including our water and electric distribution systems. We expect to be fully compliant by the end of July. Our suppliers, the DuPage Water Commission and ComEd, indicate that they will be ready for the year 2000.

For more information on our Y2K program, visit the website at www.naperville.il.us. The site includes links to Y2K information of all Naperville utility and communication providers including: ComEd, Nicor and Ameritech.

Mr. SKARR. I also encourage, as you listen to other testimony, encourage other business organizations to focus on developing local resources that local businesses, particularly smaller businesses, can use to become Y2K compliant and Y2K ready.

Last, I would congratulate you on the forum you've created today. It is reassuring to know that our government is in fact working on our behalf, and I thank you for the opportunity to be here today.

Mrs. BIGGERT. Thank you very much, Mr. Skarr, for those kind words.

Now, last but not least, is our last panelist, Ed Paulson, who is the author of the book, *Year 2000 Crisis Survival*.

Mr. PAULSON. Thank you for the invitation to address the committee this morning. I appreciate it. As you said, my name is Ed Paulson. I'm a local native Chicagoan and also a local western suburban resident. I'm the author of 12 business and/or technology books, including the recent book from McMillan on Y2K and specifically a consumer-oriented guide.

I'm also a registered Texas professional engineer and I have been in high technology now for longer than my nephew has been alive, but well over 20 years.

What I would like to do is, I have studied this problem, kind of cursory, for 15 years; but I would like to take what I've learned over the last 2 years of really intensively following this Y2K problem.

The good news is I think that the Y2K situation improves every day. A lot of it is due to the work of the committee, such as this one, the Senate committee chaired by Senator Bennett and Senator Dodd, and also John Koskinen and his committee. I think that the public awareness brought from these committees and bringing people in from the different industries to address what they are doing, I think everything works better with a deadline, and I think the committees have worked real well to move the United States forward.

And the good news is the United States is further ahead than anybody else in the rest of the world. There's some bad news associated with that, too, which I'll address in a moment.

Another good news item that I've seen is that the embedded controller problem is a smaller item today than it was originally assumed to be early on. I think that's good news. Is it still a problem? Yes. But is it as big a problem as everyone was afraid it was? I think the answer to that is now no. I'm hearing numbers of 2 to 3 percent as opposed to a 95-plus percent problem, which is good news for anybody.

My major domestic concern is that if people do not prepare for Y2K eventualities, that they may at the last minute start to panic. I go back to my situation of trying to buy a snow blower last January here in Chicago. I would call, and 15 minutes later, four snow blowers would have gone out of the local Menard store.

I had this flash when I was going through that situation last January. I had this flash in my head of what would it be like January 1st, 2000, if all of a sudden the power did go out for whatever reason, and the gas did go out for whatever reason, and people now

go to their local grocery store to buy food and they find out everyone else has had the same idea and the shelves are barren.

All of a sudden now, I think people can start to kick in a whole new level of concern, and that concerned me. So that's why I'm out talking to people, saying please take this problem seriously. It is not going to be the end of the world. We're not going to have Mad Max Beyond Thunderdome happening in January, but we are going to have, I think, a possibility of a problem arising. And I think if people prepare for that, we'll be better served going into the new year. I'll talk a little bit more about that in a moment.

The other uncertainty I have and concern I have is international, and that I think the United States is well ahead of the rest of the world, but that means everyone else is behind us. I think that presents problems from both an economic perspective in that if I need a part for a car and that part is in Korea and I need to get that part for domestic production, what's the possibility of me getting that part in?

The second one is a humanitarian issue, and that it is cold in Siberia, and if those people don't have food, water, and/or services, I think the United States and the other more ready countries may have the humanitarian position put in where we're having to assist these other countries. And I would suggest contingency planing in those areas. It may indeed be going on and I don't know about it, but I think that's an area that the more prepared countries are going to have to deal with.

Here at home, I think folks can take a look around their house to see what the susceptible devices are. The ones that are most susceptible are the ones that have day, date, and year associated with them. Your VCR, if you are one of the few people who can actually program one and you do take advantage of that, if—there is a good chance that it may or may not have a Y2K problem. It is worth it to check it out.

Home computer absolutely should be checked out, including the applications on it. Believe it or not, your camera may be because it puts a little day and date on it. It may have a problem in that the year 2000 is a leap year, but a lot of people didn't know that when they were creating the programs so there are possibilities of problems in that area, and also watches could be a problem.

Devices, though, that are on a 24-hour timer or devices that are event driven, do not have that kind of exposure. So your car, stove, refrigerator, microwave, TVs, those kinds of things will not typically have problems unless they have a day or date associated with them.

So I would suggest that people prepare for sporadic outages. Why? Because the problem is simply so complex. 85 to 95 percent of bugs can be caught in advance of putting them into production. That's basically a software industry standard. That means 5 to 15 percent are not caught. Because of that, when you started adding those 5 to 15 percents together through large networks, there's a higher than likely possibility of something going wrong. Not to the end of all utilities as we know them, but I think sporadic outages.

I'm concerned, too, that if people don't take individual responsibility, that—if they try to rely on the local services of FEMA and/or the local community services, that they're going to be in a posi-

tion where they're going to be disappointed. Because those folks are going to be busy taking care of other problems.

On the top of page 3, you'll see a preparation matrix which I won't go through in detail, other than there's two down here at the bottom that you'll see if the public is not prepared and there are no Y2K problems, we're just flat lucky; and if there are Y2K problems and the public is not prepared, we could have panic and trouble, and that's my major concern.

So the minimum preparation steps that I suggest people take: I suggest people stockpile up between 2 and 4 weeks' of food. Not a year's worth of freeze-dried raisins, but 2 to 4 weeks of food.

I don't think there's need for razor wire around your house either. Please make sure you have a means of opening the cans. Don't wait till December to do this. Gradually stockpile the food over the course of the year so you do not put a major drain on the distribution channels we talked about. Make sure you have a way of safely cooking that food over a period of time that you need to.

Have a full tank of gas going into December 31st. Keep all of your financial records for the last 6 months of 1999, and specifically for December, because if there are problems with the financial industry, which I do not expect—I agree that industry is probably as prepared as anybody—but if there are, if you have paper backup, it is a good idea.

Leave your money in the bank. It is FDIC-insured and way safer there than in your mattress or buried in the backyard. I would suggest you also verify the readiness of your mutual funds and also how they're assessing the securities in which they have specifically invested. Hold them responsible for doing the management activities that you are paying them to do with your fees.

Have a little extra money on hand. I encourage you not to have it in cash, because the less-than-honorable people in our society would love that. But I suggest having them in the form of travelers checks. If you are traveling internationally, I encourage you to check with the country specifically. The State Department is going to make an announcement later this year, I believe it is in September, about what countries they feel are the most ready, and I think if you are planning to go to a country that the State Department has got concerns about, I would be concerned about it. Also Y2K travel insurance should be considered.

Medication: If you have medication that you are required to take, talk to your doctor and pharmacist to find out if indeed if there is a problem, how are you going to get that critical medication? And, finally, prepare yourself by reading more about the problem through books like mine or other books that are on the market.

I suggest people treat Y2K like an extended storm. They prepare just like they're expecting a 2-week ice storm or hurricane to hit, without the massive damage of a hurricane. And just make the proper preparation for their own local household.

We can and will recover from Y2K as a technology problem, but recovering from the damage caused by a Y2K panicked public will

have farther reaching, longer term consequences that are best avoided by education and moderate preparation.

I thank you for the invitation to present, and I'll answer any questions.

Mrs. BIGGERT. Thank you very much.

[The prepared statement of Mr. Paulson follows:]

Congressional Testimony

Prepared By: Ed Paulson

Presentation date: July 8, 1999

Naperville, IL

Who is Ed Paulson?

Author of 12 business and technology books.

Author of recent consumer-oriented Y2K book from Macmillan.

Native Chicagoan and local Lisle, IL resident.

Registered Texas Professional Engineer.

President, Technology and Communications, Inc.

Overall Y2K Readiness Progress

Good news: Overall Y2K readiness improves every day.

Good news: The embedded controller issue appears less extensive than initially feared, although still presents a potential problem.

Good news: More accurate Y2K-readiness information becomes available every day.

Good news: The U.S. is the most globally ready, thanks to committees such as this one, the Senate Special Committee on the Year 2000 Technology Problem (Senators Bennett and Dodd) and the President's Council on Year 2000 Conversion (John Koskinen).

Concern: My major domestic concern is the potential for public panic due to lack of preparation for any number of possible Y2K-induced problems. (More on this later.)

Congressional Testimony of Ed Paulson * July 8, 1999

Concern: The uncertain and risky level of international Y2K readiness is an area of primary concern that can affect us on both an economic and humanitarian level. (Siberian Winter without heat, water or food)

General Home Readiness

1. Survey your home for susceptible devices.
2. Everything with date, day and year tracking is suspect.
 - VCR (possibly), computer, cameras, watches.
 - Even if year not shown, the year is needed to calculate the date such as with leap years.
3. Devices with 24-hour timers, or event-driven, are generally immune.
 - Car, stove, refrigerator, microwave, TV, radio, dishwasher, toaster, etc. should generally be O.K. IF THE ELECTRICITY STAYS ON.

The Case for Preparation

1. The end of the world is not coming in 2000 but Y2K is!
2. Preparing for sporadic outages in utilities, phone and other basic services makes common sense due to the complexity of the problem.
3. If Y2K does cause extensive trouble, civil and protective services will have their hands full keeping order in what might become Y2K-induced chaos.

Ed Paulson's Y2K Preparation-Panic Matrix		
	No Y2K Problems	Huge Y2K Problems
Public Prepared	<i>Enjoy New Year and eat the stockpile.</i>	<i>Able to cope and help less prepared neighbors.</i>
Public Not Prepared	<i>Lucky.</i>	<i>Panic and Trouble!</i>

The Bottom Line:

Reasonable Y2K preparation is a no-lose readiness tactic.

Minimum Preparation Steps

1. Gradually accumulate up to four weeks of food and water.
 - Verify expiration dates extend into March 2000.
 - Have means of opening cans, etc.
 - Don't wait until December or it might be too late.
 - Make sure that you have a way to cook without natural gas or electricity - camping cook stove and safely stored gasoline or propane tanks. Proper ventilation.
2. Make alternate plans for heating an area in your home, just in case. Your basement might be the best option. Be careful when placing space heaters or storing fuel.
3. Have a full tank of gas on December 31, 1999.
4. Keep paper records of all financial transactions for the last six months of 1999 in general, and December in particular.

Congressional Testimony of Ed Paulson * July 8, 1999

5. Leave your money in the bank. It is FDIC insured and far safer in the bank than under your mattress or buried in the back yard.
6. Verify Y2K-readiness of mutual funds themselves and their Y2K-readiness of assessment procedures for their underlying securities holdings.
7. Have some extra money on hand, mostly in the form of traveler's checks and a little cash.
8. If traveling, verify Y2K-readiness of destination country/state. (State Department) Y2K travel insurance?
9. Make sure that critical medication is on hand to cover you until mid-January (minimum) and Feb 1st preferred.
10. For more extensive information, a preparation checklist and additional resources refer to my book: "**Sams Teach Yourself Year 2000 Crisis Survival In 10 Minutes**" (Paulson, Ed; ISBN: 0672316358) (Barnes and Noble, Amazon, Borders, Walden, B.Dalton, Crown, etc.) or my Web site: www.edpaulson.com.

Closing Remarks

The general public should prepare for Y2K just like it would prepare for a pending ice storm that is expected to last for between 2-4 weeks.

Some people contend that treating Y2K like an ice storm is inaccurate in that an ice storm causes local problems and Y2K's impact will be international. There is some validity to this point of view.

But the end consumer's level of preparation is the same whether Y2K is a local or international incident. You cannot control the power grid, but you can control what you do if the electrical power goes out.

Please take the time to educate yourself, to make the proper preparations for your household and contingency plan as applicable to your own personal life. Nobody knows for sure whether Y2K will be a non-crisis or a major problem.

We can and will recover from Y2K as a technology problem. Recovering from the damage caused by a Y2K-panicked public will have far-reaching, longer term consequences that are best avoided by education and moderate preparation.

Thank you for your invitation to present to this committee. I will answer any questions.

Mrs. BIGGERT. I appreciate all of your testimony.

First question. Mr. Johnson, since we already have enough batteries with enough capacity to move our cars, trucks, planes, and trains—although I have seen a new car they're developing, or new truck, so that might be on its way but it won't be ready by January 1st, I guess—we really need our oil and gas products. And the oil and gas industries have relied on—the United States has a great dependency on foreign countries to augment our own supply. And in the last 3 months, our country has seen prices go from recent all-time low to high—higher than expected. So don't you have concerns that the foreign countries will not be ready for the year 2000, and what alternatives have you for the shipping industry and how about the prices? Do you expect those to go up because of this problem?

Mr. JOHNSON. First of all, price is very much a function of worldwide supply and demand, and demand for petroleum products anywhere in the world is going to have an impact on what we pay at the pump here in this country.

As far as our supplies coming from foreign suppliers, the three major sources of the foreign crude that comes into this country are Venezuela, Saudi Arabia, and Mexico, and all three of those entities have representatives on our API Y2K task force.

So we do have very current firsthand information about their readiness. We have high confidence that those three suppliers are at the same level of readiness as the domestic companies. So, as far as there being a disruption in those supplies, we didn't believe that is very likely.

Now, what the prices will do later in the year, it is anybody's guess. I mean, once again there are economic political factors around the world that are going to affect supply and demand, and I don't have a crystal ball to predict where that may be by the end of the year.

Mrs. BIGGERT. Thank you. Mr. Paulson, you talked about the problem internationally with some of the foreign countries, too; and I think that we have had some real concerns, particularly about Russia and being ready. I know that there was a recent meeting of the United Nations discussing this problem, and 173 countries attended that meeting and there were very mixed reactions as to who was really compliant or whether they've really begun or not.

It is my understanding that Yeltsin has just sent out a letter to his cabinet, or his government, suggesting that they start to look at the Y2K problem. This gives me great cause for concern that if a country of that size and with those power plants is beginning to look at Y2K—when really you are starting in 1996 which still was the average time—was not way ahead, whether these countries will be ready?

Mr. PAULSON. I would share your concern completely, because when you look at the caliber of people who sit on the panels presenting to the committees and you realize the money and talent and resource that we've been putting behind us in the United States for 3 to 5 years in some instances, and these companies are still now just getting ready—for somebody who's planning to do this in 6 months, for a country, to me that just would be a huge cause for concern. I would share your concern on that completely.

Mrs. BIGGERT. Thank you.

And then, Ms. Croft, I thank you for that testimony really to let people know that there are the scam artists that are out there. And this is one forum to do that. But what else is Jim Ryan's office doing to ensure that the public knows about what's happening, what's been happening in the neighborhoods?

Ms. CROFT. We have an outreach department that is staffed by people that do nothing except go out and give consumer education to different organizations and groups, as they request. And we just feel that the most important thing is to educate the public; and if they're educated, then they can be aware of the problems that may possibly exist.

Mrs. BIGGERT. Do you target different areas or is this just what the organization—

Ms. CROFT. We're statewide. We go all over.

Mrs. BIGGERT. Thank you.

Mr. Clark, have you begun to see people starting to put goods aside, or is this something that you wouldn't know about if it is done on a gradual basis?

Mr. CLARK. We wouldn't really have a way of knowing that. We track our sales, naturally, by month to month and we have not seen a large increase in sales. Naturally, we like to see increases, but we have not seen enough of an increase to say that it has anything to do with the Y2K problem at all.

Mrs. BIGGERT. At one of our hearings it was stated that you cannot buy a generator now, that they are all gone. Some people must be feeling concerned and going out and following suggestions. I don't advise buying a generator because I don't think that we'll need it, but I think there are people that are planning to have it.

Mr. CLARK. I feel there's going to be a certain number of people that will be concerned no matter how much information we throw at them. But I think that our industry is going to be prepared. If all else fails, we started with a hand system, we can go back to a hand system, and barring any electrical outages, people should be able to come to our units and get gas and other things that they need.

Mrs. BIGGERT. Thank you.

And, Mr. Harris, kind of the same question about whether you are seeing people starting to put aside goods but also when you stock your stores, and this is done by inventory that I would assume is by computer; so that you really need to ensure that your computers are working in order to be able to get the inventory in.

Mr. HARRIS. Correct. Everything nowadays is done by electronic data transfer. So we've checked with our wholesaler to make sure they were compliant and that our systems are working properly. As to the question of hoarding, I would think that most of the hoarding would be done in staples and in perishables, and so it is far too early at this point in time to tell.

All the information that I have would suggest that the consumer may keep an extra week's supply. Most customers shop twice a month anyway. My customers probably shop a little more often than that, feeling that they get fresher merchandise by shopping two or three times a week. But my feeling is, especially after being here and listening to the testimony today, is that any shortages or

problems with Y2K would be short term. So I would suggest at most 1 week's supply. As I've already stated, in the pipeline we have 120 days supply so I don't see any major concerns.

Mrs. BIGGERT. Thank you. I'll yield to the chairman, Mr. Horn.

Mr. HORN. Thank you very much. We will go through some of the questions that have been handed in by members of the audience to the staff of the subcommittee. And let's just start with what are the preparations that all the panelists are making in their own homes regarding toilet flushing, food, water, heat, and medicine, credit cards, cash, and stock accounts? Anybody want to say what they are doing on this? Let's go down the line. The author, and then on down.

Mr. PAULSON. I've pretty much written what I'm going to do. I think it is prudent. As I said, I don't expect that there's going to be a major disruption for months and/or years on hand, but I think a few weeks is prudent and that's what I'm doing.

I'm basically stockpiling every time I go to a store. I've set aside an area in my basement, a cool area. Every time I go to the store, I buy a couple extra cans and/or non-perishable items that I can just keep on hand as a contingency. And then I make sure that expiration dates are after March 2000 and basically accumulate that.

Also water. Some people are doing a form of bottled water and every time they go, they buy an extra 5-gallon bottle of water and they save up 10 or 15 of these. Worst case, if it doesn't turn out to be a major disaster, you just eat the food in February or March; but if it does turn out to be a problem, I'll feel better to have it on hand.

Mr. HORN. You can have a neighborhood picnic on February 1st or so.

Mr. JOHNSON. I'm not taking any extraordinary measures at my office. I live 2 blocks from my office. It is a holiday weekend. I'll be working. We're going to staff 24 hours for the day before New Year's Day and the day after. If I've got to walk to work, I've done that before. It is a holiday weekend. It is New Year's Day. I hope to watch the Rose Bowl, watch Dick Clark drop that new Waterford ball at Times Square and pretty much have a holiday weekend just like I normally would.

Mr. HORN. Mr. Clark.

Mr. CLARK. To date, I have not done any extra preparations. I'm an optimist and I feel fairly certain that in Quincy, IL we're going to be operating business as usual throughout the city. So I'm not anticipating at this point.

Mr. HORN. Ms. Croft.

Ms. CROFT. Well, my family tells me that I hoard food all the time so I don't think I really need to buy any additional food. I do have bottled water at home. I plan on having a full gas tank in my car. I will have probably a couple of dollars in the house, no more than I would have if it were any other holiday, and I think that's the basis. I don't really take medication, so that lets that out.

Mr. HORN. Mr. Harris.

Mr. HARRIS. I intend to have a week's supply of food at home, and we have bottled water at home, so we usually have a couple extra jugs which is about a 3-week supply, and have a full tank of gas and that will be the extent of my contingency plan.

Mr. HORN. Mr. Swift.

Mr. SWIFT. I've got a colleague who likes to sign his e-mail, "Hope for the best, prepare for the worst." but that is not a way I think that businesses and rational people ought to prepare. You have to temper the impact with the likelihood of it actually happening.

I've already stated, and I believe after listening to some of the people we've heard here today, for 2 years, that any shortages are going to be local and brief. I've already said that I think cash is a non-issue. I'm not going to have any extra. We are a family that drinks bottled water. We will have some of that on hand, and I would like nothing better to see my family eat its way through what's in the pantry.

Mr. HORN. Mr. Skarr.

Mr. SKARR. I really don't intend to do anything except maybe stockpile red wine, because if any of these come true, the red wine will provide me more comfort than anything else will.

Mr. HORN. Question 2 from the audience is: If you receive a phone call from someone conducting a survey about a product, company, or political situation, should you answer the questions over the telephone?

I don't know if any of us are capable on some of it. If they claim they're in a political situation, most of us that run for office do participate sometimes in surveys, and we'd certainly like honest information when we do a random sample of the home.

But, gentlemen, and Ms. Croft, if you have any thoughts let us know. Actually, it was directed to you, Ms. Croft, since you mentioned some of the scams going on.

Ms. CROFT. If it is merely a survey and if they want to answer the questions, I think it is fine. The first time they act like they want to sell something, if they're not interested, I would just simply say I am not interested and hang up immediately.

Mr. HORN. Right. That's a technique I used. Sometimes their automatic dialer comes back to you, and especially people with phones not in the book. You get sort of irked more with the product than anything else when you find a call coming in, especially at dinner time.

Mr. Johnson, a member of the audience says, how would you evaluate international Y2K readiness for delivery to the United States? Do we have any more thoughts on that one?

Mr. JOHNSON. Well, other than what I mentioned about our three biggest sources of imports, our committee has really struggled on how to report what our member companies know about the countries in which they do business. Most of that is because those companies are there at the invitation or at the whim of the local or the State owned oil companies, so they're very reluctant to be critical of those facilities. However, the three countries where we do get our biggest sources of imported crude, we have firsthand information about their level of readiness and a high level of confidence that they will be ready.

Mr. HORN. The additional part of the question then—I guess I can answer that, Mr. Willemsen—is what is the overall percentage of international readiness? It is a very difficult situation to assess.

Some capitalist-countries, democracy in Europe, when I talked to some of their leaders for the last year or so, they've said, "Oh, well, you know, these things work out—and blah, blah, blah." I thought, brother, are you in for a surprise on January 1st. Some of those smaller countries will be, and they have the money to deal with it.

The countries that really have a problem, of course, are the developing nations in Africa, in southern Asia, some in the Middle East and so forth. They have a real problem in this area.

So we've had the Central Intelligence Agency look at a lot of it and it is pretty gloomy if you've got to interact with them.

And of course a lot of our international business, you are talking about interaction in particular countries. We did suggest back in 1997 to the Secretary General of the U.N. that he needed to educate his members; and he appointed a very able Ambassador from Pakistan to do that. And last fall, December actually, we had the first conference of the 120 nations represented in New York on this. And just 2 weeks ago, I think it was 173 nations that came to New York.

So it isn't too late, but they're in the last stretch for most people. And the World Bank is trying to fund some of the developing nations to get this solved.

I don't know. Mr. Willemsen, you know a lot about it. If you want to add anything, feel free.

Mr. WILLEMSSEN. I think you summed it very well, Mr. Chairman.

Mr. HORN. We go to question 4: Can you suggest some Websites for the year 2000? And that's for Mr. Paulson, the author. Mr. Paulson, how about it? What Websites should the average citizen ought to tap into. We read ours 2 hours ago or so.

Mr. PAULSON. There are so many Websites on the Internet related to this. One of the hardest challenges I had in writing this book is finding information I trusted. There's a difference between finding Websites with information and finding Websites with valid information that doesn't have somebody trying to drum home a point. I've got one that I've put on my own Website, which is—I won't try to sell you blankets or sleeping bags or, as I said, raisins or bottled water. It is strictly for people's use to go to the Website. It is www.edpaulson.com, and there's a year 2000 link, and on there they'll find divisions for different areas—finance, government—and that will then take in other links.

So I'm hoping what people will do is use that as a resource to get to the other specialized locations, like the Board of Governors Website for the Federal Reserve. It is a hard one to find unless you know how to find it, but there you can find really credible information about what the finance industry is doing, right directly from the Federal Reserve's own statements. And there are others.

Mr. HORN. That is a great service and I thank you for offering that. The vice chairman has a question for you.

Mrs. BIGGERT. Not really a question. I just wanted to add, in the information that we have out there, we do have some of the Websites for general sites, and then government sites, and it is a sheet I believe that's out on the table.

Also, how to get testing tools and software patch sites so you can check out your software. Again, you always take it with what you

find there, but at least it is a way to start and get into the Internet on this issue.

Mr. PAULSON. There's another site that I found that I've come to discover lately that I really like. It is www.y2ktoday.com. It is been out for a while, but I've been going to it regularly and checking it out. I actually like that site a lot. That's another alternate site I would recommend to people and that will take them to other locations.

Mrs. BIGGERT. That's on this list also, as is yours.

Mr. HORN. I'm glad you mentioned it because I was going to praise you for it. This is the best list I have seen any Member of the House do, and your representative has done it and it is on the table out there. It is Y2K Readiness Guide to U.S. Representative Judy Biggert, 13th District of Illinois.

[NOTE.—See prepared statement of Judy Biggert.]

Mr. HORN. And that's very useful information I think for all of you, and you don't have to scribble notes in the audience or anything else.

I'm going to ask one last question of this panel, which I've asked every panel. Now that you are into this, what have you learned that, if you ever had to go through it again, ought to be No. 1? Let's start with Mr. Skarr up there.

Mr. SKARR. I think particularly for small business, because I'm not sure we're home free yet relative to small business, it is creating greater awareness. And even hearings like this probably should have been done earlier on just to build a sense of national awareness of the importance of this. So just plain old public awareness and business awareness is probably the issue that we needed to start a little bit earlier in my opinion.

Mr. HORN. Mr. Swift.

Mr. SWIFT. Four things come to mind. One, like everybody else, I wish we started earlier because a large portion of this work could have been accomplished as part of routine enhancements or upgrades to hardware and software.

No. 2, I wish that the lines of business in all our major organizations had accepted the reality that this is not just a technology issue but it is one that threatens whole businesses.

Three, directors and officers, I think they needed in some cases to have stepped up to their responsibilities earlier. If you asked the Federal examiners, What is the common characteristic of banks that have not performed satisfactorily? They will tell you it is not a matter that they do not have the money to throw at this or something; it is that their directors and officers have not asserted themselves aggressively in the process and have the project leaders reporting to them, and on a scheduled timetable. And then, finally—

Mr. HORN. I completely agree with you on that. I've preached that now for 3 or 4 years, and I think they got very bad advice from some of their general counsels, which sort of was, Hey, chief, if you don't say anything, they can't do anything to you in court.

Well, that's just utter baloney. You should have done what—both the government organizations and private sector and nonprofits—they should have said, "Hey, we're going to do everything we can now and if some idiot wants to sue us," which a few are out there

waiting now that they don't have all that tobacco money and the tort bar, "that we should do the best we can," and when you do the best you can, nobody is going to be able to touch you very much. And I think you are right on the target there.

Mr. SWIFT. You just stated my fourth point which is communications. I think you are going to find this summer and through the fall, banks will be much more ready to state the readiness of their organizations.

Mr. HORN. Ms. Croft.

Ms. CROFT. I think that communication and consumer education and hearings such as this to make the public aware of what is available to them and what they should be cautious of. I think those are the most important issues. From the beginning of Jim Ryan's term, he has been very instrumental in making the public aware of the problems that possibly exist and giving them a forum in which to call for information if they're in doubt.

Mr. HORN. Mr. Clark, any thoughts of what we should do first, next time around?

Mr. CLARK. I would have to echo the thoughts of others, is that we probably would have been better off starting a little earlier. But all in all, it helped us get a better handle on our inventory of equipment and so forth, but just timeliness would have, had we started earlier, would have been better.

Mr. HORN. Mr. Johnson.

Mr. JOHNSON. I think once you mentioned about breaking down the barriers of sharing information. I think the Y2K Readiness Act that was enacted last fall got a lot of the attorneys off of our backs and allowed us to speak more freely about what our readiness plans were. It has done a tremendous amount in our industry to help us share information among ourselves, and I think the lingering benefit of this exercise is that we have broken down barriers, and I think the technology and the advancements we've made are going to extend way beyond what we're gaining just as a Y2K issue.

Mr. HORN. Thank you. I agree with you completely on getting everybody off everybody else's neck and it's really been encouraging to see very bitter rival firms working together and sharing information because they've got a common interest.

Mr. JOHNSON. And we're interdependent.

Mr. HORN. Yes, exactly.

Now we have Mr. Paulson. Any more thoughts on that?

Mr. PAULSON. The only comment I would have is from my perspective is I wish I had gone public, proactively public earlier with this, trying to raise the awareness with some of the other people who were the early evangelists on public awareness on this topic.

I think the other thing I would have probably promoted is to have business start to treat this as a new beginning, not an end. I think a lot of the business has been reactive to this, like they're being attacked. And the context of how they did the work was, I think, initially almost antagonistic. Where now what I'm starting to see, that as my colleagues in the information technology industry are going through this, they're saying, "You know what, we've really cleaned up a lot of our systems." And a lot of them are treat-

ing this like we're really going into 2000 on a brand-new, stable, solid technology footing. It is kind of like cleaning house.

Some of the technology in this industry are now treating it that way, and instead of treating it like a bad thing, they're treating it like a good thing. I wish I had seen that earlier, to be able to push this.

Mr. HORN. When we question government agencies, we say, "Now, did you learn something in the process of getting rid of some of the systems or buying them, rather than having to do the expense and—when that isn't going to take you too far with the next generation?" You should be wanting the new generation.

The Federal Government is very far behind the private industry in a lot of things, computing power that they have, and they don't have this. They had to bring people out of retirement to do COBOL. Well, most people thought COBOL hasn't been used for 30 years, but it has been and it is. And those people in COBOL who didn't retire from the Office of Personnel Management said, Hey, you can keep your pension check every month. God bless you on the \$100,000 contract you are getting. People wonder where did this come from. I think those are all useful thoughts. I will try to use these when I'm trying to justify the Office of Management, because the Office of Management and Budget simply doesn't give a hoot about management problems, they're so overwhelmed with the budget problems.

So hopefully we will get something done on that front. I thank you for all your one-liners.

I want to thank you, Judy, for the great hospitality your staff has offered us and for your being here. You do an excellent job in Washington. I'm glad to see your constituents are here to see what you are doing. You sent one fine lady to Washington, DC, and I will tell you and her predecessor, who is also a great Member, we appreciated that.

I do want to thank the staff, both your district office that has helped us on these arrangements, Kristin Wolgemuth, the legislative director; Chris Close, legislative aide; John Hoffman, your district director; Yadira Rosas, staff assistant; and intern, Peter Rayor. And then your chief of staff, Kathy Lydon, and Caroline Stillman, an intern.

And then for us—put your hand up—Russell George. You are in the audience. He's the staff director of the Subcommittee on Government Management, Information, and Technology—a little shy, you can see, sitting in the audience—and chief counsel. Matthew Ryan who is to the chair's left and your right, senior policy director. He brings a great deal of experience to this situation. And then we have Patricia Jones. Where is she here—oh, she's on her way to the airport—American Political Science Association congressional fellow. Grant Newman, our clerk. There he is, back in the audience. And Laura Lufton, intern; John Philips, intern; Justin Schlueter, intern; and during the summer we have a lot of free labor. That's why we have so many interns.

And our court reporter today is Laurie Harris. Thank you, Laurie. It is great to get the transcripts from you. They're very helpful.

And I want to thank the Chair, and if she has any closing statements she'd like to make, please make them.

Mrs. BIGGERT. Thank you very much, Chairman Horn, and thank you so much for coming. I know it is quite a distance from California and we really appreciate it. I think the field hearings, where the members of the public really have an opportunity to hear about what we're doing in Washington, is a reminder this the Government Reform Committee's Subcommittee on Government Management, Information, and Technology and our chairman has led the way in really examining the Y2K bug; and I have to say that I think that that boat is almost sunk, that we really are on our way to solving the problems of Y2K.

And I want not to leave you with anything that would cause anybody to panic. Because I think that's why we're having these hearings, why people are proceeding the way that they are. So, that we will be able to celebrate the year 2000 rather than to have to worry about the glitches because it is—the year 2000 is going to be—the new millennium is going to be a wonderful time. And we want to be able to celebrate it rather than to be out in the forest by a fire.

So this is going to happen, I think. I really thank you for all that you have done over the years, and I'm very privileged to be on this committee and to have the opportunity since January to participate in these discussions. And I think that we've all learned a lot today, at least I have, I hope that everyone has, in what we should do, what responsibility we as citizens should take to be prepared for the year 2000.

I thank you very much and I again thank Mayor Pradel for the opportunity to be here in the great city of Naperville and to hold this hearing here. Thank you very much.

Mr. HORN. I want to give you a little advice from a person who is a bank vice president. I think he's right on the mark. He said: "I would like to remind everyone that the bank records for the end of December, particularly the last 3 days, 2 days, may not be available till January 4 and 5. Data processors and printing will be overloaded to get the statements out so please be patient, for they will be accurate and available." And I think that's good advice.

And with that, we go into recess until we pick up this hearing tomorrow in Detroit. And with that, we're in recess.

[Whereupon, at 12:20 p.m., the subcommittee was recessed.]

**OVERSIGHT OF THE YEAR 2000 TECHNOLOGY
PROBLEM: LESSONS TO BE LEARNED FROM
STATE AND LOCAL EXPERIENCES**

FRIDAY, JULY 9, 1999

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION, AND TECHNOLOGY,
COMMITTEE ON GOVERNMENT REFORM,
Detroit, MI.

The subcommittee met, pursuant to notice, at 9:06 a.m., in the Wayne County Commission Chambers, 600 Randolph Street, Detroit, MI, Hon. Stephen Horn (chairman of the subcommittee) presiding.

Present: Representatives Horn and Knollenberg.

Staff present: J. Russell George, staff director and chief counsel; Matthew Ryan, senior policy director; and Grant Newman, clerk.

Mr. HORN. In the interest of the time of the witnesses and also we have a few people that will be coming in, I believe Mr. Conyers, your Representative from this area, will be possibly here; Mr. Knollenberg, who is in the suburbs, he is driving in now, but I do not want to hold everybody up.

So let me thank first Commissioner George Cushingberry for helping us to arrange this beautiful historic building here and this particular Commission room. I studied General Wayne over the years when I was writing a book on President Washington's first administration and the Congress' first, so he was a great figure in American history and it is a great name. So thank you, Mr. Cushingberry, we appreciate the help.

Let me just outline some of this—I am Stephen Horn, a Member of Congress from Long Beach, CA and chairman of the House Government Reform Committee's Subcommittee on Government Management, Information, and Technology. This is an investigating committee, so we have a practice here of swearing in all the witnesses that testify before us.

Our main concern is of course the year 2000 computer problem, which affects about every aspect of Federal, State and local operations. Further, it affects private sector organizations and could impact the lives of many individuals in our Nation. From Social Security to utilities to local emergency management, the year 2000 computer bug has certainly been a large management and technological challenge for all of us. No single organization, city, State or even country can solve the year 2000 problem alone.

The problem, of course, dates back to the mid-1960's when I think most of you, if you are around my age—and most of you are not, but those that are, you will remember a whole room this size would be filled with mainframe computers. They had very little memory capacity and I guess maybe nationally programmers all over said, “Gee, why are we putting in 19 when we are putting in 1967, let us just put 67?” and we gained a lot of memory in that. And of course that whole room could be reflected now in your personal computer in terms of memory. But they knew when they hit the year 2000, that the 00 would be a problem and the computer would think it is 1900, not necessarily 2000. And so they said oh well, do not worry about it, American technology, we will always solve that problem. The fact is, there is no silver bullet, they did not solve the problem. I do not know how many people have even tried, but it is a long, laborious situation where they go through the codes and they are bringing COBOL people out of retirement, in the case of the Federal Government, which is good for those who had to study COBOL. I only did a program in it once, so it is way in my past.

The problem that we face is really a management problem, it is not a techie problem. And the ones that have succeeded in this have been individuals that have organized properly and gone through this what I called earlier a laborious matter.

More than 3 years ago, in April and June 1996, this subcommittee held the first congressional hearing on the year 2000 problem. Since that time, we have held almost 30 hearings, issued eight report cards to monitor the status of the Federal Government's year 2000 computer solutions. Current estimates show the Federal Government will spend by the end of this fiscal year on September 30, about \$9 billion to fix its computer systems. I have often said the figure will probably reach \$10 billion, and we have a few months to go after September 30th.

Recently, the President's Office of Management and Budget identified 43 essential Federal programs, such as Social Security, Medicare and the Nation's air traffic control system. Each day these programs provide critical services to millions of Americans. Of these 43 programs, 10 are federally funded, State-run programs, including Medicaid, food stamps, unemployment insurance, child support enforcement. Several of these State-run programs are not scheduled to be ready for the year 2000 until December, leaving little, if any, time to fix unforeseen problems.

Data exchanges and interdependencies exist at all levels of government and throughout the private sector. A single failure in the chain of information could have severe repercussions.

For example, let me briefly illustrate how the U.S. Social Security program uses computers. And Social Security has always received an “A” on our report cards. They faced up to this way back in 1989. The Department of Transportation could have if they had listened to the woman programmer that had laid it all out for them, but they knew better. So they are getting “F's” and “D's” usually in the last eight report cards. And of course, in that agency is the FAA, the Federal Aviation Administration. But Social Security is a prime example of how to get the job done well. When the payments are made, however, Social Security sends the payment

data to the Department of the Treasury's Financial Management Service. The Service then cuts the Federal check for about \$43 million in one program and \$50 million in the other, which is then electronically deposited directly into the person's bank account at a local financial institution. These organizations move and manipulate data to make these payments; each uses its own network of computers. If a payment is mailed to an individual's home, the U.S. Postal Service then plays a key role.

And many of the agencies in the Federal Government have said to us when we have asked where is your contingency plan, they said, "Oh, we will use the post office." In other words, mail the check, do not electronically deposit it. The humorous thing about that is when we held a joint hearing with the Postal Service Subcommittee of our full committee, the post office did not have a contingency plan. So we will see what happens.

The bottom line is if any one of these entities fails from the Federal Government to the local bank or Postal Service, a deserving individual will not receive a payment. Now multiply this situation by millions of people that receive the Social Security benefits and also remembering there are 435 Members of Congress, there are 5 from the territories and commonwealths and there are 100 U.S. Senators. And you can believe it, if grandma does not get her check, there will be a long line out of our district offices. So we are trying to avoid that situation.

But for the computers to work, we need, of course, power. One of the most essential questions concerning the year 2000 challenge is will the lights stay on? Without electricity, our modern society will be relegated back to the proverbial stone age.

I see our colleague from the suburbs of Detroit has made it through the rain, Mr. Knollenberg.

Mr. KNOLLENBERG. Good morning, how are you?

Mr. HORN. Joe, it is great seeing you. Joe is one of the most powerful guys in my class, being on the Appropriations Committee. So he can do a lot of good for the State of Michigan and the country, and he does. So we are glad to have you with us. Come on up here, Joe, you can sit here.

Mr. KNOLLENBERG. I can sit in the big chair.

Mr. HORN. No, I got rid of the big chair, but you can sit in a chair that you do not have to go backward on or something.

We are reminded of the Speaker's chair in the House, sort of as a catapult into the wall.

One of the most essential questions on the year 2000 challenge is will the lights stay on? Without electricity, our modern society would be relegated back to the proverbial stone age. I wonder how automobile plants would continue to manufacture cars without power, even if only for a short time.

From a personal standpoint, I realize that when confronted with a personal emergency, I can call 911 for assistance and feel confident the phone will be answered promptly, that a competent authority will respond rapidly. Year 2000 computer problems present other potentially serious threats at local levels—and we will cover some of those today—from the potential interruption of a citizen's call for fire or police to the delays in the State's ability to request emergency or disaster assistance from the Federal Government.

One thing is for sure, there are only 175 days left until January 1, 2000. The clock is ticking, you cannot change the date. Accordingly, the testimony we receive today will be very helpful into our understanding of the full extent of the year 2000 problem.

I would ask my colleague, Mr. Knollenberg, do you want to make any opening statement here?

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

DAN BURTON, INDIANA
CHAIRMAN
BRADYMYN A. GILMAN, NEW YORK
CONSTANCE A. MCGILLIA, MARYLAND
CHRISTOPHER SHUTE, CONNECTICUT
ILANA ROSENTHAL, FLORIDA
JOHN M. MAHONEY, NEW YORK
STEPHEN HORN, CALIFORNIA
JIMMIE MCCA, FLORIDA
DONALD W. DAVIS, VIRGINIA
DAVID AL. KUNTZOSH, INDIANA
DANK E. BRUNSER, INDIANA
JOE SCARBROUGH, FLORIDA
STEVEN C. LAFORLETTE, OHIO
MARSHALL "MARK" SANFORD, SOUTH CAROLINA
BOB BARR, GEORGIA
DAN MILLER, FLORIDA
JOHN HUTTENBACH, ARKANSAS
LEE TERRY, NEBRASKA
JUDY BISCETTE, ILLINOIS
GREG WALDEN, OREGON
OSCAR COSE, CALIFORNIA
PAUL RYAN, WISCONSIN
JOHN T. DODDLETT, CALIFORNIA
HELEN CHENOWETH, IOWA

ONE HUNDRED SIXTH CONGRESS
Congress of the United States
House of Representatives
COMMITTEE ON GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-6143

MAURPHY (202) 225-5074
HANNON (202) 225-5081
TYT (202) 225-6682

HENRY A. WYDMAN, CALIFORNIA
RANKING MEMBER
TOM LANTOS, CALIFORNIA
ROBERT E. WISE, JR., WEST VIRGINIA
MAJID R. DINEI, NEW YORK
EUGENIE TUNNEY, NEW YORK
PAUL E. GANDY, PENNSYLVANIA
GARY A. COOPER, CALIFORNIA
PATRY T. MIBK, HAWAII
CHRISTINE R. MALONEY, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
DIANA FATTAL, PENNSYLVANIA
SUZANNE CUMMINGS, MARYLAND
DENNIS A. ROZUMICH, OHIO
ROD R. BLADEN, NORTH CAROLINA
DANNY K. DAVIS, ILLINOIS
JOHN F. TERRY, MASSACHUSETTS
JIM TURNER, TEXAS
THOMAS H. ALLEN, MARYLAND
HAROLD E. FORD, JR., TENNESSEE

BERNARD SANDERS, VERMONT,
INDEPENDENT

"Oversight of the Year 2000 Problem: Lessons to Be Learned from State and Local Experiences"
Opening Statement of Chairman Stephen Horn (R-CA)
Subcommittee on Government Management, Information, and Technology
July 9, 1999
Detroit, Michigan

This hearing of the House Subcommittee on Government Management, Information, and Technology, will come to order. I am very pleased to be here today in the "Motor City."

The Year 2000 computer problem affects just about every aspect of Federal, State, and local government operations. Furthermore, it affects private sector organizations and could impact the lives of most individuals. From social security to utilities to local emergency management, the Year 2000 computer bug has certainly been a large management and technological challenge for all of us. No single organization, city, State or even country can solve the Year 2000 problem alone.

The problem, of course, dates back to the mid-1960s when programmers, seeking to conserve limited computer storage capacity, began designating the year in two digits rather than four. The year 1967, for example, simply appeared as '67.' Regardless, now we all must deal with it.

More than three years ago, our subcommittee held the first Congressional hearing on the Year 2000 problem. Since that time, we have held almost 30 hearings and issued 8 "report cards" to monitor the status of the Federal Government's Year 2000 computer solutions.

Current estimates show that the Federal Government will spend nearly 9 billion dollars to fix its computer systems. I have often said that figure will easily reach 10 billion dollars.

Recently, the President's Office of Management and Budget identified 43 essential Federal programs such as Social Security, Medicare, and the nation's Air Traffic Control system. Each day, these programs provide critical services to millions of Americans. Of these 43 programs, 10 are Federally funded, State run programs including Medicaid, Food Stamps, Unemployment Insurance, and Child Support Enforcement. Several of these State run programs are not scheduled to be ready for the Year 2000 until December, leaving little, if any, time to fix unforeseen problems.

Data exchanges and interdependencies exist at all levels of government and throughout the private sector. A single failure in the chain of information could have severe repercussions.

For example, let me briefly illustrate how the United States' Social Security program uses computers. The Social Security Administration maintains data containing pertinent Social Security payment information for eligible citizens. When payments are made, the Social Security Administration sends payment data to the Department of the Treasury's Financial Management Service. This Service then "cuts the Federal check," which is then electronically deposited directly into a person's bank account at a local financial institution. Three organizations move and manipulate data to make these payments; each uses its own network of computers. If a payment is mailed to an individual's home, the United States Postal Service then plays a key role.

The bottom line is: If any one of these entities fails, from the Federal Government to the local bank or Postal Service, a deserving individual will not receive the payment. Now multiply this situation by the millions of people that receive Social Security benefits and you can appreciate the magnitude of just one aspect of the Year 2000 issue. Fortunately, the Social Security Administration has been working on this problem for 10 years and is in good shape.

But, for computers to work, we need power. One of the most essential questions concerning the Year 2000 challenge is, "will the lights stay on?" Without electricity, our modern society would be relegated back to the proverbial "Stone Age." I wonder how automobile plants would continue to manufacture cars without power, even if for only a short time.

From a personal standpoint, I realize that when confronted with a personal emergency, I can call "911" for assistance and feel confident that the phone will be answered promptly and that a competent authority will respond rapidly. Year 2000 computer problems present other potentially serious threats at local levels, from the potential interruption of a citizen's call for fire or police assistance to delays in a State's ability to request emergency or disaster assistance from the Federal Government.

One thing is for sure, there are only about 175 days until January 1, 2000, and the clock is ticking. Accordingly, the testimony we receive today will help our understanding of the full extent of the Year 2000 computer problem.

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

Mr. KNOLLENBERG. Mr. Horn, I will be very brief.

Steve is very kind to introduce me as a person of influence because I am on the Appropriations Committee. That means I write the checks and obviously sometimes that is not so easy because I also sit on the Budget Committee and I have to style the budget to get to the point where we can write the checks, but nonetheless everybody likes me because I am the check writer. But I hope you understand that everybody likes to talk to me about whatever is on their mind.

I, very briefly, will just add this. Steve Horn has been a leader on this issue from the very, very beginning. And with his leadership, the Federal agencies are closer to compliance. And I think he has already told you, they are not there either, and you hear stories about, for example, the FAA air traffic control is not yet prepared to deal with the day January 1, 2000.

I think that he may have already talked to you about the point that we have reached here is that the House did pass overwhelmingly the Y2K litigation reform, 404 to 24. I think you might have mentioned also that the Senate did likewise on the very same day, July 1st. So we are moving forward, but as Steve Horn says, the clock is ticking, there is 175 days now and the end, while it is not near, the end of the time that it takes to actually bring about architecting the right kind of program that leaves us frankly on top of things and not behind the eight ball is rapidly approaching.

So I am going to conclude with those remarks. I am just delighted to be here with Steve and look forward to the testimony of the panel and obviously to the point of perhaps asking a question or two.

Thank you.

Mr. HORN. Thank you very much. We appreciate you coming. When Members are home in the District, it is awful nice of them to break away from that and get their wisdom on some of these questions.

Let me just note our procedures here. We have panel one before us and there will be panels two and three. And the way we work is we swear in all witnesses, as I mentioned earlier, and when we introduce you—and we introduce you in the system laid out on the agenda—your full statement is automatically put in the record. We do not want you to read your statement, we have had a chance of those that we do have, to read them, and we would like you to sort of summarize it in 5 minutes. And the reason for that is we can then get into a dialog between members of the panel and between ourselves and the panel. And we get a lot more from that than hearing statements we already have.

So if you could just summarize it in 5 minutes, we will—counsel for us will hold up a 1-minute sort of marker, so that you will know you have 1 minute to wind it up. He is keeping the time.

We also have another routine on these field hearings in the States. We started in Topeka 2 days ago, and were in the Chicago area yesterday and Detroit will end it. And we found it very useful that we pass out cards for those in the audience, and if there is a question you would like us to raise with the panel, we are glad to do that. And we found we have been able to get a tremendous amount of information out of that because a lot of people in the au-

diences often have some real questions from their industry standpoint or the governmental standpoint.

So, if the panel will stand and raise your right hands, we will swear you in.

[Witnesses sworn.]

Mr. HORN. Thank you. The clerk will note that all five witnesses affirmed the oath. And we will begin with a witness that has probably had about 100,000 miles of travel with us over the last couple of years, and that is Joel C. Willemsen, the Director for Civil Agencies Information Systems of the General Accounting Office. The General Accounting Office is part of the legislative branch of government under the Budget and Accounting Act of 1921. It is Congress' right arm, originally for fiscal review, in the traditional accounting office role. But in the post-war period, for programmatic review. And they do an outstanding job on doing that and doing special studies for the Appropriations Committee, the Government Reform Committee, this subcommittee, so forth.

So Mr. Willemsen has one of the most overall bits of knowledge on this problem. So Joel, go ahead.

STATEMENTS OF JOEL C. WILLEMSSEN, DIRECTOR, CIVIL AGENCIES INFORMATION SYSTEMS, GENERAL ACCOUNTING OFFICE; GEORGE BOERSMA, DIRECTOR, MANAGEMENT AND BUDGET, STATE OF MICHIGAN; CAPTAIN ED BUIKEMA, DEPUTY STATE DIRECTOR OF EMERGENCY MANAGEMENT, MICHIGAN STATE POLICE; ARUN GULATI, DEPUTY DIRECTOR, DEPARTMENT OF INFORMATION PROCESSING, WAYNE COUNTY, MI; AND KATHLEEN LEAVEY, DEPUTY DIRECTOR, DETROIT WATER AND SEWERAGE DEPARTMENT

Mr. WILLEMSSEN. Thank you, Mr. Chairman, Congressman, thank you for inviting GAO to testify today. As requested, I will briefly summarize our statement on the Y2K readiness of the Federal Government, State and local governments, and key economic sectors.

Regarding the Federal Government, the most recent reports indicate continued progress in fixing, testing, and implementing mission critical systems. Nevertheless, numerous critical systems must still be made compliant and must undergo independent verification and validation. Our own reviews of selected agencies have shown uneven progress and remaining risks in addressing Y2K, and therefore point to the importance of business continuity and contingency planning.

If we look beyond individual agencies and individual systems, the Federal Government's future actions will need to be increasingly focused on making sure that its high priority programs are compliant. In line with this, OMB has identified 43 high impact programs such as Medicare and Social Security. And as you know, Mr. Chairman, we are currently reviewing for you the executive branch's progress in addressing those programs. However, at this point, it is very clear that much additional work is needed to make all those programs ready for the turn of the century.

Available information on the Y2K readiness of State and local governments indicates that much work remains. For example, according to recent information on States reported to the National

Association of State Information Resources Executives, about 18 States had completed implementing less than 75 percent of their mission critical systems. State audit organizations have also identified significant Y2K concerns in areas such as testing, embedded systems, and contingency planning.

Recent reports have also highlighted Y2K issues at the local government level. For example, a March 1999 National League of Cities poll of over 400 representatives found that almost 70 stated they would finish 75 percent or less of their systems by January 1, 2000.

Another area of risk is represented by Federal human services programs administered by States, programs such as Medicaid and food stamps. Of the 43 high impact priorities that I mentioned earlier 10 of these are State-administered Federal programs. The available OMB reported data on the systems supporting these programs show that numerous States are not planning to be ready until close to the end of the year. Specifically, a large number of State systems are not due to be compliant until the last quarter of 1999. And further, that is based on data that has not been independently verified.

If we look at the risks beyond those facing our governments and the risks that Y2K poses to our infrastructure, key economic sectors and to other countries, we have made a number of recommendations to the chairman of the President's Y2K Conversion Council, John Koskinen, and the Council has made some major strides in addressing these areas. Nevertheless, there is a good deal of variance on the Y2K readiness among these various sectors. Accordingly, there will be a need for continuing emphasis, which will be critical to fully address those areas in the less than 6 months that remains.

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

Thank you.

Mr. HORN. Thank you very much for that. We will move through the various witnesses and then we will open it up to questions.

Mr. George Boersma, the director of management and budget for the State of Michigan is our next witness. Welcome.

[The prepared statement of Mr. Willemsen follows:]

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Government Management,
Information and Technology, Committee on Government
Reform, House of Representatives

For Release on Delivery
Expected at
9 a.m. EDT
Friday,
July 9, 1999

YEAR 2000
COMPUTING
CHALLENGE

Important Progress
Made, Yet Much Work
Remains to Avoid
Disruption of Critical
Services

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



Mr. Chairman and Members of the Subcommittee:

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 a high-risk area for the federal government.² Since that time, we have issued over 120 reports and testimony statements detailing specific findings and numerous 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 challenges that remain in correcting its systems; identify state and local government Year 2000 issues; and provide an overview of available information on the readiness of key public infrastructure and economic sectors.

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

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

³A list of these publications is included as an attachment to this statement. These publications can be obtained through GAO's World Wide Web page at www.gao.gov/y2kr.htm.

⁴Year 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 RISK OF
YEAR 2000 DISRUPTIONS

The public faces the 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
- 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 signed an executive order that established the President's Council on Year 2000 Conversion, chaired 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.

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

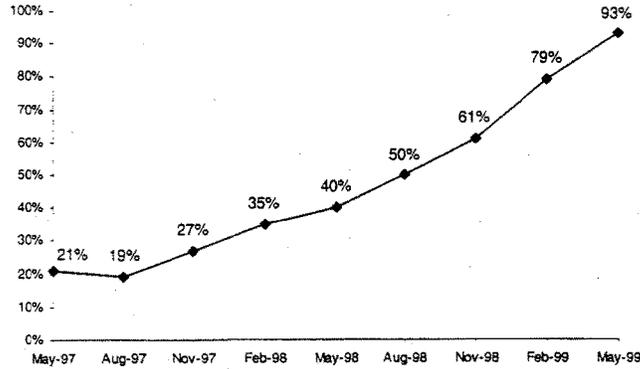
⁶Defense Computers: Year 2000 Computer Problems Threaten DOD Operations (GAO/AIMD-98-72, April 30, 1998).

IMPROVEMENTS MADE BUT
MUCH WORK REMAINS

Addressing the Year 2000 problem is 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 costs and business continuity and contingency plans.

The federal government's most recent reports show improvement in addressing the Year 2000 problem. While much work remains, the federal government has significantly increased its percentage of mission-critical systems that are reported to be Year 2000 compliant, as chart 1 illustrates. In particular, while the federal government did not meet its goal of having all mission-critical systems compliant by March 1999, as of mid-May 1999, 93 percent of these systems were reported compliant.

Chart 1: Mission-Critical Systems Reported Year 2000 Compliant, May 1997-May 1999

Source: May 1997 – May 1999 data are from the OMB quarterly reports.

While this reported progress is notable, OMB reported that 10 agencies have mission-critical systems that were not yet compliant.⁷ In addition, as we testified in April, some of the systems that were not yet compliant support vital government functions.⁸ For example, some of the systems that were not compliant were among the 26 mission-critical systems that the Federal Aviation Administration (FAA) has identified as posing the greatest risk to the National Airspace System—the network of equipment, facilities, and information that supports U.S. aviation operations.

Additionally, not all systems have undergone an independent verification and validation process. For example, in April 1999 the Department of Commerce awarded a contract for independent verification and validation reviews of approximately 40 mission-critical systems that support that Department's most critical business processes. These reviews are to continue through the summer of 1999. In some cases, independent verification and

⁷The 10 agencies were the Departments of Agriculture, Commerce, Defense, Energy, Health and Human Services, Justice, Transportation, Treasury; the National Aeronautics and Space Administration; and the U.S. Agency for International Development.

⁸Year 2000 Computing Challenge: Federal Government Making Progress But Critical Issues Must Still Be Addressed to Minimize Disruptions (GAO/T-AIMD-99-144, April 14, 1999).

validation of compliant systems have found serious problems. For example, as we testified this past February,⁹ none of 54 external mission-critical systems of the Health Care Financing Administration reported by the Department of Health and Human Services (HHS) as compliant as of December 31, 1998, was Year 2000 ready, based on serious qualifications identified by the independent verification and validation contractor.

Reviews Show Uneven Federal Agency Progress

While the overall 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. For example:

- In March we testified that FAA had made tremendous progress over the prior year.¹⁰ However, much remained to be done to complete validating and implementing FAA's mission-critical systems. Specifically, the challenges that FAA faced included (1) ensuring that systems validation efforts were adequate, (2) implementing multiple systems at numerous facilities, (3) completing data exchange efforts, and (4) completing end-to-end testing. Because of the risks associated with FAA's Year 2000 program, we have advocated that the agency develop business continuity and contingency plans.¹¹ FAA agreed and has activities underway, which we are currently reviewing.
- In May we testified¹² that the Department of Education had made progress toward addressing the significant risks we had identified in September 1998¹³ related to systems testing, exchanging data with internal and external partners, and developing business continuity and contingency plans. Nevertheless, work remained ongoing in these areas. For example, Education had scheduled a series of tests with its data exchange partners, such as schools, through the early part of the fall.

⁹Year 2000 Computing Crisis: Readiness Status of the Department of Health and Human Services (GAO/T-AIMD-99-92, February 26, 1999).

¹⁰Year 2000 Computing Crisis: FAA Is Making Progress But Important Challenges Remain (GAO/T-AIMD/RCED-99-118, March 15, 1999).

¹¹FAA Computer Systems: Limited Progress on Year 2000 Issue Increases Risk Dramatically (GAO/AIMD-98-45, January 30, 1998); GAO/T-AIMD-98-251, August 6, 1998; and GAO/T-AIMD/RCED-99-118, March 15, 1999.

¹²Year 2000 Computing Challenge: Education Taking Needed Actions But Work Remains (GAO/T-AIMD-99-180, May 12, 1999).

¹³Year 2000 Computing Crisis: Significant Risks Remain to Department of Education's Student Financial Aid Systems (GAO/T-AIMD-98-302, September 17, 1998).

- Our work has shown that the Department of Defense and the military services face significant problems.¹⁴ In March we testified that, despite considerable progress made in the preceding 3 months, Defense was still well behind schedule.¹⁵ We found that DOD faced two significant challenges: (1) completing remediation and testing of its mission-critical systems and (2) having a reasonable level of assurance that key processes will continue to work on a day-to-day basis and key operational missions necessary for national defense can be successfully accomplished. We concluded that such assurance could only be provided if Defense took steps to improve its visibility over the status of key business processes.

End-To-End Testing Must Be Completed

While it is important to achieve compliance for individual mission-critical systems, realizing such compliance alone does not ensure that business functions will continue to operate through the change of century—the ultimate goal of Year 2000 efforts. The purpose of end-to-end testing is to verify that a defined set of interrelated systems, which collectively support an organizational core business area or function, 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—are 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.)¹⁶

In January we testified that 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 the tests.¹⁷ On March 31, OMB and the Chair of the President's Council on Year 2000 Conversion announced that one of the key priorities that federal agencies will be pursuing during the rest of 1999 will be cooperative end-to-end testing to demonstrate the Year 2000 readiness of federal programs with states and other partners.

¹⁴Defense 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).

¹⁵Year 2000 Computing Crisis: Defense Has Made Progress, But Additional Management Controls Are Needed (GAO/T-AIMD-99-101, March 2, 1999).

¹⁶GAO/AIMD-10.1.21, November 1998.

¹⁷Year 2000 Computing Crisis: Readiness Improving, But Much Work Remains to Avoid Major Disruptions (GAO/T-AIMD-99-50, January 20, 1999).

Agencies have also acted to address end-to-end testing. For example, our March FAA testimony¹⁸ found that the agency had addressed our prior concerns about the lack of detail in its draft end-to-end test program plan and had developed a detailed end-to-end testing strategy and plans.¹⁹ At the Department of Defense, last month we reported²⁰ that the department had underway or planned hundreds of related Year 2000 end-to-end test and evaluation activities and that, thus far, it was taking steps to ensure that these related end-to-end tests were effectively coordinated. However, we concluded that Defense was far from successfully finishing its various Year 2000 end-to-end test activities and that it must complete efforts to establish end-to-end management controls, such as establishing an independent quality assurance program.

Business Continuity and Contingency Plans Are Needed

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, in April 1998 we recommended that the Council require agencies to develop contingency plans for all critical core business processes.²¹

OMB has clarified its contingency plan instructions and, along with the Chief Information Officers Council, has adopted our business continuity and contingency planning guide.²² In particular, on January 26, 1999, OMB called on federal agencies to identify and report on the high-level core business functions that are to be addressed in their business continuity and contingency plans, as well as to provide key milestones for development and testing of such plans in their February 1999 quarterly reports. In addition, on May 13 OMB required agencies to submit high-level versions of these plans by June 15. According to an OMB official, OMB has received almost all of the agency plans. This official stated that OMB planned to review the plans, discuss them with the agencies, determine whether there were any common themes, and report on the plans' status in its next quarterly report.

To provide assurance that agencies' business continuity and contingency plans will work

¹⁸GAO/T-AIMD/RCED-99-118, March 15, 1999.

¹⁹GAO/T-AIMD-98-251, August 6, 1998.

²⁰Defense Computers: Management Controls Are Critical To Effective Year 2000 Testing (GAO/AIMD-99-172, June 30, 1999).

²¹Year 2000 Computing Crisis: Potential for Widespread Disruption Calls for Strong Leadership and Partnerships (GAO/AIMD-98-85, April 30, 1998).

²²GAO/AIMD-10.1.19, August 1998.

if needed, on January 20 we suggested that 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.²³ Our review of the 24 major departments and agencies' May 1999 quarterly reports found 14 cases in which agencies did not identify test dates for their business continuity and contingency plans or reported test dates subsequent to September 30, 1999.

On March 31, OMB and the Chair of the President's Council announced that completing and testing business continuity and contingency plans as insurance against disruptions to federal service delivery and operations from Year 2000-related failures will be one of the key priorities that federal agencies will be pursuing through the rest of 1999. Accordingly, OMB should implement our suggestion and establish a target date for the validation of these business continuity and contingency plans.

Recent OMB Action Could Help Ensure
Business Continuity of High-Impact Programs

While individual agencies have been identifying and remediating mission-critical systems, the government's future actions need to be focused on its high-priority programs and ensuring the continuity of these programs, including the continuity of federal programs that are administered by states. Accordingly, governmentwide priorities need to be based on such criteria as the potential for adverse health and safety effects, adverse financial effects on American citizens, detrimental effects on national security, and adverse economic consequences. In April 1998 we recommended that the President's Council on Year 2000 Conversion establish governmentwide priorities and ensure that agencies set agencywide priorities.²⁴

On March 26, OMB implemented our recommendation by issuing a memorandum to federal agencies designating lead agencies for the government's 42 high-impact programs (e.g., food stamps, Medicare, and federal electric power generation and delivery). (OMB later added a 43rd high-impact program.) Appendix I lists these programs and their lead agencies. For each program, the lead agency was charged with identifying to OMB the partners integral to program delivery; taking a leadership role in convening those partners; assuring that each partner has an adequate Year 2000 plan and, if not, helping each partner without one; and developing a plan to ensure that the program will operate effectively. According to OMB, such a plan might include testing data exchanges across partners, developing complementary business continuity and contingency plans, sharing key information on readiness with other partners and the public, and taking other steps necessary to ensure that the program will work. OMB directed the lead agencies to provide a schedule and milestones of key activities in the plan by April 15. OMB also asked agencies to provide monthly progress reports. As you know, we are currently reviewing agencies' progress in ensuring the readiness of their high-impact programs for this subcommittee.

²³GAO/T-AIMD-99-50, January 20, 1999.

²⁴GAO/AIMD-98-85, April 30, 1998.

STATE AND LOCAL GOVERNMENTS
FACE SIGNIFICANT YEAR 2000 RISKS

Just as the federal government faces significant Year 2000 risks, so too do state and local governments. If the Year 2000 problem is not properly addressed, for example, (1) food stamps and other types of payments may not be made or could be made for incorrect amounts; (2) date-dependent signal timing patterns could be incorrectly implemented at highway intersections, with safety severely compromised; and (3) prisoner release or parole eligibility determinations may be adversely affected. Nevertheless, available information on the Year 2000 readiness of state and local governments indicates that much work remains.

According to information on state Year 2000 activities reported to the National Association of State Information Resource Executives as of June 17, 1999,²⁵ states²⁶ reported having thousands of mission-critical systems.²⁷ With respect to completing the implementation phase for these systems,

- 5 states²⁸ reported that they had completed between 25 and 49 percent,
- 13 states²⁹ reported completing between 50 and 74 percent, and
- 30 states³⁰ reported completing 75 percent or more.³¹

All of the states responding to the National Association of State Information Resource Executives survey reported that they were actively engaged in internal and external contingency planning and that they had established target dates for the completion of these plans; 14 (28 percent) reported the deadline as October 1999 or later.

²⁵Individual states submit periodic updates to the National Association of State Information Resource Executives. For the June 17 report, over half of the states submitted their data in May and June 1999. The oldest data were provided on March 4 and the most recent data on June 16. All but three states responded to the survey.

²⁶In the context of the National Association of State Information Resource Executives survey, the term "states" includes the District of Columbia, Guam, and Puerto Rico.

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

²⁸Three states reported on their mission-critical systems, one state reported on its processes, and one reported on its functions.

²⁹Eleven states reported on their mission-critical systems, one reported on all systems, and one reported on projects.

³⁰Twenty-five states reported on their mission-critical systems, two states reported on their applications, one reported on its "priority business activities," one reported on its "critical compliance units," and one reported on all systems.

³¹Of the states that responded to the survey, two did not respond to this question.

State audit organizations have also identified significant Year 2000 concerns. In January, the National State Auditors Association reported on the results of its mid-1998 survey of Year 2000 compliance among states.³² This report stated that, for the 12 state audit organizations that provided Year 2000-related reports, concerns had been raised in areas such as planning, testing, embedded systems, business continuity and contingency planning, and the adequacy of resources to address the problem.

We identified additional products by 15 state-level audit organizations and Guam that discussed the Year 2000 problem and that had been issued since October 1, 1998. Several of these state-level audit organizations noted that progress had been made. However, the audit organizations also expressed concerns that were consistent with those reported by the National State Auditors Association. For example:

- In December 1998 the Vermont State Auditor reported³³ that the state Chief Information Officer did not have a comprehensive control list of the state's information technology systems. Accordingly, the audit office stated that, even if all mission-critical state systems were checked, these systems could be endangered by information technology components that had not been checked or by linkages with the state's external electronic partners.
- In April, New York's Division of Management Audit and State Financial Services reported that state agencies did not adequately control the critical process of testing remediated systems.³⁴ Further, most agencies were in the early stages of addressing potential problems related to data exchanges and embedded systems and none had completed substantive work on contingency planning. The New York audit office subsequently issued 7 reports on 13 of the state's mission-critical and high-priority systems that included concerns about contingency planning and testing.
- In February, the California State Auditor reported³⁵ that key agencies responsible for emergency services, corrections, and water resources, among other areas, had not fully addressed embedded technology-related threats. Regarding emergency services, the California report stated that if remediation of the embedded technology in its networks were not completed, the Office of Emergency Services might have to rely on cumbersome manual processes, significantly increasing response time to disasters.

³²Year 2000: State Compliance Efforts (National State Auditors Association, January 1999).

³³Vermont State Auditor's Report on State Government's Year 2000 Preparedness (Y2K Compliance) for the Period Ending November 1, 1998 (Office of the State Auditor, December 31, 1998).

³⁴New York's Preparation for the Year 2000: A Second Look (Office of the State Comptroller, Division of Management Audit and State Financial Services, Report 98-S-21, April 5, 1999).

³⁵Year 2000 Computer Problem: The State's Agencies Are Progressing Toward Compliance but Key Steps Remain Incomplete (California State Auditor, February 18, 1999).

- In March, Oregon's Audits Division reported³⁶ that 11 of the 12 state agencies reviewed did not have business continuity plans addressing potential Year 2000 problems for their core business functions.
- In March, North Carolina's State Auditor reported³⁷ that resource restrictions had limited the state's Year 2000 Project Office's ability to verify data reported by state agencies.

In the case of Michigan, in May 1999, the Office of the Auditor General reported that the state's Year 2000 Project Office had effectively implemented key processes to achieve Year 2000 compliance.³⁸ However, the report stated that because of the unprecedented nature of the Year 2000 issue, sufficient audit evidence did not exist to conclude that the state will be successful in its remediation efforts or that essential business functions will not be affected by either internal or external factors. The audit office also found that state agencies had not reported their assessments of, for example, the status of regulated industries' Year 2000 remediation efforts to the Emergency Management Division. The audit office concluded that without this information, the Emergency Management Division would find it more difficult to assess the vulnerabilities of the state's health and safety infrastructure.

It is also critical that local government systems be ready for the change of century since critical functions involving, for example, public safety and traffic management, are performed at the local level. Recent reports on local governments have highlighted Year 2000 concerns. For example:

- On June 23, the National Association of Counties announced the results of its April survey of 500 randomly selected counties. This survey found that (1) 74 percent of respondents had a countywide plan to address Year 2000 issues, (2) 51 percent had completed system assessments, and (3) 27 percent had completed system testing. In addition, 190 counties had prepared contingency plans and 289 had not. Further, of the 114 counties reporting that they planned to develop Year 2000 contingency plans, 22 planned to develop the plan in April-June, 64 in July-September, 18 in October-December, and 10 did not yet know.
- The National League of Cities conducted a poll during its annual conference in March 1999 that included over 400 responses. The poll found that (1) 340 respondents

³⁶Department of Administrative Services Year 2000 Statewide Project Office Review (Secretary of State, Audits Division, State of Oregon Report No. 99-05, March 16, 1999).

³⁷Department of Commerce, Information Technology Services Year 2000 Project Office (Office of the State Auditor, State of North Carolina, March 18, 1999).

³⁸Performance Audit of the Year 2000 Issues For Information Systems, Year 2000 Project Office, Department of Management and Budget (Office of the Auditor General, State of Michigan, May 1999).

stated that over 75 percent of their cities' critical systems would be Year 2000 compliant by January 1, 2000. (2) 35 stated that 51-75 percent would be compliant, (3) 16 stated that 25-50 percent would be compliant, and (4) 16 stated that less than 25 percent would be compliant. Moreover, 34 percent of respondents reported that they had contingency plans, 46 percent stated that they were in the process of developing plans, 12 percent stated that plans would be developed, and 8 percent said they did not intend to develop contingency plans.

- In January 1999, the United States Conference of Mayors reported on the results of its survey of 220 cities. It found that (1) 97 percent had a citywide plan to address Year 2000 issues, (2) 22 percent had repaired or replaced less than half of their systems, and (3) 45 percent had completed less than half of their testing.

Of critical importance to the nation are services essential to the safety and well-being of individuals across the country, namely 9-1-1 systems and law enforcement. For the most part, responsibility for ensuring continuity of service for 9-1-1 calls and law enforcement resides with thousands of state and local jurisdictions. On April 29 we testified that not enough was known about the status of either 9-1-1 systems or of state and local law enforcement activities to conclude about either's ability during the transition to the year 2000 to meet the public safety and well-being needs of local communities across the nation.³⁹ While the federal government planned additional actions to determine the status of these areas, we stated that the President's Council on Year 2000 Conversion should use such information to identify specific risks and develop appropriate strategies and contingency plans to respond to those risks.

Recognizing the seriousness of the Year 2000 risks facing state and local governments, the President's Council has developed initiatives to address the readiness of state and local governments. For example:

- The Council established working groups on state and local governments and tribal governments.
- Council officials participate in monthly multistate conference calls.
- In July 1998 and March 1999, the Council, in partnership with the National Governors' Association, convened Year 2000 summits with state and U.S. territory Year 2000 coordinators.
- On May 24, the Council announced a nationwide campaign to promote "Y2K Community Conversations" to support and encourage efforts of government officials, business leaders, and interested citizens to share information on their progress. To support this initiative, the Council has developed and is distributing a toolkit that

³⁹Year 2000 Computing Challenge: Status of Emergency and State and Local Law Enforcement Systems Is Still Unknown (GAO/T-AIMD-99-163, April 29, 1999).

provides examples of which sectors should be represented at these events and issues that should be addressed.

State-Administered Federal Human Services Programs Are At Risk

Among the critical functions performed by states are the administration of federal human services programs. As we reported in November 1998, many systems that support state-administered federal human services programs were at risk, and much work remained to ensure that services would continue.⁴⁰ In February of this year, we testified that while some progress had been achieved, many states' systems were not scheduled to become compliant until the last half of 1999.⁴¹ Accordingly, we concluded that, given these risks, business continuity and contingency planning was even more important in ensuring continuity of program operations and benefits in the event of systems failures.

Subsequent to our November 1998 report, OMB directed federal oversight agencies to include the status of selected state human services systems in their quarterly reports. Specifically, in January 1999, OMB requested that agencies describe actions to help ensure that federally supported, state-run programs will be able to provide services and benefits. OMB further asked that agencies report the date when each state's systems will be Year 2000-compliant. Tables 1 and 2 summarize the information gathered by the Departments of Agriculture and Health and Human Services, respectively, on the compliance status of state-level organizations. The information indicates that a number of states do not plan to complete their Year 2000 efforts until the last quarter of 1999.

⁴⁰Year 2000 Computing Crisis: Readiness of State Automated Systems to Support Federal Welfare Programs (GAO/AIMD-99-28, November 6, 1998).

⁴¹Year 2000 Computing Crisis: Readiness of State Automated Systems That Support Federal Human Services Programs (GAO/T-AIMD-99-91, February 24, 1999).

Table 1: Reported State-level Readiness for Federally Supported Programs, Department of Agriculture, May 1999^a

Program	Compliant	April-June	July-September	October-December	Unknown ^b
Food Stamps	25	12	14	3	0
Child Nutrition	29	9	10	4	2
Women, Infants, and Children	33	11	7	3	0

^aThis chart contains readiness information from the 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands.

^bUnknown indicates the state did not provide a date or the date was unknown.

Source: Department of Agriculture.

Table 2: Reported State-level^a Readiness for Federally Supported Programs, Department of Health and Human Services^b

Program	Compliant ^c	Jan.- March	April- June	July- Sept.	Oct.- Dec.	Unk. ^d	N/A ^e
Child Care	24	5	5	8	2	6	4
Child Support Enforcement	15	4	13	8	8	6	0
Child Welfare	20	5	9	11	3	5	1
Low Income Housing Energy Assistance Program	10	0	3	7	1	32	1
Medicaid – Integrated Eligibility System	20	0	15	15	4	0	0
Medicaid – Management Information System	17	0	19	14	4	0	0
Temporary Assistance for Needy Families	19	3	12	15	1	4	0

^aThis chart contains readiness information from the 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands.

^bThe OMB report stated that this information was as of January 31, 1999. However, OMB provided a draft table to the National Association of State Information Resource Executives which, in turn, provided the draft table to the states. The states were asked to contact HHS and provide corrections by June 1, 1999. For its part, HHS submitted updated state data to OMB in early June.

^cIn many cases the report indicated a date instead of whether the state was compliant. We assumed that states reporting completion dates in 1998 or earlier were compliant.

^dUnknown indicates that, according to OMB, the data reported by the states were unclear or that no information was reported by the agency.

^eN/A indicates that the states or territories reported that the data requested were not applicable to them.

Source: Progress on Year 2000 Conversion: 9th Quarterly Report (OMB, issued on June 15, 1999).

In addition, in June 1999, OMB reported that, as of March 31, 1999, 27 states' unemployment insurance systems were compliant, 11 planned to be completed between April and June 1999, 10 planned to be completed between July and September, and 5 planned to be completed between October and December.

Along with obtaining readiness information from the states, agencies have initiated additional actions to help ensure the Year 2000 compliance of state-administered programs. About a quarter of the federal government's programs designated high-impact by OMB are state-administered, such as Food Stamps and Temporary Assistance for

Needy Families. In response to OMB's March memorandum regarding the high-impact programs, the Departments of Agriculture, Health and Human Services, and Labor reported on various actions that they are taking or plan to take to help ensure the Year 2000 compliance of their state-administered programs. For example:

- The Department of Agriculture reported in May that its Food and Nutrition Service requested that states provide their contingency plans and had contracted for technical support services to review these plans, as needed, and to assist in its oversight of other state Year 2000 activities.
- The Department of Health and Human Services reported that its Administration for Children and Families and Health Care Financing Administration had contracted for on-site assessments of state partners, which will include reviews of business continuity and contingency plans.
- The Department of Labor reported that states are required to submit a certification of Year 2000 compliance for their benefit and tax systems along with an independent verification and validation report. In addition, Labor required that state agencies prepare business continuity and contingency plans, which will be reviewed by Labor officials. Further, the department plans to design and develop a prototype PC-based system to be used in the event that a state's unemployment insurance system is unusable due to a Year 2000-induced problem.

An example of the benefits that federal/state partnerships can provide is illustrated by the Department of Labor's unemployment services program. In September 1998, we reported that many State Employment Security Agencies were at risk of failure as early as January 1999 and urged the Department of Labor to initiate the development of realistic contingency plans to ensure continuity of core business processes in the event of Year 2000-induced failures.⁴² Just last month, we testified that four state agencies' systems could have failed if systems in those states had not been programmed with an emergency patch in December 1998. This patch was developed by several of the state agencies and promoted to other state agencies by the Department of Labor.⁴³

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

Beyond the risks faced by 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

⁴²Year 2000 Computing Crisis: Progress Made at Department of Labor, But Key Systems at Risk (GAO/T-AIMD-98-303, September 17, 1998).

⁴³Year 2000 Computing Challenge: Labor Has Progressed But Selected Systems Remain at Risk (GAO/T-AIMD-99-179, May 12, 1999).

use a sector-based approach and establish the effective public-private partnerships necessary to address this issue.⁴⁴ 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 has formed 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.

Our April 1998 report also recommended that the President's Council 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 then planned to issue quarterly public reports summarizing these assessments. The first such report was issued on January 7, 1999.

The Council's second report was issued on April 21, 1999.⁴⁵ The report stated that substantial progress had been made in the prior 6 to 12 months, but that there was still much work to be done. According to the Council, most industries had projected completion target dates between June and September and were in, or would soon be moving into, the critical testing phase. Key points in the Council's April assessment included the following:

- National Year 2000 failures in key U.S. infrastructures such as power, banking, telecommunications, and transportation are unlikely.
- Organizations that are not paying appropriate attention to the Year 2000 problem or that are adopting a "wait and see" strategy—an attitude prevalent among some small businesses and local governments—are putting themselves and those that depend upon them at great risk.
- International Year 2000 activity, although increasing, is lagging and will be the source of the greatest risk.

⁴⁴GAO/AIMD-98-85, April 30, 1998.

⁴⁵Both of the Council's reports are available on its web site, www.y2k.gov. In addition, the Council, in conjunction with the Federal Trade Commission and the General Services Administration, has established a toll-free Year 2000 information line, 1-888-USA-4Y2K. The Federal Trade Commission has also included Year 2000 information of interest to consumers on its web site, www.consumer.gov.

The Council's assessment reports have substantially increased the nation's understanding of the Year 2000 readiness of key industries. However, the picture remained incomplete in certain key areas because the surveys conducted did not have a high response rate, the assessment was general, or the data were old. For example, according to the assessment report, only 13 percent of the nation's 9-1-1 centers had responded to a survey being conducted by the Federal Emergency Management Agency in conjunction with the National Emergency Number Association, calling into question whether the results of the survey accurately portrayed the readiness of the sector. In the case of drinking water, both the January and April reports provided a general assessment but did 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). Finally, in some cases, such as the transit industry, the sector surveys had been conducted months earlier.

The President's Council is to be commended on the strides that it has made to obtain Year 2000 readiness data 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, in testimony this January, we suggested that the Council consider additional actions such as continuing to aggressively pursue readiness information in the areas in which it is lacking.⁴⁶ If the current approach of using associations to voluntarily collect information does not yield the necessary information, we suggested that the Council may wish to consider whether legislative remedies (such as requiring disclosure of Year 2000 readiness data) should be proposed. In response to this suggestion, the Council Chair stated that the Council has focused on collaboration and communication with associations and other groups as a means to get industries to share information on their Year 2000 readiness and that the Council did not believe that legislation would be necessary. The Council's next sector report is expected to be released later this month.

Subsequent to the Council's April report, surveys in key sectors have been issued. In addition, we have issued several products related to several of these sectors. I will now discuss the results of some of these surveys and our reviews.

Energy Sector

In April, we reported that while the electric power industry had concluded that it had made substantial progress in making its systems and equipment ready to continue operations into the year 2000, significant risks remained since many reporting organizations did not expect to be Year 2000 ready within the June 1999 industry target date.⁴⁷ We, therefore, suggested that the Department of Energy (1) work with the Electric Power Working Group to ensure that remediation activities were accelerated for the utilities that expected to miss the June 1999 deadline for achieving Year 2000

⁴⁶GAO/T-AIMD-99-50, January 20, 1999.

⁴⁷Year 2000 Computing Crisis: Readiness of the Electric Power Industry (GAO/AIMD-99-114, April 6, 1999).

readiness and (2) encourage state regulatory utility commissions to require a full public disclosure of Year 2000 readiness status of entities transmitting and distributing electric power. The Department of Energy generally agreed with our suggestions. We also suggested that the Nuclear Regulatory Commission (1) in cooperation with the Nuclear Energy Institute, work with nuclear power plant licensees to accelerate the Year 2000 remediation efforts among the nuclear power plants that expect to meet the June 1999 deadline for achieving readiness and (2) publicly disclose the Year 2000 readiness of each of the nation's operational nuclear reactors. In response, the Nuclear Regulatory Commission stated that it plans to focus its efforts on nuclear power plants that may miss the July 1, 1999 milestone and that it would release the readiness information on individual plants that same month.

Subsequent to our report, on April 30, 1999, the North American Electric Reliability Council released its third status report on electric power systems. According to the North American Electric Reliability Council, as of March 31, 1999, reporting organizations, on average, had completed 99 percent of the inventory phase, 95 percent of the assessment phase, and 75 percent of the remediation/testing phase.

In May, we reported⁴⁸ that while the domestic oil and gas industries had reported that they had made substantial progress in making their equipment and systems ready to continue operations into the year 2000, risks remained. In particular, a February industrywide survey found that over a quarter of the oil and gas industries reported that they did not expect to be Year 2000 ready until the second half of 1999—leaving little time for resolving unexpected problems. Moreover, although over half of our oil is imported, little was known about the Year 2000 readiness of foreign oil suppliers. Further, while individual domestic companies reported that they were developing Year 2000 contingency plans, there were no plans to perform a national-level risk assessment and develop contingency plans to deal with potential shortages or disruptions in the nation's overall oil and gas supplies. We suggested that the Council's oil and gas working group (1) work with industry associations to perform national-level risk assessments and develop and publish credible, national-level scenarios regarding the impact of potential Year 2000 failures and (2) develop national-level contingency plans. The working group generally agreed with these suggestions.

Water Sector

As I previously mentioned, the Council's January and April assessment reports provided only a general assessment of the drinking water sector and did not contain detailed data. Similarly, in April we reported⁴⁹ that insufficient information was available to assess and manage Year 2000 efforts in the water sector, and little additional information was

⁴⁸Year 2000 Computing Crisis: Readiness of the Oil and Gas Industries (GAO/AIMD-99-162, May 19, 1999).

⁴⁹Year 2000 Computing Crisis: Status of the Water Industry (GAO/AIMD-99-151, April 21, 1999).

expected under the current regulatory approach. While the Council's water sector working group had undertaken an awareness campaign and had urged national water sector associations to continue to survey their memberships, survey response rates had been low. Further, Environmental Protection Agency officials stated that the agency lacked the rules and regulations necessary to require water and wastewater facilities to report on their Year 2000 status.

Our survey of state regulators found that a few states were proactively collecting Year 2000 compliance data from regulated facilities, a much larger group of states was disseminating Year 2000 information, while another group was not actively using either approach. Additionally, only a handful of state regulators believed that they were responsible for ensuring facilities' Year 2000 compliance or overseeing facilities' business continuity and contingency plans. Among our suggested actions was that the Council, the Environmental Protection Agency, and the states determine which regulatory organization should take responsibility for assessing and publicly disclosing the status and outlook of water sector facilities' Year 2000 business continuity and contingency plans. The Environmental Protection Agency generally agreed with our suggestions but one official noted that additional legislation may be needed if the agency is to take responsibility for overseeing facilities' Year 2000 business continuity and contingency plans.

Health Sector

The health sector includes health care providers (such as hospitals and emergency health care services), insurers (such as Medicare and Medicaid), and biomedical equipment. With respect to biomedical equipment, on June 10 we testified⁵⁰ that, in response to our September 1998 recommendation,⁵¹ HHS, in conjunction with the Department of Veterans Affairs, had established a clearinghouse on biomedical equipment. As of June 1, 1999, 4,142 biomedical equipment manufacturers had submitted data to the clearinghouse. About 61 percent of these manufacturers reported having products that do not employ dates and about 8 percent (311 manufacturers) reported having date-related problems such as an incorrect display of date/time. According to the Food and Drug Administration, the 311 manufacturers reported 897 products with date-related problems. However, not all compliance information was available on the clearinghouse because the clearinghouse referred the user to 427 manufacturers' web sites. Accordingly, we reviewed the web sites of these manufacturers and found, as of June 1, 1999, a total of 35,446 products.⁵² Of these products, 18,466 were reported as not employing a date,

⁵⁰Year 2000 Computing Challenge: Concerns About Compliance Information on Biomedical Equipment (GAO/T-AIMD-99-209, June 10, 1999).

⁵¹Year 2000 Computing Crisis: Compliance Status of Many Biomedical Equipment Items Still Unknown (GAO/AIMD-98-240, September 18, 1998).

⁵²Because of limitations in many of the manufacturers web sites, our ability to determine the total number of biomedical equipment products reported and their compliance status was impaired. Accordingly, the actual number of products reported by the manufacturers could be significantly higher than the 35,446 products that we counted.

11,211 were reported as compliant, 4,445 were shown as not compliant, and the compliance status of 1,324 was unknown.

In addition to the establishment of a clearinghouse, our September 1998 report also recommended that HHS and the Department of Veterans Affairs take prudent steps to jointly review manufacturers' test results for critical care/life support biomedical equipment. We were especially concerned that the departments review test results for equipment previously deemed to be noncompliant but now deemed by manufacturers to be compliant, or equipment for which concerns about compliance remained. In May 1999, the Food and Drug Administration, a component agency of HHS, announced that it planned to develop a list of critical care/life support medical devices and the manufacturers of these devices, select a sample of manufacturers for review, and hire a contractor to develop a program to assess manufacturers' activities to identify and correct Year 2000 problems for these medical devices. In addition, if the results of this review indicated a need for further review of manufacturer activities, the contractor would review a portion of the remaining manufacturers not yet reviewed. Moreover, according to the Food and Drug Administration, any manufacturer whose quality assurance system appeared deficient based on the contractors review would be subject to additional reviews to determine what actions would be required to eliminate any risk posed by noncompliant devices.

In April testimony⁵³ we also reported on the results of a Department of Veterans Affairs survey of 384 pharmaceutical firms and 459 medical-surgical firms with whom it does business. Of the 52 percent of pharmaceutical firms that responded to the survey, 32 percent reported that they were compliant. Of the 54 percent of the medical-surgical firms that responded, about two-thirds reported that they were compliant.

Banking and Finance Sector

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 agencies⁵⁴ to ensure that the institutions that they oversee are ready to handle the Year 2000 problem.⁵⁵ We concluded that the regulators had made significant progress in assessing the readiness of member institutions and in 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

⁵³Year 2000 Computing Crisis: Action Needed to Ensure Continued Delivery of Veterans Benefits and Health Care Services (GAO/T-AIMD-99-136, April 15, 1999).

⁵⁴The 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.

⁵⁵Year 2000 Computing Crisis: Federal Depository Institution Regulators Are Making Progress, But Challenges Remain (GAO/T-AIMD-98-305, September 17, 1998).

address those institutions that falter in the later stages of correction and to address disruptions caused by international and public infrastructure failures.

In April, we reported that the Federal Reserve System--which is instrumental to our nation's economic well-being, since it provides depository institutions and government agencies services such as processing checks and transferring funds and securities, has effective controls to help ensure that its Year 2000 progress is reported accurately and reliably.⁵⁶ We also found that it is effectively managing the renovation and testing of its internal systems and the development and planned testing of contingency plans for continuity of business operations. Nevertheless, the Federal Reserve System still had much to accomplish before it is fully ready for January 1, 2000, such as completing validation and implementation of all of its internal systems and completing its contingency plans.

In addition to the domestic banking and finance sector, large U.S. financial institutions have financial exposures and relationships with international financial institutions and markets that may be at risk if these international organizations are not ready for the date change occurring on January 1, 2000. In April, we reported⁵⁷ that foreign financial institutions had reportedly lagged behind their U.S. counterparts in preparing for the Year 2000 date change. Officials from four of the seven large foreign financial institutions we visited said they had scheduled completion of their Year 2000 preparations about 3 to 6 months after their U.S. counterparts, but they planned to complete their efforts by mid-1999 at the latest. Moreover, key international market supporters, such as those that transmit financial messages and provide clearing and settlement services, told us that their systems were ready for the date change and that they had begun testing with the financial organizations that depended on these systems. Further, we found that seven large U.S. banks and securities firms we visited were taking actions to address their international risks. In addition, U.S. banking and securities regulators were also addressing the international Year 2000 risks of the institutions that they oversee.

With respect to the insurance industry, in March, we concluded that insurance regulator presence regarding the Year 2000 area was not as strong as that exhibited by the banking and securities industry.⁵⁸ State insurance regulators we contacted were late in raising industry awareness of potential Year 2000 problems, provided little guidance to regulated institutions, and failed to convey clear regulatory expectations to companies about Year 2000 preparations and milestones. Nevertheless, the insurance industry is reported by both its regulators and by other outside observers to be generally on track to being ready for 2000. However, most of these reports are based on self-reported information and,

⁵⁶Year 2000 Computing Crisis: Federal Reserve Has Established Effective Year 2000 Management Controls for Internal Systems Conversion (GAO/AIMD-99-78, April 9, 1999).

⁵⁷Year 2000: Financial Institution and Regulatory Efforts to Address International Risks (GAO/GGD-99-62, April 27, 1999).

⁵⁸Insurance Industry: Regulators Are Less Active in Encouraging and Validating Year 2000 Preparedness (GAO/T-GGD-99-56, March 11, 1999).

compared to other financial regulators, insurance regulators' efforts to validate this information generally began late and were more limited.

In a related report in April,⁵⁹ we stated that variations in oversight approaches by state insurance regulators also made it difficult to ascertain the overall status of the insurance industry's Year 2000 readiness. We reported that the magnitude of insurers' Year 2000-related liability exposures could not be estimated at that time but that costs associated with these exposures could be substantial for some property-casualty insurers, particularly those concentrated in commercial-market sectors. In addition, despite efforts to mitigate potential exposures, the Year 2000-related costs that may be incurred by insurers would remain uncertain until key legal issues and actions on pending legislation were resolved.

Transportation Sector

A key component to the nation's transportation sector are airports. This January we reported on our survey of 413 airports.⁶⁰ We found that while the nation's airports are making progress in preparing for the year 2000, such progress varied. Of the 334 airports responding to our survey, about one-third reported that they would complete their Year 2000 preparations by June 30, 1999. The other two-thirds either planned on a later date or failed to estimate any completion date, and half of these airports did not have contingency plans for any of 14 core airport functions. Although most of those not expecting to be ready by June 30 are small airports, 26 of them are among the nation's largest 50 airports.

On June 18, the Federal Aviation Administration issued an air industry Year 2000 status report that included information on airports and airline carriers. Table 3 provides the assessment, renovation, validation, and implementation information contained in this report.

⁵⁹Year 2000: State Insurance Regulators Face Challenges in Determining Industry Readiness (GAO/GGD-99-87, April 30, 1999).

⁶⁰Year 2000 Computing Crisis: Status of Airports' Efforts to Deal With Date Change Problem (GAO/RCED/AIMD-99-57, January 29, 1999).

Table 3: Industry Segment Percentage Completion of Year 2000 Remediation Phases

Industry Segment	Assessment	Renovation	Validation	Implementation
Large hub airports	98%	63%	31%	26%
Medium hub airports	100%	70%	43%	37%
Small hub airports	94%	61%	55%	48%
Non-hub airports	93%	67%	67%	70%
Major carriers	100%	75%	50%	^a
Low-cost carriers	73%	38%	19%	18%

^aImplementation was occurring as validation and testing were completed.

Note: Airport information was based on data as of March 15, 1999 from the American Association of Airport Executives and the Airports Council International/North America. The major carrier information based on data as of February 22, 1999 from the Air Transport Association of America, and the low-cost carrier information was based on data as of November 30, 1998 from the National Air Carriers Association, Inc.

Source: Federal Aviation Administration.

Manufacturing and Small Business Sector

The manufacturing and small business sector includes the entities that produce or sell a myriad of products such as chemicals, electronics, heavy equipment, food, textiles, and automobiles. With respect to the chemical industry, table 4 contains the latest survey data by Chemical Manufacturers Association--which represents over 190 primarily large chemical companies--and shows that while some companies' systems are Year 2000 ready, others are in varying stages of completion. This survey provided information on the Year 2000 readiness stage of 123 respondents with respect to their business systems, manufacturing, inventory, and distribution systems, embedded systems, and supply chain as of May 12, 1999.

Table 4: Results of May 12, 1999 Survey of Chemical Manufacturers Association^a

Function	Year 2000 Ready	Planning	Inventory/ Assessment	Remediation	Validation
Business systems	26	1	5	51	27
Manufacturing, inventory, and distribution systems	18	2	7	53	28
Embedded systems	15	2	26	52	13
Supply chain	10	4	51	22	21

^aSome respondents did not provide information to all questions or stated that the question was not applicable.

Source: Chemical Manufacturers Association statement before the Senate Special Committee on the Year 2000 Technology Problem, May 14, 1999.

Since the Chemical Manufacturers Association represented mainly large companies, a survey of small and mid-sized chemical companies was sponsored by several industry associations⁶¹ to assist the Congress, the administration, and the U.S. Chemical Safety and Hazard Investigation Board by obtaining information on the preparedness of this segment of the industry. Table 5 contains the results of the survey, which was conducted between March and May 1999.

⁶¹The sponsors of the survey were the American Crop Protection Association, Chemical Producers & Distributors Association, Chemical Specialties Manufacturers Association, International Sanitary Supply Association, National Association of Chemical Distributors, Responsible Industry for a Sound Environment, and the Synthetic Organic Chemical Manufacturers Association.

Table 5: Readiness Stage of Small and Medium-Sized Chemical Companies^a

Function	Year 2000 Ready	Planning	Inventory/ Assessment	Remediation	Validation
Business systems	147	8	4	24	12
Manufacturing, inventory, and distribution systems	133	8	3	21	13
Embedded systems	83	3	7	13	6
Supply chain	80	17	29	17	25

^aSome respondents did not provide information to all questions or stated that the question was not applicable.

Source: Year 2000 Readiness Disclosure Survey of Small & Mid-Sized Chemical Companies, June 9, 1999.

Another key segment of the economy are small businesses. The National Federation of Independent Business and Wells Fargo sponsored a third survey of the Year 2000 preparedness of small businesses between mid-April and mid-May 1999. This survey found that 84 percent of small businesses are directly exposed to a possible Year 2000 problem. Of the small businesses directly exposed to the Year 2000 problem, 59 percent had taken action, 12 percent planned to take action, and 28 percent did not plan to take action (the other 1 percent responded that the question was not applicable). In addition, 43 percent of the small businesses that were aware of the Year 2000 problem had made contingency plans to minimize the impact of potential problems.

In summary, while improvement has been shown, much work remains at the national, federal, state, and local levels to ensure that major service disruptions do not occur. Specifically, remediation must be completed, end-to-end testing performed, and business continuity and contingency plans developed. Similar actions remain to be completed by the nation's key sectors. Accordingly, whether the United States successfully confronts the Year 2000 challenge will largely depend on the success of federal, state, and local governments, as well as the private sector working separately and together to complete these actions. Accordingly, strong leadership and partnerships must be maintained to ensure that the needs of the public are met at the turn of the century.

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

APPENDIX I

Federal High-Impact Programs and Lead Agencies

APPENDIX I

Agency	Program
Department of Agriculture	Child Nutrition Programs
Department of Agriculture	Food Safety Inspection
Department of Agriculture	Food Stamps
Department of Agriculture	Special Supplemental Nutrition Program for Women, Infants, and Children
Department of Commerce	Patent and trademark processing
Department of Commerce	Weather Service
Department of Defense	Military Hospitals
Department of Defense	Military Retirement
Department of Education	Student Aid
Department of Energy	Federal electric power generation and delivery
Department of Health and Human Services	Child Care
Department of Health and Human Services	Child Support Enforcement
Department of Health and Human Services	Child Welfare
Department of Health and Human Services	Disease monitoring and the ability to issue warnings
Department of Health and Human Services	Indian Health Service
Department of Health and Human Services	Low Income Home Energy Assistance Program
Department of Health and Human Services	Medicaid
Department of Health and Human Services	Medicare
Department of Health and Human Services	Organ Transplants
Department of Health and Human Services	Temporary Assistance for Needy Families
Department of Housing and Urban Development	Housing loans (Government National Mortgage Association)

Department of Housing and Urban Development	Section 8 Rental Assistance
Department of Housing and Urban Development	Public Housing
Department of Housing and Urban Development	FHA Mortgage Insurance
Department of Housing and Urban Development	Community Development Block Grants
Department of the Interior	Bureau of Indians Affairs programs
Department of Justice	Federal Prisons
Department of Justice	Immigration
Department of Justice	National Crime Information Center
Department of Labor	Unemployment Insurance
Department of State	Passport Applications and Processing
Department of Transportation	Air Traffic Control System
Department of Transportation	Maritime Safety Program
Department of the Treasury	Cross-border Inspection Services
Department of Veterans Affairs	Veterans' Benefits
Department of Veterans Affairs	Veterans' Health Care
Federal Emergency Management Agency	Disaster Relief
Office of Personnel Management	Federal Employee Health Benefits
Office of Personnel Management	Federal Employee Life Insurance
Office of Personnel Management	Federal Employee Retirement Benefits
Railroad Retirement Board	Retired Rail Workers Benefits
Social Security Administration	Social Security Benefits
U.S. Postal Service	Mail Service

GAO REPORTS AND TESTIMONY ADDRESSING THE YEAR 2000 CRISIS

Defense Computers: Management Controls Are Critical To Effective Year 2000 Testing
(GAO/AIMD-99-172, June 30, 1999)

Year 2000 Computing Crisis: Customs is Making Good Progress (GAO/T-AIMD-99-225, June 29, 1999)

Year 2000 Computing Challenge: Delivery of Key Benefits Hinges on States' Achieving Compliance (GAO/T-AIMD/GGD-99-221, June 23, 1999)

Year 2000 Computing Challenge: Estimated Costs, Planned Uses of Emergency Funding, and Future Implications (GAO/T-AIMD-99-214, June 22, 1999)

GSA's Effort to Develop Year 2000 Business Continuity and Contingency Plans for Telecommunications Systems (GAO/AIMD-99-201R, June 16, 1999)

Year 2000 Computing Crisis: Actions Needed to Ensure Continued Delivery of Veterans Benefits and Health Care Services (GAO/AIMD-99-190R, June 11, 1999)

Year 2000 Computing Challenge: Concerns About Compliance Information on Biomedical Equipment (GAO/T-AIMD-99-209, June 10, 1999)

Year 2000 Computing Challenge: Much Biomedical Equipment Status Information Available, Yet Concerns Remain (GAO/T-AIMD-99-197, May 25, 1999)

Year 2000 Computing Challenge: OPM Has Made Progress on Business Continuity Planning (GAO/GGD-99-66, May 24, 1999)

VA Y2K Challenges: Responses to Post-Testimony Questions (GAO/AIMD-99-199R, May 24, 1999)

Year 2000 Computing Crisis: USDA Needs to Accelerate Time Frames for Completing Contingency Planning (GAO/AIMD-99-178, May 21, 1999)

Year 2000 Computing Crisis: Readiness of the Oil and Gas Industries (GAO/AIMD-99-162, May 19, 1999)

Year 2000 Computing Challenge: Time Issues Affecting the Global Positioning System (GAO/T-AIMD-99-187, May 12, 1999)

Year 2000 Computing Challenge: Education Taking Needed Actions But Work Remains (GAO/T-AIMD-99-180, May 12, 1999)

Year 2000 Computing Challenge: Labor Has Progressed But Selected Systems Remain at Risk (GAO/T-AIMD-99-179, May 12, 1999)

Year 2000: State Insurance Regulators Face Challenges in Determining Industry Readiness (GAO/GGD-99-87, April 30, 1999)

Year 2000 Computing Challenge: Status of Emergency and State and Local Law Enforcement Systems Is Still Unknown (GAO/T-AIMD-99-163, April 29, 1999)

Year 2000 Computing Crisis: Costs and Planned Use of Emergency Funds (GAO/AIMD-99-154, April 28, 1999)

Year 2000: Financial Institution and Regulatory Efforts to Address International Risks (GAO/GGD-99-62, April 27, 1999)

Year 2000 Computing Crisis: Readiness of Medicare and the Health Care Sector (GAO/T-AIMD-99-160, April 27, 1999)

U.S. Postal Service: Subcommittee Questions Concerning Year 2000 Challenges Facing the Service (GAO/AIMD-99-150R, April 23, 1999)

Year 2000 Computing Crisis: Status of the Water Industry (GAO/AIMD-99-151, April 21, 1999)

Year 2000 Computing Crisis: Key Actions Remain to Ensure Delivery of Veterans Benefits and Health Services (GAO/T-AIMD-99-152, April 20, 1999)

Year 2000 Computing Crisis: Readiness Improving But Much Work Remains To Ensure Delivery of Critical Services (GAO/T-AIMD-99-149, April 19, 1999)

Year 2000 Computing Crisis: Action Needed to Ensure Continued Delivery of Veterans Benefits and Health Care Services (GAO/T-AIMD-99-136, April 15, 1999)

Year 2000 Computing Challenge: Federal Government Making Progress But Critical Issues Must Still Be Addressed to Minimize Disruptions (GAO/T-AIMD-99-114, April 14, 1999)

Year 2000 Computing Crisis: Additional Work Remains to Ensure Delivery of Critical Services (GAO/T-AIMD-99-143, April 13, 1999)

Tax Administration: IRS' Fiscal Year 2000 Budget Request and 1999 Tax Filing Season (GAO/T-GGD/AIMD-99-140, April 13, 1999).

Year 2000 Computing Crisis: Federal Reserve Has Established Effective Year 2000 Management Controls for Internal Systems Conversion (GAO/AIMD-99-78, April 9, 1999)

Year 2000 Computing Crisis: Readiness of the Electric Power Industry (GAO/AIMD-99-114, April 6, 1999)

Year 2000 Computing Crisis: Customs Has Established Effective Year 2000 Program Controls (GAO/AIMD-99-37, March 29, 1999)

Year 2000 Computing Crisis: FAA Is Making Progress But Important Challenges Remain (GAO/T-AIMD/RCED-99-118, March 15, 1999)

Insurance Industry: Regulators Are Less Active in Encouraging and Validating Year 2000 Preparedness (GAO/T-GGD-99-56, March 11, 1999)

Year 2000 Computing Crisis: Defense Has Made Progress, But Additional Management Controls Are Needed (GAO/T-AIMD-99-101, March 2, 1999)

Year 2000 Computing Crisis: Readiness Status of the Department of Health and Human Services (GAO/T-AIMD-99-92, February 26, 1999)

Defense Information Management: Continuing Implementation Challenges Highlight the Need for Improvement (GAO/T-AIMD-99-93, February 25, 1999)

IRS' Year 2000 Efforts: Status and Remaining Challenges (GAO/T-GGD-99-35, February 24, 1999)

Department of Commerce: National Weather Service Modernization and NOAA Fleet Issues (GAO/T-AIMD/GGD-99-97, February 24, 1999)

Year 2000 Computing Crisis: Medicare and the Delivery of Health Services Are at Risk (GAO/T-AIMD-99-89, February 24, 1999)

Year 2000 Computing Crisis: Readiness of State Automated Systems That Support Federal Human Services Programs (GAO/T-AIMD-99-91, February 24, 1999)

Year 2000 Computing Crisis: Customs Is Effectively Managing Its Year 2000 Program (GAO/T-AIMD-99-85, February 24, 1999)

Year 2000 Computing Crisis: Update on the Readiness of the Social Security Administration (GAO/T-AIMD-99-90, February 24, 1999)

Year 2000 Computing Crisis: Challenges Still Facing the U.S. Postal Service (GAO/T-AIMD-99-86, February 23, 1999)

Year 2000 Computing Crisis: The District of Columbia Remains Behind Schedule (GAO/T-AIMD-99-84, February 19, 1999)

High-Risk Series: An Update (GAO/HR-99-1, January 1999)

Year 2000 Computing Crisis: Status of Airports' Efforts to Deal With Date Change Problem (GAO/RCED/AIMD-99-57, January 29, 1999)

Defense Computers: DOD's Plan for Execution of Simulated Year 2000 Exercises (GAO/AIMD-99-52R, January 29, 1999)

Year 2000 Computing Crisis: Status of Bureau of Prisons' Year 2000 Efforts (GAO/AIMD-99-23, January 27, 1999)

Year 2000 Computing Crisis: Readiness Improving, But Much Work Remains to Avoid Major Disruptions (GAO/T-AIMD-99-50, January 20, 1999)

Year 2000 Computing Challenge: Readiness Improving, But Critical Risks Remain (GAO/T-AIMD-99-49, January 20, 1999)

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-98-273, 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)

(511773)

Mr. BOERSMA. Thank you. I appreciate the opportunity to be here today to talk about the State of Michigan and what we have done to provide Y2K readiness for State government services.

When the State started this program in earnest in the middle of 1996, we wanted to make sure that the year 2000 project addressed issues such as correcting date problems to prevent any material impact to government services to our citizens. We wanted to make sure it was cost-effective. And we also wanted to go and make sure that we took something away from this as opposed to just fixing the problem, we were able to use something down the road.

We have gone and we have been able to look at the executive branch of State government in a lot of different areas as it relates to application software, systems software, hardware, telecommunications, physical plant as well as the State vendors that we have—that we deal with, to make sure that they are Y2K compliant as well.

We spent a lot of time in the 1996–1997 area to do discovery and assessment. In 1997 and 1998, we spent a lot of time fixing the problem and 1999 is a year that we are making sure that the problems that have been fixed are in fact correct, so that we can go and do business as usual in the year 2000.

I am happy to report that of the 672 critical applications within State government, that 99 percent are compliant and back in operation. There are five applications that still need to be compliant and they will be done around the end of—the schedule right now is the end of August and they will all be completed.

So we have spent a lot of time and effort to make sure that all of our systems are up and running. We are spending 1999 to make sure—as I said earlier, we are working on closing the remaining open systems that we have. We are making sure that our infrastructure is ready with additional testing. We are working on all of our embedded technology in all of our areas, whether it be in our hospitals or prisons, et cetera, to ensure that all of those particular chips have been tested and are compliant.

We have a supplier compliance data base listing close to 7,000 items that we have on the Internet for not only the State to use but also for letting others use as well, to see what issues are compliant.

In addition to the regular testing that we have done on our very critical applications, we have done what is called end-to-end testing, to make absolutely sure that these critical applications are in fact compliant. And to date, we have had very, very little problems in doing that end-to-end testing.

We have had independent consultants come in to do an independent verification and validation of all of our processes within all of our agencies, and we have gotten an approval with our agencies on the way we have handled this entire operation.

I should also point out that many of the Federal agencies have had auditors come in to check all of our applications and at this point in time, again, we have received a clean bill of health on all of those particular applications that they have audited.

We are spending a lot of time in the awareness and communications area, both within government, but also outside of government

and Captain Ed Buikema will talk more about that in his presentation.

We are spending a considerable amount of time now on business continuity and contingency planning. We have identified some 82 essential functions that we believe are essential—that need to be basically provided within the zero to 5 day category. So we are in the process of completing contingency plans on all of those essential functions right now. We have the first drafts in and we are reviewing those at this time and they look—right now, they look very good.

The other thing we are doing is we are calling it zero day planning. Basically we have identified some key dates, October 1st, which is the State's fiscal year, as well as the end of the year, whereby we are basically looking at best practices as to what we should do, each agency should do, on those particular dates to make sure that come January 3rd, that the State government can work as normal. And so we are working in that regard as well.

We have prepared a tool kit that is in the packet that I have submitted to you, which has been sent to all the local governments and school districts for their review, so that they can go and look at what the State has done. And this is a guideline that they can use to do that. We also have gone and, as I said, prepared various types of awareness sessions throughout the State.

I would be happy to answer any additional questions later.

Mr. HORN. Well, thank you. That is a very interesting proposal that you have been through and that has been successful.

Our third witness on this panel is Captain Ed Buikema, the deputy State director of emergency management for the Michigan State Police. Welcome.

[The prepared statement of Mr. Boersma follows:]

MICHIGAN'S YEAR 2000 PROGRAM

**A Status Report to the U.S. House Subcommittee on
Government Management, Information, and Technology**

The Honorable Stephen Horn, Chair

July 9, 1999

"Information contained in this letter is a Year 2000 READINESS DISCLOSURE as defined by the "Year 2000 Information and Readiness Disclosure Act," P.L. 105-271, 1998 (S.2392)."

Year 2000 Project Goals State Operations

The goals of the State of Michigan Year 2000 Project are to:

- Identify and correct Year 2000 date problems so as to prevent any material impact on governmental services to citizens;
- Ensure that cost-effective approaches are utilized to correct date related problems; and
- Leverage the investment made in making Year 2000 changes to the advantage of the State in moving into the 21st Century.

The Year 2000 Scope

- The scope of the State of Michigan Year 2000 Project includes all agencies within the Executive Branch of Government.
 - Institutions of Higher Education and Legislative and Judicial branch agencies are individually responsible for addressing their issues.
- The Year 2000 Project includes making the following components Year 2000 operable:
 - Application software, both purchased and custom written;
 - Systems software;
 - Network and computing hardware;
 - Telecommunications equipment; and
 - Physical plant and equipment with embedded technology.
 - State Vendors and Suppliers

3

Michigan's Timetable for Y2K

Phase	Critical Applications	IT Infrastructure	Embedded Technology and Suppliers
1. Discovery & Assessment	1996-1997	1996-1997	1998-1999
2. Fixing the Problem	1997-1998	1997-1999	1998-1999
3. Making Sure	1999	1999	1999
4. Business as Usual	2000+	2000+	2000+

4

Results to Date As of June 30, 1999

	<u>Most</u>	<u>Critical</u>	<u>Systems</u>
	<u>Number Done</u>		<u>Percent Done</u>
ASSESSMENT	672		100%
REMEDICATION	668		99%
VALIDATION	664		99%
YEAR 2000 READY	664		99%

Year 2000 Tasks For 1999

<ul style="list-style-type: none">• Closure of All Open Systems• IT Infrastructure Readiness• Embedded Technology• Supplier Compliance• Enterprise Integration Testing• Independent Verification & Validation• Awareness and Communication• Business Continuity/Contingency Planning• Zero-Day Planning

Business Continuity/Contingency Planning

- DMB Guidance Issued March, 1999 Requiring:
 - Essential Functions*, Process Maps and Compliance Units
 - Draft Plans by June, 1999
- BCCP Consultants Are Available to Assist Agencies
- Current Status:
 - 82 Essential Functions Identified
 - Six Agencies with No Essential Functions
 - Nine Agencies Making Good Progress
 - Four Agencies' Data Under Review

7

Zero-Day Planning

- Key Dates
 - October 1, 1999
 - December 31, 1999--January 3, 2000
 - February 28--March 1, 2000
- Best Practices
 - Check Outputs to Customers--Create Feedback Loops
 - Have Key Staff Available--On Call and On Duty
 - Check Facilities, PC's, Servers, Networks, Telephones
 - Run Tests and Check Systems

8

How We Are Helping

- Awareness and Outreach
(Year 2000 Project Office, 517.373.3725)

- Information
 - Standards / Policies
 - Best Practices
 - Supplier Compliance Database
(www.state.mi.us/dmb/year2000)

- Access to Pre-Approved Vendors
(Office of Purchasing, 517.241.1647)

- Toolkit for Michigan's Local Governments

9

Summary of Michigan's Year 2000 Program

We are positioned to succeed

- | | |
|---------------|------------------------|
| ● Awareness | ● Resources |
| ● Budget | • Over 1 million hours |
| ● Plans | • EMD Partnership |
| ● Schedule | ● Risks |
| ● Methodology | ● Reporting |
| | ● Quality Assurance |

10

Mr. BUIKEMA. Thank you, Mr. Chairman, and good morning; good morning, Congressman Knollenberg. I appreciate the opportunity to be here this morning testifying before your committee.

By statute, the director of the Michigan State Police is the director of emergency management within our State. But the legislature created the Emergency Management Division to manage the day-to-day activities within the State and local jurisdictions pertaining to emergency management.

Our responsibility is to coordinate State government response to emergencies and disasters of all kinds. Now as we face the Y2K issue, we figured—we determined that the issue of information was absolutely critical, that we could get our arms around what to expect, what level of planning had taken place and what kind of guidance and information we could provide, especially to local units of government in preparing for Y2K.

So we embarked on a series of infrastructure round tables where we would bring folks in and ask them some very direct questions as to where were they in their preparedness activities for Y2K, what kind of problems could we expect and what kind of guidance could we provide to local government in terms of emergency planning. We have held infrastructure round tables, which is what we are calling them, with electric utilities, for both the big electric utilities as well as with the rural electric cooperatives and the municipal power providers, with natural gas providers, chemical manufacturers, transportation, telecommunications, water and waste water, as well as with the Michigan Hospital Association, and we are planning a round table with 911 providers at the end of the month.

During each of these round tables, we would have a transcriber present, who would transcribe the proceedings. We then passed them out extensively to local government, we put them on our Website, with the intention again of providing the best and most recent information about those elements of the critical infrastructure to local government, to provide them a basis for putting together plans for Y2K.

A companion effort in that regard was providing guidance to local government as to how to proceed with planning for this Y2K issue. We produced a couple of documents similar to what has been done in other States. First of all, we put together an assessment tool which has been provided widely to local jurisdictions in the State of Michigan to again help them assess their risks and vulnerabilities. And then we developed a contingency planning guide as well that has been widely distributed to help them put together contingency plans for their jurisdictions as they look at the Y2K issue. Again, both of those documents have been placed on our Website and have been widely distributed throughout the State.

The State of Michigan then on June 2nd, conducted an exercise for State agencies and there were about 125 persons present at that exercise, and we asked a lot of the what-if questions and worked our way through those in the form of a table top. We are in the process of developing an after-action report for that exercise, which should be completed very soon.

In terms of training and outreach to both State government, but specifically to local government, there has been a lot of activity in our State this year. We have a structure in our State where we

have district personnel and we have encouraged them, as well as the local emergency managers that exist all over the State, to conduct town meetings within their jurisdictions or conferences or forums or seminars. And from our staff, we have provided support to those folks, and at last count, we have appeared at over 100 of those local presentations around the State of Michigan.

More recently, we put on three large Y2K symposiums throughout the State and we brought in a number of State agency representatives to describe where their agencies were in terms of Y2K preparedness, as well as our partners from the utilities as well, to again describe where they were. And we received pretty good media coverage as well, describing that entire effort.

For the end of the year, again as with most States, the State Emergency Operations Center here in Michigan will be activated. We will be asking for information from local units of government on a timely basis; specifically, on January 1st, to tell us what, if anything, has occurred in their jurisdiction. We expect to put together a joint public information center where we are partnering with a variety of State agencies as well as with our utilities, making sure we can receive information in from local jurisdictions and provide guidance and direction as well to the media as well as to our citizens throughout the turnover.

We recognize that this is a unique situation for us, as you mentioned, the Y2K date is non-negotiable. But we also recognize that it provides a real opportunity for us to strengthen the relationships in the emergency management field and we expect to reap the benefits of those relationships well beyond the turnover.

So with that, that gives you an overview of some of the activities that have been taking place in our State and I would be happy to answer any questions later on. Thank you.

Mr. HORN. Well, that is very helpful and I think we will probably have a lot of questions because that point you made in ending, particularly, on the relationships that are established in the long run is what is really helpful here out of this.

Our next presenter is Mr. Arun Gulati, the deputy director, Department of Information Processing for Wayne County, MI. Glad to have you here.

[The prepared statement of Captain Buikema follows:]

**Testimony of
Captain Edward Buikema, Commanding Officer
Emergency Management Division
Michigan Department of State Police**

**Prepared for the House Subcommittee on
Government Management, Information, and Technology**

July 9, 1999

Detroit, Michigan

**MICHIGAN'S YEAR 2000 (Y2K) PREPAREDNESS PROGRAM
Emergency Preparedness and Contingency Planning**

Mr. Chairman and Distinguished Members of the Committee:

Thank you for the opportunity to testify on Michigan's Year 2000 Preparedness Program. The Michigan State Police very much appreciates the leadership that Representative Horn and this Subcommittee have shown in examining Year 2000 issues. With the Year 2000 rollover only 175 days away, it is important that we continue to assess our readiness and preparation efforts to meet this potential problem.

By statute, the Director of the Michigan State Police is the State Director of Emergency Management. The Michigan Emergency Management Act (Act 390) created the Emergency Management Division (EMD) within the Department of State Police. The Commanding Officer of the Emergency Management Division serves as the Deputy State Director of Emergency Management.

As such, the Emergency Management Division is the agency responsible for coordinating state response to emergencies and disasters, regardless of their cause, on behalf of the Governor's Office. In November of 1998, the Division created the *Y2K Preparedness Unit* to coordinate those issues that relate directly to "consequence management" of Y2K issues that could impact public health, safety, and welfare.

Essential Infrastructure Roundtables

The core effort of Year 2000 readiness for the emergency management community and government is to assure the continued delivery of essential services. Essential services are those that are seen as being so vital that their loss or degradation would have a significant negative impact on public health, safety, and welfare for the community, the region, or the state. To assess how prepared we are, the Division has held infrastructure roundtables to provide an assessment of the readiness of essential service infrastructure and identify potential risk areas

that could impact delivery of services. Roundtables have been held for the following sectors:

- Electric Utilities
- Natural Gas Utilities
- Chemical Manufacturers
- Transportation
- Telecommunication Utilities
- Water & Wastewater Utilities
- Hospitals

A 911 roundtable has been scheduled by the Emergency Management Division for July 30, 1999.

Assessment and Contingency Planning Guidance

The Emergency Management Division has also been working proactively to support Michigan's local emergency management programs in preparing for the Year 2000. The Division developed and widely distributed several guidance documents. The first, an assessment tool, was distributed in December 1998, "Maintaining Essential Services in the New Millennium: A Year 2000 Assessment Tool". The workbook serves as a resource and guide for the emergency management community in looking at Year 2000 issues.

The second publication addresses contingency planning and was distributed in January 1999. "Contingency Planning For Essential Services in the New Millennium: A Year 2000 Guide" is the companion to the Emergency Management Division's publication "Maintaining Essential Services in the New Millennium: A Year 2000 Assessment Tool". It provides guidance on developing an overall contingency planning strategy and a sample format for organizing the contingency plan.

Exercising

A state Y2K exercise was held on June 2, 1999. Over 125 people, representing most of the State's agencies, participated in the exercise. Key objectives included:

- To evaluate the state's ability to manage and respond to simultaneous Y2K incidents varying in magnitude and scale.
- To evaluate the State Emergency Operation Center's ability to prioritize response activities based on available resources and manpower.
- To assess the state's ability to coordinate and disseminate timely and accurate information to the public through the media.

Results of the exercise indicate that the state agencies are positioned to transition to the Year 2000 with minimal disruption in the ability to deliver essential services to the people of the State of Michigan.

Training & Outreach

The Division has provided a variety of Y2K training related opportunities and outreach at the local level and to other state agencies. Key activities include:

- Y2K Symposiums held June 22 in Marquette, June 23 in Grayling, and June 24 in Lansing. The symposiums provided information on the preparedness efforts of key state agencies and utilities.
- Public Official Conferences have been scheduled to keep local officials informed as well as providing assistance in the area of Y2K emergency readiness.
- To date, Division staff has made over 100 public presentations statewide on Y2K preparation and contingency planning.
- A Y2K component has been added to the MSP EMD website: www.mspemd.org for information sharing.

Zero-Day Planning Activities

In preparation for the end of year rollover, the Emergency Management Division is planning on executing the following activities:

- **State Emergency Operations Center (SEOC) Activation:** the SEOC will be activated on December 31, 1999, and remain at a defined level of operation readiness to address any potential Y2K disruptions that may occur. Key elements include:
 - Utility liaisons will support the SEOC.
 - Year 2000 monitoring will be underway throughout the transition.
 - Proactive reporting format for assessing local jurisdictions and infrastructure.
 - SEOC will provide information to support Joint Public Information Center Operations.
- **Joint Public Information Center (JPIC) Activation:** a JPIC will be established for the end of year rollover period. The facility will be located at the Collins Center complex.

Upcoming Activities

The Division is working with the Michigan Department of Management and Budget, Year 2000 Project Office to jointly produce a "State of Michigan Year 2000 Readiness Report". The report will be ready by the end of July.

In summary, the Emergency Management Division recognizes the Year 2000 problem as a very real threat to the people and agencies in the State. The Division is working diligently to make sure that we mitigate the exposure to potential problems and position the emergency management organizations to successfully meet the challenges presented by the Year 2000.

Again, thank you for the opportunity to testify.

Mr. GULATI. Good morning and thank you for giving us the opportunity this morning to share the information with you in regard to the actions the county has taken to ensure to our stakeholders that our services will not be impacted because of the Y2K issues.

Realizing the importance of having management involved as well as the number of days left to address the Y2K issue, last year the county formed a management team which includes the directors of all departments and representation from the legislative branch as well as the judicial branch. The executive team also includes representation of elected offices as well as agencies.

The goal through this management team is to ensure that we have the necessary team to make the necessary decisions to move forward in a manner so that we can quickly make the decisions and correct the Y2K issues.

The Y2K program is being directed by Ms. Carol Steffani, she is the director of information processing. Our program follows a detailed charter and we have all the information relating to the charter on the Internet to share with our public. The county program includes three areas—technical, legal and the contingency planning.

The technical area is to ensure that we have identified all the areas and taken the necessary steps to ensure that components will work as we move into Y2K.

The legal is to ensure this team that we are minimizing the liability by taking the necessary steps to do that by communicating to our vendors as well as suppliers as well as our other partners.

Contingency planning is to define that we must have backup plans to ensure that all critical systems will operate as we move into Y2K.

The county has adopted the GAO standard which includes different phases—awareness, inventory and assessment, conversion/remediation, test, and implement and certification. Though these are different phases, they are being run to ensure this team that not only we remediate, but after we remediate, we go back and test to ensure this team if the remediation was not correct, we can go back and forth to ensure that it is functioning as we designed it to.

The county has completed the inventory and assessment of all the information technology components and also completed the remediation of the system running on the mainframe. Though some of the systems will not be implemented in production until later in this quarter, we expect to complete the remediation of the mainframe applications as well as the network by the end of September.

In order to ensure that all technical components are Y2K compliant, we are also going in and remediating approximately 3,200 PCs and we have provided the necessary tools to our users as well as the departments to ensure this team that they run the necessary check, that not only the applications are Y2K compliant, but also the data on those applications.

The county is also examining 70-plus facilities. These facilities include jails, airport, some of the key buildings within the county.

In order to manage all the projects that we have, we have a Y2K program office which is presently tracking over 250 projects and

out of those 250, there are 42 that are mission-critical. And that is producing the necessary reports for the management team.

Through some of the testing we have done, we have found that some of the applications that the vendors informed us were Y2K ready, when we plug in all the dates that are related to the Y2K, they are not ready and some of the vendors have gone back and they are going to bring in the necessary changes to ensure that those products are Y2K ready.

The key dates for the county to be ready for the Y2K are June 30th, that is the date to be ready and have all the contingency plans for the airport. The airport must complete compliance documentation of all critical systems and put written contingency plans in place. That is the key date and yes, we have completed that.

July 16th is a date when we are going to bring the management team together for a table top emergency preparedness exercise.

September 30th is the date to complete the remediation and also the testing.

Wayne County has also adopted a formal emergency readiness plan which specifically defines the steps that we will take to ensure this team that we have prepared for the Y2K.

Contingency plans are being prepared as we speak, and yes, we will have the contingency plan for all mission-critical systems.

Realizing the complexity that we face with the Y2K, we are also looking at developing the transition plan into the last quarter of this year. This transition plan will assure that as we gather and learn new information, we have the team together to manage the risks for going into the year 2000.

In conclusion, yes, we will be ready for the Y2K. But again, we have realized over the last 2 or 3 years now that not only our computers, but the operation of all computers that may be of the citizens, of the State or the Fed, must function properly in order to be ready for the Y2K.

And we very much appreciate your having this forum to share this information and giving us the chance to learn about others also. That is the overview of my testimony and I will be here to answer any questions later on.

Mr. HORN. Thank you. We appreciate that.

Our last presenter on this panel is Kathleen Leavey, the deputy director of the Detroit Water and Sewerage Department.

[The prepared statement of Mr. Gulati follows:]

**Statement by
Mr. Arun Gulati
Deputy Director, Department of Information Processing
Wayne County, Michigan**

before the
**SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION, AND TECHNOLOGY**

of the
**COMMITTEE ON
GOVERNMENT REFORM AND OVERSIGHT**

U. S. HOUSE OF REPRESENTATIVES

July 9, 1999

Mr. Chairman and Members of the Committee:

Good morning. My name is Arun Gulati and I am the Deputy Director of Wayne County's Department of Information Processing. Thank you for the opportunity to inform your committee, and the public, of the activities undertaken by Wayne County, Michigan, to ensure that services to its stakeholders are not impacted by Year 2000 issues.

Wayne County, Michigan, covers an area of approximately 643 square miles and has a population of 2,123,000. Of the 43 cities, villages and townships in Wayne County, visitors are most familiar with Detroit and think of this area as the home of the automotive industry. The headquarters for both Ford Motor Company and General Motors Corporation are located in Wayne County. The County's economic base is large and varied beyond the automotive industry.

The County has an annual budget of \$2 billion, with over 7000 employees providing services.

Year 2000 Compliance Program

The County's comprehensive Year 2000 Compliance Program is directed by Carol Steffanni, Director, Department of Information Processing. The Program reports to an Executive Committee, which also approves policies and standards employed in the Program. The Committee consists of:

- the directors of the eleven executive departments of the County
- representatives from the legislative branch of the County, the Wayne County Commission

YEAR 2000 DISCLOSURE under the Year 2000 Information Readiness & Disclosure Act.

- representatives of the judicial branch through the Probate Court and Third Judicial Circuit Court
- the five elected offices of the County: Clerk, Prosecutor, Register of Deeds, Sheriff, Treasurer; and
- one agency, the Retirement system.

The Program follows a detailed charter, defining the scope of the program, reporting requirements, project management, and other methodologies. The County's Program has benefited from the detailed information shared on the Internet by federal, state and local governmental entities. The County has similarly posted its program documents on its web site for the benefit of others.

The County's Program contains three main components:

1. Technical - Identification and remediation of Year 2000 issues in mainframe systems, PCs, network & operating systems, applications, embedded systems, and external interfaces
2. Legal - There are liability issues if the problems are not addressed and documentation centrally maintained of all efforts
3. Contingency Planning - Mission critical systems must have back up plans in case of failure

The County chose to adapt the methodology described by the U.S. General Accounting Office, dividing the program into phases while recognizing that many of the phases run concurrently or in parallel with each other. They are:

- Awareness
 - Provide information on the potential problem, develop a written program, implement a management structure, and obtain executive level sponsorship
- Inventory and Assessment
 - Take inventory of all systems and equipment which may be affected and prioritize their importance to the County overall, emphasizing public health and safety as the highest priority
 - Assess the remediation required
- Conversion/Remediation
 - Replace, repair, upgrade, re-engineer, retire affected systems or equipment
 - Ensure interfaces will exchange/share data accurately
- Test

- Implement
 - Install and support
- Certification

The County has inventoried and assessed its information technology systems and completed remediation of mainframe hardware, operating systems, software and applications, but for roll-out into production of the last parts of the replacement financial application. Remediation of the network infrastructure, including circuits, hubs, router, servers and network operating system is in progress. Testing has begun on the mainframe and network infrastructure and will be completed by September 30, 1999.

The County is remediating hardware, operating system and software on 3200+ PCs. In addition, we are working with the disparate business areas served by Information Processing to provide Year 2000 compliant versions of department/office specific software unique to their business functions. Tools have also been provided to allow departments to check the Year 2000 compliance of spreadsheets and data. Beyond that, there are 130+ departmental applications in remediation/testing at the present time. All remediation work and testing are scheduled to be completed by September 30, 1999.

The County is also examining 70+ facilities, including the Detroit Metropolitan Wayne County Airport, the fifth busiest in airport operations in the world; Willow Run Airport; 3 Jails, and other governmental buildings. Among the embedded systems being analyzed are the following:

- Heating, ventilation and air conditioning equipment
- Access control systems and alarm systems
- Environmental monitoring systems and sprinkler systems
- Wastewater Treatment plant and retention basins control systems
- Pumps and valves for sewerage systems and removal of water from roads
- Traffic signal devices
- Airport runway and lighting systems
- Kitchen equipment for Meals on Wheels, jails
- Laboratory equipment for the Medical Examiner Examiner's Office, and divisions of the Department of Environment

The County has a centralized Program Office coordinating program management and tracking 250+ individual projects, including 42 Mission Critical Projects. A monthly color-coded status report is provided to the Executive Committee indicating projects on schedule (green), projects 5% or less behind schedule (yellow), and projects more than 5% behind schedule (red).

Issues disclosed in our embedded systems tests are the following:

1. Airport Friction Testing Device
 - The device was upgraded based upon manufacturer specifications
 - The device rolled over from 12/31/1999 to 01/01/2000, but would not accept the four-digit year at leap year testing
 - The vendor is re-working the software application controlling the device
2. Combined Sewer Overflow (CSO) Basins
 - All software is being upgraded
 - One control system is being completely replaced
3. Heating Ventilation Air Conditioner (HVAC)
 - The testing tool identified and resolved a problem completely unrelated to Y2K which had not been solved before
 - Software and logic boards need replacing in several buildings

The County's Year 2000 Program has the following key dates:

- June 30, 1999 – The Airport completed the compliance documentation of all critical systems and/or put written contingency plans in place
- July 16, 1999 – A Countywide tabletop emergency preparedness exercise will be run, including both public safety and business continuity issues
- September 30, 1999 - all County systems are to be remediated and testing completed, unless a written justification has been approved by the Director, Department of Information Processing, for a later date

Wayne County was the first in the state of Michigan to adopt a formal Emergency Readiness Plan specifically to address Year 2000 potential problems. It was signed by County Executive Edward H. McNamara on November 10, 1998. The Plan defines Y2K as potential cause which may trigger public safety emergencies or impede the County's ability to provide public safety services. It establishes efforts to be implemented, and a timetable for their completion, to enhance the County's readiness response. It also designates Emergency Management Division as the County's coordinator of contingency planning efforts. The County's Y2K alert period has been set from 10 pm December 31, 1999, to 5 am on January 1, 2000, and the County's Emergency Operations Center will be staffed.

Contingency plans are being developed now for all mission critical projects, expanding existing emergency readiness plans to include the potential impact of

multiple internal and external factors. The County will also be implementing a transition plan in the last quarter of 1999 to walk the County through the rollover and the first quarter of 2000 by managing risks to avoid service interruption to County stakeholders.

In conclusion, Wayne County is confident that its Year 2000 Compliance Program will be successful. As the testimony of this hearing and other such forums evidences, we are all facing this problem. We have all learned how interdependent we have become, and how we have taken for granted the technology which allows us to provide services. Only by sharing information with each other and the public may we continue to feel confident that we are prepared for this and other potential disruptions. Knowledge and preparation are key to successfully managing such disruptions. Your hearings have provided a forum for the sharing of such information. Thank you.

Ms. LEAVEY. Good morning, Congressman Horn and Congressman Knollenberg. I appreciate the opportunity to be here this morning to advise you on the status of our Y2K readiness.

I can tell you that we are confident that we have identified and are in the process of remediating all of our mission-critical systems and processes so that we can fulfill our mission of providing water and sewer service on January 1, 2000.

Because we are an environmental agency and because we are charged with public health and safety responsibilities, we have followed the EPA guide on the process that should be followed for the readiness on Y2K. That includes the same steps that are in the GAO, but they are a little bit different. We do have awareness, assessment, correction/remediation, contingency planning, testing and implementation.

We are working on all of these areas simultaneously. I am the department's Y2K coordinator, I have a team that is comprised of both consultants and employees who have been working on this process for the last 3 years. We have gone through the department, we too have a lot of facilities, and most of our facilities are active process service facilities. We have a concern, obviously, that we be able to turn on our tap on January 1st and get water, et cetera.

We have been meeting with all of the other utilities in southeastern Michigan to ensure that we are all on target for January 1st. The electric industry, Michigan Consolidated, Ameritech, ourselves and any other utility services have had a round table that we have been working in for the last year. Our purpose is to assist each other and to know what each other's contingency plans are, so we are all on the same line on December 31st. I can tell you in meeting with the other utilities that we are confident that they are doing everything possible to be ready, as are we, on January 1st.

We also have been participating and working with the State emergency planning. There also is a regional planning center that is an emergency center that is going to be set up, an operations center in I think it is Northfield, for the State. We are going to participate in that. We also have a city of Detroit Emergency Center which we will participate in, but we also will have our own emergency operations setup.

At this point we have, for the last 16 years, done table top exercises and contingency planning, again because of the nature of our business. We have worked closely with the University of Michigan and they are developing and we have already done one Y2k table top. We will do others and probably later on in the year, we will involve our customers in that as well.

We have a service area that is approximately 1,000 square miles. We serve 126 communities with water, we serve 76 communities with wastewater services. We have formed a customer task force on Y2K because we want to be able to keep the lines of communications open with our customers. They are an integral part of our contingency communication plan and they will be involved in assisting in either manning or operating processes in the various areas where they are located.

We, as I said, are doing everything we think is necessary. Our contingency plans are not real complicated. We are intending to invest a great deal of money to provide backup service at stations

and facilities that we have identified as critical. Those generators are being manufactured as we speak and installed and tested as we progress through the year. In order not to waste any money on that, we have very involved plans for their use after the rollover date.

But that is our primary contingency plan. However, as I indicated, we have been doing table top emergency exercises for over 16 years. We are treating the Y2K rollover as if it were an emergency, because essentially, if our services stop, we want to find alternative ways to provide service to our customers. We do have a redundant system; that is, most of our large water plants, all of our large water plants and our customers have service, water service coming from two different directions. So if it is shut off in one direction, we have the ability to feed from another. We have water plants located as far north as Port Huron and as far south as Allen Park, we have a total of five. Most of the water plants predate the computer in 2001, so we do not have to worry really about embedded chips there. They have never been operated by computers, they have a life span that exceeds most computers and they will be operating fine and they have been tested.

On the wastewater side, we have some newer computerized processes and those we have been remediating for at least 3 to 5 years.

We, again, feel very confident that we will be on target on January 1. What we have tried to do is to get information to our customers and that is our biggest concern at this point. We do not want people panicking, but we do want people to be prepared in the event that something other than Y2K happens.

As the State Police Chief mentioned, this is an opportunity for all of us to bone up on our emergency operations. We pulled out a booklet that we have had for about 15 years and are using that as one of the things that we distribute to our customers, what to do if you are concerned about a water emergency, what are you going to do if you are concerned about the rollover time, December 31. So we are giving advice in those regards in both water and wastewater service areas.

So our next area we are going to tackle is trying to find a way to make sure our employees are comfortable when they come to work that night, and that is making sure their families are in a place that is safe and sound and they can feel confident and comfortable that their families are OK.

That concludes my testimony, I will be here for questions obviously. Thank you.

[The prepared statement of Ms. Leavey follows:]

Detroit Water & Sewerage Department

Year 2000 Readiness

Dennis W. Archer,
Mayor

Detroit City Council

Gil Hill, President
Maryann Mahaffey, Pro Tem
Clyde Cleveland
Kenneth V. Cockrel, Jr.
Shella M. Cockrel
Kay Everett
Nicholas Hood III
Brenda M. Scott
Alberta Tinsley-Williams

Stephen F. Gorden,
Director

Kathleen Leavey,
Deputy Director

Board of Water Commissioners
Warren C. Evens, President
Mary E. Blackmon, Vice President
Marva L. Goldsmith
Marilynn E. Gosling
Hilliard L. Hampton
David S. Robinson Jr.
Thomas S. Welsh

Detroit Water and Sewerage Department Year 2000 Readiness

- ◆ Mission Statement
- ◆ Introduction (Goals)
- ◆ DWSD's Approach
- ◆ DWSD Readiness Plan
- ◆ EPA Six Step Process
- ◆ External Dependencies
- ◆ Conclusions
- ◆ Questions

Detroit Water & Sewerage Department Year 2000 Readiness

Mission statement

To exceed our customers' expectations through the innovative treatment and transmission of water and wastewater, and the provision of services that promotes healthy communities and economic growth.

Detroit Water and Sewerage Department Year 2000 Readiness

Resources:

The Water and Sewerage Department initiative has been ongoing since 1997.

- ♦ There are currently two teams working on the Y2K initiative for the Department.
- ♦ In excess of 65 million dollars has been appropriated for this effort.

Detroit Water and Sewerage Department Year 2000 Readiness

✓ Establish a Y2K Team, Develop a Project Plan

EXECUTIVE SPONSOR
Deputy Director
Kathleen Leavey

EXECUTIVE MANAGEMENT TEAM

Y2K COORDINATION GROUP
Directors Office, Public Relations, IS
Managers, Y2K Managers, Engineers, etc.

Y2K CORE GROUP
Dep. Director, Asst. to Director, IS
Managers, Y2K Managers, Admin, Asst.

**EMERGENCY MANAGEMENT
COORDINATOR**
Lucille Walker

WASTEWATER OPERATIONS GROUP
Y2K Program Manager
Kevin Quiggie

WATER OPERATIONS
Y2K Program Manager
Theresa McClean

LANCE MITCHELL

BETTY AFARI

**BUSINESS
CONTINUITY
PLANNING**

**CONTINGENCY
PLANNING**

**EMBEDDED
TECHNOLOGIES**

**SUPPLIER CHAIN
MANAGEMENT**

**BUSINESS
CONTINUITY
PLANNING**

**CONTINGENCY
PLANNING**

**EMBEDDED
TECHNOLOGIES**

**SUPPLIER CHAIN
MANAGEMENT**

Detroit Water and Sewerage Department Year 2000 Readiness

- EPA Six Step Approach
- Following industry standards:
 - ◆ Awareness
 - ◆ Assessment
 - ◆ Correction/Remediation
 - ◆ Contingency Planning
 - ◆ Testing/Validation
 - ◆ Implementation

Detroit Water and Sewerage Department Year 2000 Readiness

EPA Step 1: Awareness

Define the Problem and Gain Executive-Level Support

- ♦ Make Y2K a Priority
- ♦ Establish a Y2K Team and Develop a Project Plan
- ♦ Inform/Update Customers

Detroit Water and Sewerage Department Year 2000 Readiness

Inform, update customers

Public Awareness of the Y2K issue has been promoted through the following methods:

- Presentations to Public Groups
- DWSD Hotline
- Brochures, Water Bill Inserts, and Letters to Customers
- Use of Local Cable
- Internal Workshops With Employees

Detroit Water and Sewerage Department Year 2000 Readiness

EPA Step 2: Assessment

- Examine Each Component (Through Inventory)
- Prioritize Systems and Functions (Critical Systems)
- Contact Vendors and Suppliers
- Review Construction Contracts
- Review Long-Term Maintenance Contracts
- Develop Plans for Compliance

Detroit Water and Sewerage Department Year 2000 Readiness

EPA Step 2: Assessment (continued)

Identify Critical Processes and Systems:

- Network Equipment
- Treatment Systems
- Computer Systems Hardware & Applications
- Operating Systems and Databases
- External Interfaces
- Packaged Devices and Automated Devices
- Others

Detroit Water and Sewerage Department Year 2000 Readiness

EPA Step 3: Correction and Remediation

- Change Systems, Upgrade Hardware
- Replace, Upgrade, or Retire Systems or Applications
- Send Out Surveys, Meet With Suppliers
- Convert, Replace, Work Around
- Eliminate

Detroit Water and Sewerage Department

Year 2000 Readiness

EPA Step 4: Contingency Planning

- Responsibility and Notification
- Local/Manual Operation
- Communications
- Standby Capacity
- Staffing
- Verification

Detroit Water and Sewerage Department Year 2000 Readiness

EPA Step 4: Contingency Planning (continued)

Contingency Planning and Disaster Recovery

University of Michigan Involvement:

- + Mock Exercises
- + Loss of Electrical Power
- + Loss of Telecommunication Systems
- + Failure of Other Infrastructure
- + Real Exercises
- + Water and Wastewater Plant Tests
- + Testing (2nd and 3rd quarters of 1999)

Detroit Water and Sewerage Department Year 2000 Readiness

EPÁ Step 5: Testing and Validation

- ♦ Acquire Additional Testing Equipment
- ♦ Follow-up with Suppliers
- ♦ Assess Risk for Non-Responsive Suppliers
- ♦ Verify All Renovated/Upgraded Systems & External Interfaces
- ♦ Re-assess Confidence Levels
- ♦ Verify All Contingency Plans

Detroit Water and Sewerage Department Year 2000 Readiness

EPA Step 6: Implementation

- ♦ Monitor Suppliers, Make Final Assessments
- ♦ Schedule and Coordinate
- ♦ Renovate/Upgrade Systems and Hardware Implementation
- ♦ Remove Designated Applications/Software
- ♦ Revise Recovery Plan
- ♦ Notify System Users

400

Detroit Water and Sewerage Department Year 2000 Readiness

JUNE 1999 - Ramp Up Awareness Campaign
JULY 1999 - Applications Ready
SEP. 1999 - SCADA* Systems Review Complete
SEP. 1999 - Contingency Plans Ready
OCT. 1999 - Facilities Ready
DEC. 1999 - Testing Complete

*Supervisory Control and Data Acquisition

Detroit Water and Sewerage - Readiness Disclosure as per
"Year 2000 Information and Readiness Disclosure Act"

Detroit Water and Sewerage Department

Year 2000 Readiness

External Dependencies

Working with other utilities and suppliers to minimize the impact of external Y2K influences:

- ♦ Ameritech
- ♦ Detroit Edison
- ♦ MichCon
- ♦ PLD (Public Lighting Department)

Detroit Water and Sewerage Department
Year 2000 Readiness

DWSD is actively involved with Y2K Activities.

For further information call the Detroit Water and Sewerage Department Y2K Hotline:

(313) 964-9562

DWSD will also provide periodic updates.

Detroit Water & Sewerage Department Year 2000 Readiness

Introduction - DWSD Goals

- ◆ Provide complete water treatment and service at all times, including at the Millennium
- ◆ Provide full sewerage services and treatment at all times, including at the Millennium

Detroit Water and Sewerage Department Year 2000 Readiness

Conclusion

The department's staff is equipped and experienced in dealing with emergencies. Activities are taking place to augment the Department's current approach, and there will be continuous work on this concern. We are confident that our personnel will respond with the appropriate professionalism to address any Y2K issues that might arise.

Detroit Water and Sewerage Department Year 2000 Readiness

Meeting the needs of the customer:

The water transmission and wastewater treatment, processing, and collection systems are sufficient to meet the current needs of our retail and wholesale customers, as well as those of the Environmental Protection Agency (EPA).

**Detroit Water and Sewerage Department
Year 2000 Readiness**

Questions

Mr. HORN. Thank you. Let us now open it up for questions. I would like Mr. Knollenberg to begin the questioning and we will sort of alternate maybe every 5 minutes and we will get the questions from the audience and then we will get a dialog among yourselves. So Mr. Knollenberg.

Mr. KNOLLENBERG. Thank you, Mr. Chairman. And thank you for your testimony.

Let me start with Ms. Leavey, regarding the water situation, you seem to feel comfortable that things are in relatively decent shape. There is about 200,000 public water systems regulated under, as you know, the Safe Drinking Water Act that serves some 240 million people. The balance of the population is serviced of course from private wells.

Can the Detroit Water and Sewerage Department ensure that there are no violations associated with the Safe Drinking Water Act?

Ms. LEAVEY. Yes, we can do that now, we expect to be able to do that on January 1st. We have never had a problem with that, our water source is very clean, the Detroit River and Lake Huron are very good sources for our customers.

Mr. KNOLLENBERG. And the redundancies you spoke of, you feel pretty comfortable about those functioning as backups in the event there are failures?

Ms. LEAVEY. Yes, we do. We think that if there is any kind of failure in the electric grid, that it will probably be isolated, but we are looking at a normal situation when the power goes down, how do we respond. Normally we have a 3-day turnaround, 1 day turnaround. We can have the same thing happen if a water line breaks like it did in Auburn Hills, where we have people without water service for several days.

So we do not expect Y2K to shut us down. We really do not expect to be shut down by Edison or any of the other utilities. Our biggest concern is that it is the winter time, in the city of Detroit, that is the time where we have more breaks than anything else, and we are concerned that people, if anything happens, will say aha, Y2K. And that is not what is going to happen.

Mr. KNOLLENBERG. It becomes a whipping boy, I take it, for everything.

Ms. LEAVEY. Oh, sure.

Mr. KNOLLENBERG. If I could, Mr. Chairman, one other question I would like to direct. This could be to any of the panel members, but it has to do with emergency management and I think Captain Buikema, you are probably the person that this could go to.

As I travel throughout this part of the State and my district and beyond, I have become acquainted with the inconsistency of the 911 systems that are in place and some rely on older telecommunications, some are certainly—and the best computer equipment is available in some cases. Have you done an assessment that looks at testing these various computer systems associated with both the police force and the fire department in the State of Michigan?

Mr. BUIKEMA. Well, we are planning, as I mentioned, to do a round table with—we have invited I think something like 50 911s to attend at the end of the month on July 30th. And we expect to

have an extensive dialog with them about that very issue at that time.

Up to this point, we have reached out to 911 directors and 911 centers, both—we have encouraged the local emergency management coordinators to have a dialog with those folks to ask the questions that you just asked as well as the State police post commanders—and there are some 64–65 State police posts in the State of Michigan—to also have a dialog with our 911 providers.

We hear anecdotal information concerning various pieces of equipment, some of which have been installed as recently as last year, that are not Y2K compliant, and we are hearing stories that the typical public safety answering points, PSAPs is what they are called, are having to spend anywhere from \$20,000 to \$40,000 to bring them up to be Y2K compliant.

But we do not have a good assessment overall on that, which is why we want to hold that round table at the end of the month, to get our hands around it a little bit better.

Mr. KNOLLENBERG. Would you say that that is something in your discussions with members from other States that is a problem that they have as well?

Mr. BUIKEMA. Yes, just this past Wednesday, I participated in a public safety round table in Washington, DC, with John Koskinen. And there were representatives from around the country there and the issue of 911s was one of the areas of uncertainty, let me put it that way. I think it is just unknown—there were statistics, there are estimates I guess that there are something like 7,000 911 centers in the United States. Assessments have been done in some fashion, but only less than half of them have returned their surveys back. So there are still a lot of unknowns concerning them and Michigan is no different than any of those other States.

Mr. KNOLLENBERG. Thank you. Mr. Chairman.

Mr. HORN. I was very interested in the water and sewerage particularly. Did you read about the Los Angeles situation? That was not a really Y2K situation, but tell me what you have learned from that and are you testing along the line they were? That was what, a 300 million sewage—

Ms. LEAVEY. Gallons of sewage, yeah.

Mr. HORN [continuing]. Spilled, yeah.

Ms. LEAVEY. It was our understanding—and yes, we are aware of it certainly, it gave everybody a heads up. It was our understanding that they were in fact doing a Y2K test on some of their machinery and discharged accidentally. We certainly have no intent of discharging intentionally or accidentally but we are aware now that we have to test those portions of the system as well. However, we already have been looking at those in terms of assessment and inventory, checking with the manufacturers, et cetera, doing the normal process to determine if they are Y2K compliant. We are pretty confident that they are.

Mr. HORN. Well, that is good news, because I think that is one of the things that would really disrupt a community, not just the water, but what the use of the water is.

Ms. LEAVEY. Well, yeah. We do have a concern about that, but our greater concern is individual—well, we have two concerns, the water consumption, public health. We also have a concern about

public health in regard to any backups into people's basements. If there is a very large storm and there are any power shutdowns related to the transmission system for either water or for wastewater, then to protect public health, we may discharge into the Detroit River. But it is our expectation that at that time of year, we would not experience anything like that. But we have met with the State Department of Environmental Quality. In an emergency situation, we would always opt for that as opposed to storing it in people's basements.

Mr. HORN. One question that I am always interested in is since you have gone through this situation of planning and adapting and remediating and so forth, I ask the whole panel, what have you learned that if you had to go through this situation again, what would you want to do first that maybe you did not do in this, because we have all been working our way along trying to solve the problem, or at least remediate it.

Let us start with the first presenter here and that is—we will wait on Mr. Willemsen a minute. Mr. Boersma, what do you think from the State level you would have done differently?

Mr. BOERSMA. I started as the CIO of the State in July 1996 and that was the No. 1 priority that we dealt with. So I think that from that perspective, we certainly had to initially in the first year, year and a half, we had to make up some time. And so we really pushed forward, because the goal—knowing that a lot of IT projects, whether it be public or private sector, do not get done on time, we wanted to make sure that we were not in that situation because, as you said earlier, the date is not going to change.

So we made it a goal that the majority of our critical applications had to be remediated, tested and back into service by the end of this past year. We were successful in doing almost all of those with the exception of a few. So that was a very critical thing. Obviously I think everybody would say one of the key issues is to start earlier on this so that there was more time to go and do this. But we have—as a State, we have learned a lot with Y2K and that is the fact that we did this centrally so we took best practices, even though all of our agencies were involved in this. We took best practices of the agencies and really made it a team effort and we put over a million hours of effort into this and we had very good reporting, so we knew application by application exactly where we were from an effort perspective. It took a lot of upfront time and effort by the agencies to put all this information together, but it proved to be very successful.

Because as you do, we have given all our agencies score cards as well, and I can tell you, the ones that were in the red, we had various meetings with them and their goal was to get out of the red very quickly and that proved to be very beneficial for us.

Mr. HORN. Well, I am glad to hear that. A number of Cabinet officers have told me in Washington that our report card has given them a good excuse to beat the bureaucracy to get the job done. So, they do not like the "F's" and "D's" and "C's," but it has worked out, some of them are now at the "B's" and the "A's," which was the whole aim of the thing.

Let me ask Mr. Buikema, what have you learned that you would like to have done differently?

Mr. BUIKEMA. I probably would echo what George Boersma just said, in terms of getting started earlier. I think the process that we are following getting information from the critical infrastructure, promoting awareness, developing guidance, that is a sound process, working closely with the Federal agencies, specifically FEMA on this issue, as well as with local agencies and State departments. But I wish we could have gotten started earlier like everybody else did.

But I think we are building on what exists for all hazards, as most States or all States are. There is an existing emergency management structure in the United States that has all hazard emergency operations plans that are flexible enough to respond to most hazards. The Y2K issue of course has some unique circumstances to it, which is why we are promoting contingency planning.

And in summary, I guess we could have gotten started a little bit earlier on that aspect.

Mr. HORN. Mr. Gulati, now that you have been through it, what would you have done first next time around?

Mr. GULATI. I guess if we had more time, that would have definitely helped. And also in an ongoing operation of anything, I think we need to take in account that when the programmers developed applications back in the 1960's, they only thought that they were developing for only the next 5 years. We need to look at it that yes, we are making something for a much longer period of time.

And another challenge we ran into is the inventory aspect, of what all do we have. I think the county adopting a mechanism so that on an ongoing basis we know what we have, so that if a need arises, to come up with a plan to address whatever, you have the necessary information there to be able to make the management decisions on that.

Mr. HORN. Well, thank you. Ms. Leavey, what would you do differently?

Ms. LEAVEY. I would definitely start earlier, for sure.

Mr. HORN. When did you start?

Ms. LEAVEY. We started in 1996, but really I do not think at the start, anybody had a sense of the volume of what we would have to do.

I think another thing that we would do is begin educating the public a lot earlier, getting our Websites up and running earlier.

Mr. HORN. Let me just go back down the line on the date when you started.

Mr. Gulati, when was that?

Mr. GULATI. We started back in 1996.

Mr. HORN. In 1996. And Captain, when did you start?

Mr. BUIKEMA. We really did not start on Y2K until last fall.

Mr. HORN. Well, you are about like the executive branch of the Federal Government on that one.

How about it, when did the State of Michigan start on this?

Mr. BOERSMA. We had new applications that we had installed in the early 1990's that we made sure they were Y2K compliant, but we really did not start in earnest on this until mid-1996.

Mr. HORN. Federal Government did not really in earnest start on this until April 1998, despite 2 years of prodding this subcommittee had given them. But they finally faced up to it.

Mr. Willemsen, what would you like to ask or comment after what you have heard?

Mr. WILLEMSSEN. Just a couple of points I would like to emphasize of what I heard from the other witnesses. One is that it is especially important from here on out that the organizations make sure that they do have independent verification and validation of their efforts. Another set of eyes to let top management of the organizations know that the testing and remediation has gone as expected. It is usually the case that some things have been overlooked or some things have been missed and therefore, an independent verification and validation agent can be especially useful in focusing on that.

And second, I think it is also very important for the organizations to look beyond the boundaries of their own organization. It is one thing to say that they are Y2K compliant, but unfortunately because of the high level of connectivity and the reliance on other organizations in our computerized world, they also need to make sure that they understand the compliance status of the other organizations they interact with. So that will be increasingly important over the next several months.

Thanks.

Mr. HORN. Thank you. I want to ask Commissioner Cushingberry if he has any questions he would like to ask the panel, since he, like Mr. Knollenberg and I, are down there at the grassroots and we get a lot of questions from a lot of people and they wonder how they are doing.

Mr. CUSHINGBERRY. Mr. Chairman, for the record, I serve as a member of the Information Tech Committee of the National Association of County Commissioners, so I am pleased to be here to testify on our behalf. We are meeting with the Allied Council in St. Louis, MO, where all the county commissioners across the country get together. We are pleased that your committee has had such leadership. We are participating as part of the Information Task Force through the National Association of County Commissioners. My distinguished colleague, Commissioner Cavanaugh of the east side of Detroit, is also on what is known as the Research Technology Committee and we are trying to work with the major universities across the country to see to it that we get the better theoretical methodologies included in our future plans.

[Inaudible comments.]

Mr. HORN. Well, thank you. If I had to sit here making decisions every week, I would day dream and just look at the architecture. So how do you focus around here with this type of beauty. Thank you again.

Mr. Knollenberg, any further questions?

Mr. KNOLLENBERG. I am satisfied, Mr. Chairman, thank you.

Mr. HORN. Mr. Willemsen and I are on the same track, because I was going to get on verification and I think he is very right. Sometimes we have internal verification but sometimes you need external verification.

So we thank this panel.

We did not have any questions from the audience that the staff picked up. But hopefully there are other things, as we go ahead

this morning, feel free to write the questions and we will put it to the panel.

But thank you very much, those on panel one, you have given us some good testimony and we appreciate it.

So panel two will come forward. We have Mr. Surdu, Mr. Costantino, Mr. Buck, Mr. Parker.

Gentlemen, if you would stand and we will administer the oath. [Witnesses sworn.]

Mr. HORN. The clerk will note all four witnesses took the oath. And we will begin with George Surdu, the director of technical services organization of the Ford Motor Co. We are delighted to have all of you automobile people here. It is key to the country. Please proceed. And as you heard earlier, if you could summarize the testimony in 5 minutes or so, that gives us more time for interaction because we do have your fine statements.

STATEMENTS OF GEORGE SURDU, DIRECTOR, TECHNICAL SERVICES ORGANIZATION, FORD MOTOR CO.; DON COSTANTINO, DIRECTOR, CORPORATE YEAR 2000 PROGRAM, GENERAL MOTORS CORP.; ROGER BUCK, DAIMLER-CHRYSLER CORP.; AND JOHN PARKER, VICE PRESIDENT, INFORMATION SERVICES, NORTHWEST AIRLINES, INC.

Mr. SURDU. I would first like to thank the subcommittee for affording Ford Motor Co. the opportunity to provide an update on the year 2000 program. As you just mentioned, I am the director of technical services and the global year 2000 program manager for Ford Motor Co. I have been in that position since the inception of our program in 1996.

In 1996, Ford Motor Co. initiated a formal program to address this year 2000 challenge. We established a senior level steering committee that has been headed up by our chief financial officer, our vice president of quality and process leadership and our chief information officer. A global year 2000 program office was created and a robust program management process was put in place to guide compliance actions across all the potential impact areas.

I believe we did a very innovative thing within Ford Motor Co. in that we really sliced the business across technology lines. So we began taking a look at all the major impact areas, which include business computer systems. Ford Motor Co. has about 300 million lines of code, about 2,700 systems, and about a third of those have been deemed mission critical.

In addition, we have looked at our technical infrastructure, our plant floor equipment, our product development test equipment, our suppliers, dealers and affiliates, end-user computing which includes all of the spreadsheets and the access databases, those kinds of things that our business partners create on a year-to-year basis to support the business, our building infrastructure, and of course, our vehicle components.

In addition, we have continued to monitor the compliance actions of other impact areas as we move forward on the programs, such as our transportation carriers, our medical equipment suppliers and in fact customs offices around the globe.

The sophistication of this program has been recognized by the Information Technology Association of America, with certification

that Ford's program meets the challenging Y2K best practices standards.

We established stretch objectives back in 1996 across all of these major impact areas, and to have all of those impact areas compliant by the middle of this year. We are going to be fundamentally there in all those areas, we are going to use the summer shutdown period to complete some of the remediation work, but I would like to give you some data to give you a sense of where we are at across the program.

As of this report, 98 percent of all of our critical systems are compliant, 97 percent of all systems are compliant, that is all 2,700 systems. They have been remediated, tested and are now back in service.

In addition, an enterprise test plan has been established for all of our key business processes, with completion of that enterprise testing by September.

On the plant floor side, for the 167 plants and warehouse facilities around the globe, we presently have 99 percent of all the equipment has been remediated. We have got a handful of equipment that we are waiting again until the shutdown period to make sure that all of that is working properly.

In conjunction with the Automotive Industry Action Group, and I think you will hear from my team mates here today a little bit more about that, we have been involved with the AIAG, the Automotive Industry Action Group, and other organizations similar to that around the globe, the VDA in Europe, as an example. We have been participating in a global supplier readiness program for our production and what we call our non-production suppliers and that includes our utilities, of course some of the folks that have already provided feedback this morning.

As of this report, 80 percent of these suppliers are responding that they are ready. That is as of June, with 100 percent to be ready by the end of the year. About 10 percent of our suppliers have not responded and we have additional actions underway to validate the status of these suppliers and any suppliers that are not anticipating being ready by September.

We have a very similar program that we have put in place for our affiliates and today 89 percent are ready, with 100 percent ready by the end of the year.

Compliance in some of the other impact areas that I would mention very quickly, 86 percent of all of our critical product development test equipment are compliant and back in service; 93 percent of all of our end-user using technology is compliant; 95 percent of all of our technical infrastructure is compliant; 83 percent of our end dealership systems and 93 percent of all of our physical properties and infrastructures. And finally, 100 percent of all of our vehicle components are compliant and have continued to be compliant since we began evaluating that back in 1996.

As previously stated in our most recent SEC filing, Ford is anticipating spending about \$375 million to complete the program. When it actually formally commenced, we absorbed our funding initially within our own process leadership organization when we kicked this program off, but this \$375 million began about mid-1997 and

is going to carry us through about the middle of 2000. This outlay accounts for about 10 percent of our total infrastructure costs.

We are very, very confident in our readiness as well as that of our affiliates, dealers and suppliers. However, the inter-dependence of the entire supply chain—and you heard a little bit about that this morning—does represent the greatest risk to Ford. In particular, an extended infrastructure failure; that is, electric, gas or water, would make it difficult for us to operate our manufacturing operations. Accordingly, during the fourth quarter of last year, we began to develop contingency plans. Most of those plans are now complete, we are going to validate those plans by September. In addition, we have created what we have called a global response center, we actually launched that July 1st, and that center is collecting information and will act as an information clearinghouse for the most current status available as we enter the new millennium.

Finally, I should mention that we have notified a small number of our employees that we intend to have onsite or on call over the holiday period, to coordinate any unexpected glitches that may be experienced.

Finally, and it was mentioned again earlier, we have engaged an outside organization to do independent verification and validation. Even though all of our critical systems were compliant, those—a third of the inventory that I mentioned were all compliant by the end of last year. We have been doing enterprise testing and now we have an independent organization that is reviewing all of those critical systems to make sure that we have not missed anything.

So with that, that is a summary of my prepared statement and I would be happy to answer any questions when the time comes.

Mr. HORN. Well, thank you, that is very helpful information.

Next is Don Costantino, director of corporate year 2000 program for the General Motors Corp.

[The prepared statement of Mr. Surdu follows:]

Ford Motor Company
Prepared Year 2000 Statement to the
Subcommittee on Government Management, Information, and Technology
July 9, 1999

Good morning. I first would like to thank the Subcommittee for affording Ford Motor Company the opportunity to provide an update on our Year 2000 Program. My name is George Surdu, and I am the Director of Technical Services, and Ford Motor Company's Year 2000 Global Program Manager. I have been the Year 2000 Global Program Manager since the inception of the Company's formal program in 1996.

In 1996, Ford Motor Company initiated a formal program to address the Year 2000 challenge. A senior level steering committee was established, co-sponsored by our Chief Financial Officer, our vice President of Quality and Process Leadership and our Chief Information Officer. A global Year 2000 Central Program Office was created under my leadership, and a robust program management process was created to guide compliance actions across all potential impact areas. Areas identified include: Business Computer Systems; Technical Infrastructure; Plantfloor Equipment; Product Development Test Equipment; Suppliers, Dealers and Affiliates; End-User Computing; Building Infrastructure; and Vehicle Components. In addition, we have continued to monitor the compliance actions of other impact areas such as our transportation carriers, medical equipment suppliers and customs offices. The sophistication of Ford's Y2K program was recognized by the Information Technology Association of America with a certification that Ford's program meets its challenging Y2K "best practices" standards.

Stretch compliance objectives were established for all impact areas, with the majority of work to be completed by mid-year 1999. Summer shut-down periods are being used to complete remediation work. As of this report, 98% of critical business systems and 97% of all business

systems have been remediated, tested and back in service. In addition, an enterprise test plan for all key business processes has been developed, with completion scheduled for September.

For plant floor equipment, Ford has implemented a process to assess equipment and machinery in its 167 manufacturing and assembly plants and parts warehouse facilities. Presently, 99% of all plant floor equipment is compliant.

In conjunction with the Automotive Industry Action Group in North America, and other industry trade associations such as the VDA in Europe, Ford has been participating in a global supplier readiness program for production and critical non-production suppliers. As of this report, about 80% of suppliers responding are deemed ready, with 100% to be ready by year-end. About 10% have not responded; additional actions are underway to validate status of these suppliers and others that do not anticipate readiness by September. A similar program has been established for Ford's affiliates. To date, 89% are ready, with 100% slated to be ready by December 1999.

Compliance to date for the other impact areas include: 86% of all critical Product Development Test Equipment; 93% of End-user Computing; 95% of our Technical Infrastructure; 83% of in-dealership systems; and 93% of all physical properties and infrastructures. Finally, 100% of the components in our vehicles are compliant.

As previously stated in our most recent SEC filing, Ford estimates its total Y2K spending to be about \$375 million, incurred over a three-year period that commenced mid-1997 and will end mid-2000. This outlay constitutes about 10% of our total annual information technology budget.

Ford Motor Company is confident as to its readiness, as well as that of its affiliates, dealers and suppliers. However, the interdependence of the entire supply chain does represent the greatest risk

to Ford. In particular, an extended infrastructure failure, that is electric, gas and water, would make it difficult to operate manufacturing operations. Accordingly, during the fourth quarter of 1998, we began the development of business contingency plans for all of our critical business processes. Most of these plans are now complete. Validation of all contingency plans will be completed in September. In addition, Ford has created a Global Y2K Response Center to be used as an information clearinghouse for the most current status available as we enter the new millennium. Finally, a number of employees are being notified now to serve as on-site or on-call support over the holiday period to coordinate a response to any unexpected glitches that may be experienced by Ford or those who rely on Ford's consumer products and services.

This concludes my prepared statement. I would again like to thank the sub-committee for this time to provide an update on Ford's Year 2000 Program. I would now be happy to respond to any questions you may have.

Mr. COSTANTINO. Good morning, Congressman Knollenberg and Representative Horn.

Mr. HORN. Thank you for being here.

Mr. COSTANTINO. I am happy to be here today to represent General Motors.

We too have a very formal program inside of General Motors. It is headed up by our vice president and chief information officer. We report directly to both the Board of Directors and our Automotive Strategy Board, which is our lead group, on a regular basis.

Getting into some of the specifics of our program, we have approximately 6,100 application type systems—things like financial systems, scheduling systems, et cetera—comprising probably a billion and a half lines of code. At the present time, we are well over 99 percent complete, we have less than a handful of those left to be done. They have all been inventoried, they have all been assessed, they have all been remediated and put back into service.

From the systems and component area where we talk about the plant floors, we talk about engineering work stations, computers, et cetera, we have over 1.4 million of these devices which we had to inventory and assess. We are currently in a position now of well over 99 percent of those complete and they will be finalized during the month of August during the plant shutdown period. So we will be basically complete with the remediation and testing of all of our applications and infrastructure globally.

We have moved into a very serious readiness testing phase. This is a phase in which we basically test all of our systems, either singularly or connected, since most of our functions connect, of course, across different departments. These are done in a setting of a future clock, with future data, so that basically they are all being tested, in an environment that duplicates the year 2000. We are probably going to run about 3,000 of these tests either individually or in conjunction with other systems in an integrated fashion. At this point in time, we are probably about 90 percent complete with that testing.

We have also put in place what we call a live production test in all of our assembly and manufacturing plants. We have run over 100 of these so far, and this is actually building cars or parts in the plant with future clock, future data. So we have basically put our assembly plants into the year 2000, run the product and then turn the clock back to bring it back into the current timeframe.

As with, I am sure, everybody else on this panel, we are also doing independent verification of our systems with an outside firm. Although in our case, we also use EDS obviously that did most of the remediation of our applications work.

From a supplier standpoint, this has always been a very critical area of our program. We obviously participated with the Automotive Industry Action Group [AIAG], in the self-assessment survey but we went I think quite a bit farther than that. We have had teams in place globally for at least the last 2½ years. We have done onsite visits with trained assessors at over 3,500 suppliers. We have held workshops across the globe that have brought in another 3,000 suppliers and basically feel at this point in time we have an excellent understanding of our supplier base and it's readiness. We have narrowed this down now to several hundred sup-

pliers that we believe still need some additional attention, which is less than 10 percent of our supply base. And we are in the process now of further evaluating them to determine what type of contingency plans we will have to put in place if in fact they are unable to be ready for the year 2000.

In conjunction with that, we have also looked at logistic suppliers worldwide, and obviously we are looking at both indirect and direct. We have also just in the last 3 months spent a great deal of time internationally looking at the infrastructure in various countries focusing on utilities. We are fairly satisfied that the United States is in pretty good shape, but since we have operations worldwide and suppliers worldwide, in order for us to better understand what type of contingency plan we would have to develop, we needed an understanding of the overseas utilities environment and that is basically now complete and we are now applying that against our supplier base to determine what type of contingency plan we will have to put in place.

Contingency planning, as mentioned by George, is ongoing now in all areas and will be complete and basically be in the test phase starting in September; although in most cases, the contingency planning is actually a reflection of our normal planning that we would have for any type of a disaster recovery.

Command centers are being put in place, one in Detroit and the rest of them globally. They will be integrated throughout the month of December and January to assure that we can respond properly to any issues if we do have them, although at this time we do not anticipate anything of a real material impact, but probably more like a minor shutdown. We have informed, as George has at Ford, our employees, a number of them that they will not get vacation, they will be working and the EDS organization has put all people on notice throughout their company, from the month beginning the middle of December through the middle of January, so we will have our technical resources in place if we need them.

Finally, from an expenditure standpoint, GM, is at the current time estimating that we will spend about \$540 to \$600 million. About \$190 million of that will go to EDS, our primary supplier of services.

Thank you.

Mr. HORN. Well, thank you, we appreciate the testimony.

Next is Roger Buck of the DaimlerChrysler Corp.

[The prepared statement of Mr. Costantino follows:]

GENERAL MOTORS YEAR 2000 STATEMENT

Subcommittee on Government Management Information Technology
July 9, 1999

YEAR 2000 READINESS DISCLOSURE**Executive Summary**

GM anticipates no problems with past, current, or future model vehicles, and no significant disruption of GM's business as a result of the Year 2000 problem.

GM's passenger vehicles, with their growing use of sophisticated electronics, were among the company's earliest priorities for analysis of potential Y2K-related problems. GM vehicles have long been equipped with microprocessors which today, depending on the vehicle, are used for powertrain management, automatic climate control, anti-lock braking systems, traction control, stability enhancement, driver information centers, supplemental inflatable restraint systems, head-up display, real-time damping, navigation systems, seat, steering column and mirror memory positioning, remote keyless entry, entertainment systems, interior and exterior lighting systems, entry control, cellular communications and anti-theft systems.

GM has analyzed the microprocessors in its current and planned models. Additionally, the company has checked the microprocessors in past models dating back to when we first started installing "date processing-capable" microchips in our cars and trucks. GM found most of these electronic systems have no date-related functionality and, therefore, pose no Year 2000-related problems. Those few systems that have date-related functionality were found to be Year 2000 ready.

GM is executing a comprehensive plan to make GM Y2K ready. Details and milestones of the plan include the following:

- The plan's major process steps include inventory, assessment, remediation, system testing, implementation, readiness testing, and contingency planning.
- GM is working to maintain uninterrupted electronic communications with its dealers, suppliers and other companies with whom it does business.
- Comprehensive Supplier Y2K Readiness is a vital part of the program.
- Remediation of systems is substantially completed.
- Testing will occur throughout 1999 to confirm GM's year 2000 readiness.
- Contingency plans are being identified and put in place

YEAR 2000 READINESS DISCLOSURE

GM's Year 2000 Program

Many computerized systems and microprocessors that are embedded in a variety of products either made or used by GM have the potential for operational problems if they lack the ability to handle the transition to the Year 2000. Because this issue has the potential to cause disruption of GM's business operations, GM has developed a comprehensive worldwide program to identify and remediate potential Year 2000 problems in its business information systems and other systems embedded in its engineering and manufacturing operations. Additionally, GM has initiated communications and site assessments with its suppliers, its dealers and other third parties in order to assess and reduce the risk that GM's operations could be adversely affected by the failure of these third parties to adequately address the Year 2000 issue.

One of GM's first priorities was the analysis of microprocessors used in GM passenger cars and trucks. This review included all current and planned models as well as the electronics in older cars and trucks produced during the period of approximately the last 15 years. GM began installing microchips capable of processing date information approximately 15 years ago. Most of the processors reviewed have no date-related functionality, and accordingly have no Year 2000 issues. Of the vehicles with processors that perform date-related functions, none have any Year 2000 issues.

GM's Year 2000 program teams are responsible for remediating all of GM's information technology and embedded systems. Information technology principally consists of business information systems (such as mainframe and other shared computers and associated business application software) and infrastructure (such as personal computers, operating systems, networks and devices like switches and routers). Embedded systems include microprocessors used in factory automation and in systems such as elevators, security and facility management. GM's Year 2000 program includes assessment and remediation services provided by Electronic Data Systems Corporation (EDS) pursuant to a Master Service Agreement with GM.

The Year 2000 program is being implemented in seven phases, some of which were and are being conducted concurrently:

Inventory -- identification and validation of an inventory of all systems that could be affected by the Year 2000 issue. The inventory phase commenced in earnest in 1996 and is substantially complete. GM has identified approximately 6,100 business information systems and about 1.4 million infrastructure items and embedded systems.

Assessment -- initial testing, code scanning, and supplier contacts to determine whether remediation is needed and developing a remediation plan, if applicable. The assessment of business information systems is substantially complete and included a determination that about one quarter of such systems should be regarded as "critical" based on criteria such as the potential for business disruption. The assessment of infrastructure items and embedded systems was substantially completed by the end of 1998.

YEAR 2000 READINESS DISCLOSURE

Page 2

Remediation -- design and execution of a remediation plan, followed by testing for adherence to the design. GM has substantially completed the remediation of its critical and non-critical systems. A small number of systems will be remediated or replaced in 1999. Inconsequential systems have been and will continue to be removed from GM's Year 2000 inventory and will not be remediated. GM believes that it will meet its targets for Year 2000 readiness.

System Test -- testing of remediated items to ensure that they function normally after being replaced in their original operating environment. This phase is closely related to the remediation phase and follows essentially the same schedule.

Implementation -- return of items to normal operation after satisfactory performance in system testing. This phase follows essentially the same schedule as remediation and system testing.

Readiness Testing -- planning for and testing of integrated systems in a Year 2000 ready environment, including ongoing auditing and follow-up. Readiness testing is currently under way. This phase commenced during the fourth quarter of 1998 and is expected to be the major focus of the Year 2000 program throughout 1999.

Contingency Planning -- development and execution of plans that narrow the focus on specific areas of significant concern and concentrate resources to address them. GM currently believes that the most reasonably likely worst case scenario is that there will be some localized disruptions of systems that will affect individual business processes, facilities or suppliers for a short time rather than systemic or long-term problems affecting its business operations as a whole. GM contingency planning continues to identify systems or other aspects of GM's business or that of its suppliers that it believes would be most likely to experience Year 2000 problems. GM contingency planning also addresses those business operations in which a localized disruption could have the potential for causing a wider problem by interrupting the flow of products, materials or data to other operations. Because there is uncertainty as to which activities may be affected and the exact nature of the problems that may arise, GM's contingency planning will focus on minimizing the scope and duration of any disruptions by having sufficient personnel, inventory and other resources in place to permit a flexible, real-time response to specific problems as they may arise at individual locations around the world. Some of the actions that GM may consider include the deployment of emergency response teams on a regional or local basis and the development of plans for the allocation, stockpiling or resourcing of components and materials that may be critical to our continued production. Specific contingency plans and resources for permitting the necessary flexibility of response are expected to be identified and put into place commencing in mid-1999.

YEAR 2000 READINESS DISCLOSURE

Page 3

GM's communication with its suppliers is a focused element of the assessment and remediation phases described above. GM is a leading participant in an industry trade association, the Automotive Industry Action Group, which has distributed Year 2000 compliance questionnaires as well as numerous awareness and assistance mailings to about half of the 90,000 supplier sites that service GM throughout the world. Responses to these questionnaires, which were generally sent to GM's principal suppliers, have been received from about half of the supplier sites to which they were sent. Many of the non-responding suppliers are communicating directly with GM on an informal basis. Additionally, GM has initiated its own review of suppliers considered to be critical to GM's operations, including more than 3,000 on-site assessments to date. These assessment efforts have been substantially completed with respect to the critical supplier sites. Based on its assessment activity to date, GM believes that a substantial majority of its suppliers are making acceptable progress toward Year 2000-readiness. GM has established a program to provide further assistance to suppliers that desire more input or that are believed to be at high risk of noncompliance as a result of the foregoing assessment efforts. This supplier assistance program currently includes providing compliance workshops and remediation consultants to work with suppliers on developing and implementing their own remediation programs. GM's contingency planning efforts described above are also expected to address any critical suppliers that GM identifies as being at high risk of encountering Year 2000 problems.

GM is not relying entirely on the receipt of written assurances from suppliers with respect to their Year 2000 compliance. GM is also evaluating certain suppliers on a first-hand basis and seeking to enhance their likelihood of full Year 2000 readiness by actively assisting them with training and consultation regarding Year 2000 remediation projects. GM expects that information from our suppliers, written responses and interactions with them, will provide GM with a basis for further contingency planning and risk management.

GM also has a program to work with its independent dealers on their Year 2000 readiness. This program includes distributing materials that assist dealers in designing and executing their own assessment and remediation efforts. GM has also included Year 2000 compliance criteria as part of its established program for certifying that third-party business information systems properly interface with other systems provided to dealers by GM.

GM's direct Year 2000 program cost is being expensed as incurred with the exception of capitalizable replacement hardware and, beginning in 1999, internal-use software. Total incremental spending by GM is not expected to be material to the Corporation's operations, liquidity or capital resources.

YEAR 2000 READINESS DISCLOSURE

Page 4

In addition to the work for which GM has direct financial responsibility, EDS is providing Year 2000-related services to GM, as required under a Master Service Agreement. These services are being provided by EDS as part of normal fixed price services and other on-going payments to EDS.

GM's current forecast is that its total direct expenditures plus the value of services performed by EDS attributable to GM's Year 2000 program will be between \$540 million and \$600 million. This amount includes the following:

- An estimated \$350 million to \$410 million in direct GM expenditures. This estimate includes a \$60 million payment from GM to EDS at the end of the first quarter of 2000 if systems remediated by EDS do not cause a significant business disruption that results in material financial loss to GM; and
- An estimated \$190 million representing EDS' expenditures attributable to GM Year 2000 program.

Despite the incremental Year 2000 spending expected to be incurred throughout the Corporation, GM's current business plan projects continued declining information technology expenses. GM's total Year 2000 costs noted above do not include information technology projects that have been accelerated due to Year 2000, which are estimated to be approximately \$20 million.

In view of the foregoing, GM does not currently anticipate that it will experience a significant disruption of its business as a result of the Year 2000 issue. However, there is still uncertainty about the broader scope of the Year 2000 issue as it may affect GM and third parties that are critical to GM's operations. For example, lack of readiness by electrical and water utilities, financial institutions, government agencies or other providers of general infrastructure could, in some geographic areas, pose significant impediments to GM's ability to carry on its normal operations in the area or areas so affected.

Statements made herein about the implementation of various phases of GM's Year 2000 program, the costs expected to be associated with that program and the results that GM expects to achieve constitute forward-looking information. As noted above, there are many uncertainties involved in the Year 2000 issue, including the extent to which GM will be able to successfully remediate systems and adequately provide for contingencies that may arise, as well as the broader scope of the Year 2000 issue as it may affect third parties that are not controlled by GM. Accordingly, the costs and results of GM's Year 2000 program and the extent of any impact on GM's operations could vary materially from those stated herein.

YEAR 2000 READINESS DISCLOSURE

Page 5

Note: The expenditures and other figures contained in this document represent GM's latest estimates following the May, 1999, spin-off of Delphi Automotive. Additional information of GM's Y2K readiness is available at (www.gm.com) and (www.gmacfs.com).

YEAR 2000 READINESS DISCLOSURE

Mr. BUCK. Thank you, Representative Horn and Knollenberg for asking me to be here today. Before I begin, I need to cover a topic on this non-receipt of Federal funds. We are filling it out currently and will have it to your office shortly.

We take this issue at DaimlerChrysler of Y2K very seriously. We have project teams in both Stuttgart and Auburn Hills and we are coordinating our efforts. These efforts began, of course, when we were separate companies, Daimler-Benz and Chrysler.

Each team is responsible for developing a comprehensive compliance program to assess potential problems within DaimlerChrysler and its key suppliers, implement and verify remediation action and devise contingency plans. Each team has allocated resources based on our internal assessments to address the issue, and the potential impact to our company, both its operations and financial conditions.

The teams both report to the Board of Management of DaimlerChrysler AG which is our parent company.

We believe we will achieve our goal of substantially completing Y2K remediation at our facilities around the globe by September 30th of this year. This includes addressing the problems of Y2K with our business computer systems, our shop floor devices, our sales and service activities and PCs for each of our business units. Critical business computer systems were 99 percent remediated at the end of 1998. This has allowed us to perform additional integration testing using CPUs rolled forward into the year 2000. The upgrading of critical shop floor equipment will be completed this summer with our shutdown period. There are several items that needed 1 to 2 weeks to actually fix. We cannot find a single failure in any of our vehicles when the clock rolls over to January 2000.

In addition, the European Airbus consortium has issued a report indicating that date sensitive embedded chips in Airbus products will not be materially adversely affected by the Y2K problem. Our automotive dealer's business systems in all the major markets are Y2K ready. Even our employees are wrapping up their efforts to make sure their desktop PCs are ready for Y2K.

DaimlerChrysler's largest Y2K business risk continues to be our suppliers. We participate in some automotive industry trade associations, both in North America and globally, the AIAG here in North America and the VDA in Europe. Each group has developed a common approach to the compliance along with its members, which includes seminars for first, second, third tier suppliers and confirming compliance through either questionnaires or reviews. We have sent questionnaires and done reviews and about 85 percent of our suppliers have said they will complete their remediation by June 30th of this year. We also offer remediation assistance to suppliers who we believe have not made adequate progress and we are also reviewing suppliers on a selective basis for compliance. We are now asking each of our key suppliers to provide a statement of readiness to confirm that they have achieved their expected compliance. Suppliers that are not compliant by September 30 will be reviewed, and if appropriate, asked to establish contingency plans to ensure an uninterrupted supply of parts for DaimlerChrysler.

As part of DaimlerChrysler's Y2K efforts, each of its sites is required to prepare a Y2K rollover plan. This rollover plan will as-

sess the readiness of key infrastructure items, including process equipment, business computer system availability, building facility readiness which includes such things as electricity, gas, water, sewage, heat, fire alarms, emergency services, securities and phones, and community readiness—police, fire, emergency management services, hospitals, et cetera. Each site will report their status to a central location on Saturday, January 1st and Sunday, January 2nd.

We do not have a crystal ball to tell us where the world might have missed Y2K problems. Disruptions to basic critical infrastructures like electricity, gas, water, sewer, telephones, et cetera will make it virtually impossible to operate plants. We believe, however, DaimlerChrysler has taken every possible step to ensure that internal Y2K problems have been eliminated in all material respects and external risks have been significantly reduced. We fully expect all DaimlerChrysler facilities to operate normally on Monday, January 3, 2000.

I will be available for questions.

Mr. HORN. Thank you very much. After Mr. Parker, we will.

John Parker is the vice president, information services, Northwest Airlines. I take it we should all fly Northwest now since you have the highest paid flight attendants in the United States and the world. [Laughter.]

Congratulations. You are one of my favorite airlines.

[The prepared statement of Mr. Buck follows:]

DAIMLERCHRYSLER YEAR2000 PREPAREDNESS

United States House of Representatives

Subcommittee on Government Management, Information, and Technology

Detroit, Michigan, July 9, 1999

DaimlerChrysler takes the Y2K issue very seriously. DaimlerChrysler's Y2K Project Teams in Stuttgart and Auburn Hills are coordinating the compliance efforts initiated by Daimler-Benz and Chrysler before their business combination. The Y2K Project Teams are responsible for developing a comprehensive compliance program to assess potential problems within DaimlerChrysler and its key suppliers, implement and verify remedial action, and devise contingency plans. The Teams have allocated resources to address Y2K compliance issues based on internal assessments of the potential impact of non-compliance on DaimlerChrysler's operations and financial condition. The Teams report to the Board of Management of DaimlerChrysler AG.

We believe we will achieve our goal of substantially completing Y2K remediation at our facilities around the globe by September 30, 1999. This includes addressing Y2K problems with Business Computer Systems, Shop Floor Devices, Sales / Service Activities, and PCs for each DaimlerChrysler Business Unit. Critical Business Computer Systems were 99% remediated at the end of 1998. This has allowed for additional integration testing using CPU dates in the year 2000. The upgrading of Critical Shop Floor Equipment will be completed this summer. We cannot find a single Y2K failure that will occur in our vehicles when the clock rolls over to January 1, 2000. In addition, the European Airbus consortium, Airbus Industrie G.I.E., has issued a report indicating that date-sensitive embedded systems in Airbus Industrie products will not be materially adversely affected by the Y2K problem. Automotive Dealer's Business Systems in all major markets are Y2K ready. Even DaimlerChrysler employees are wrapping up their efforts to make sure their desktop PCs are ready for Y2K. DaimlerChrysler's largest Y2K business risk continues to be with Suppliers.

DaimlerChrysler participates in automotive industry trade associations in both North America and Germany (the Automotive Industry Action Group and the *Verband der Automobilindustrie*). Each group has developed a common approach to Y2K compliance among its members, which includes offering Y2K seminars to first, second, and third tier production and non-production suppliers, and confirming their Y2K compliance status through

questionnaires and on site auditing. Questionnaires have been sent to those suppliers and a majority have responded. About 85% of our suppliers have said they would be completed with Y2K remediation by June 30, 1999. DaimlerChrysler offers a Y2K Remediation Assistance Program to suppliers without adequate compliance programs, and is reviewing key suppliers on a selective basis for compliance. DaimlerChrysler has asked each key supplier to provide a Y2K Statement of Readiness to confirm that they have achieved their expected Y2K compliance. Suppliers that will not be Y2K compliant by September 30, 1999 will be reviewed and if appropriate, asked to establish contingency plans to insure an uninterrupted supply of parts to DaimlerChrysler.

As part of DaimlerChrysler's Y2K compliant efforts, each of its sites is required to prepare a Y2K Rollover Plan. This Y2K Rollover Plan will assess the readiness of key infrastructure items including Process Equipment, Business Computer System availability, Building Facility readiness (electricity, gas, water, sewage, heat, fire alarms, emergency services, security, phones, etc.), and community readiness (police, fire, EMS, hospitals, etc.). Each site will report their status to a central location on Saturday, January 1st and Sunday, January 2nd, 2000

We do not have a crystal ball that will tell us where the world might have missed Y2K problems. Disruptions to basic critical infrastructures like electricity, gas, water, sewage, telephones, etc. would make it virtually impossible to operate plants. We believe, however, DaimlerChrysler has taken every possible step to insure that internal Y2K problems have been eliminated in all material respects and external risks have been significantly reduced. We fully expect, all DaimlerChrysler to operate normally on Monday, January 3, 2000.

Mr. PARKER. Thank you for inviting me to appear before this committee to give you an update on Northwest Airlines' Y2K readiness. I would like to begin by assuring the committee that Northwest Airlines expects to offer its passenger and cargo customers a full, regular and normal schedule of services as we begin the new century. As always, we will make any adjustments necessary to ensure the safety and integrity of our operations and the convenience and comfort of our passengers. Ensuring safe operations is the No. 1 priority of our airline and the basis on which we have built our Y2K program.

Northwest recognizes the importance and magnitude of making the necessary changes required for operating successfully in the 21st century and is working both internally and with external entities worldwide to ensure a smooth transition to the Y2K.

I will give you a brief overview of how we at Northwest have approached the Y2K challenge, our collaboration within the airline industry, the current status of our program and what we expect to do for the remainder of 1999.

Northwest's effort on the Y2K transition program began in January 1996. We currently employ a full time staff of 26 who are dedicated to leading more than 200 Northwest people on Y2K related activities. Our estimated costs for Y2K related activities is somewhere between \$45 and \$55 million and we have currently spent over \$30 million to date.

Our objectives are clearly defined and focused to ensure that Northwest's computers and computer-related systems will function properly on January 1, 2000 and beyond; to assess the Y2K compliance of the external organizations on which we rely; to develop workable contingency plans which will enable Northwest to maintain safe, reliable air transport of passengers and cargo.

To effectively address the Y2K issues, Northwest adopted the methodology prescribed by the General Accounting Office's Guide on the Y2K Computing Crisis. The phases that we followed were awareness, assessment, renovation, validation and implementation, as outlined in this document and it has served us very well in dealing with the complex and interdependent nature of the problem in the airline industry. In a similar way, we followed the GAO's Business Continuity and Contingency Planning guidelines which were published last year. Additionally, we have an assessment and evaluation of all supporting documentation and compliance to these guidelines that is subject to independent verification by the Northwest Audit and Security Department.

Within this context, we have identified 531 internal systems which are approximately half of all of our systems, which required conversion or replacement to be Y2K compliant. In addition, all of our business areas were tasked with identifying and assessing their critical components and suppliers for Y2K compliance; again, which followed the guidelines.

Assessment of domestic and international airport and air traffic control systems readiness has been undertaken with a cooperatively and jointly funded effort with the Air Transport Association and the International Air Transport Association, and other trade groups. Member airlines, in addition to their own Y2K programs

have invested \$44.5 million in the Y2K programs of these associations.

Northwest has worked closely with Boeing and Airbus to assess and test our fleet of more than 400 aircraft and our fleet of 20 flight simulators which must be identical to our actual aircraft to be suitable for training and certification of pilots.

To assess the readiness of the worldwide infrastructure systems, Northwest initiated a collaboration with the Gartner Group that is being used by many airlines.

And finally, we have established a cross department steering committee which was charged with identifying and developing contingency plans for processes considered essential for maintaining the airlines' normal operations and where the potential for failure is high.

At present, Northwest has completed approximately 98 percent of its application remediation and completed testing of more than 90 percent of our high priority applications. The remaining renovation and testing is on target to be completed within the third quarter of 1999.

Minor modifications have also been made to bring Northwest's aircraft fleet into Y2K compliance. It is important to note that no Y2K safety of flight issues have ever been documented within Northwest's aircraft fleet.

Northwest's reservation systems were successfully renovated and capable of booking and selling tickets through all of our distribution channels, including our Internet site. Since February 4 of 1999, and to date we have—more than 75 of Northwest's major internal systems have successfully passed their initial failure dates.

I would also like to highlight two industry reports that give a snapshot of the industry. The ATA reported to the President's Council on Year 2000 Conversion on July 1, 1999, that United States and Canadian airlines are 95 percent finished with their Y2K remediation efforts. The Nation's airports are on schedule with their own Y2K efforts and the FAA has met its June 30, 1999 completion date for Y2K remediation. And that final independent verification by outside contractors and government agencies is pending.

An additional status report was presented to the International Civil Aviation Organization, ICAO, to the United Nations National Y2K Coordinators Meeting on June 23rd. It reports substantial progress in all critical areas of air transport and in the development of contingency plans for all contracting States of ICAO.

Mr. Chairman, what I have been discussing to this point has shown how Northwest Airlines and the aviation industry are addressing Y2K readiness. For the remainder of 1999, Northwest will shift its primary focus into what we are calling transition management. This consists of executing contingency plans as necessary, developing alternative flight schedule scenarios as required and dealing with events as they actually occur through the transition.

As the year progresses and more information becomes available on the status and readiness of our destinations, Northwest will make and announce changes to our flight schedule. And you can rest assured, Mr. Chairman, that should any adjustments to North-

west's schedules be deemed necessary, those changes will be promptly communicated to the traveling public.

Northwest will continue to be actively engaged with industry activities to complete remediation and to reassure the public that they can plan to travel during the transition period with full confidence and that the same standards for safety, which have been the hallmark of the airline industry, have been rigorously applied to our Y2K remediation work.

In conclusion, I want to again assure you and the committee that Northwest Airlines is on track with its Y2K program, that we are working closely with our industry associations to complete readiness and contingency planning activities and that we expect to have normal operations at the start of year 2000.

I will be glad to take any questions.

[The prepared statement of Mr. Parker follows:]



**NORTHWEST
AIRLINES**

Department Number

Northwest Airlines, Inc.
5101 Northwest Drive
St. Paul MN 55111-3034

**Statement by
JOHN C. PARKER
VICE PRESIDENT INFORMATION SERVICES
NORTHWEST AIRLINES**

before the
**SUBCOMMITTEE ON GOVERNMENT
MANAGEMENT,
INFORMATION AND TECHNOLOGY**

of the
**COMMITTEE ON
GOVERNMENT REFORM AND OVERSIGHT**

U.S. HOUSE OF REPRESENTATIVES

July 9, 1999

Mr. Chairman, thank you for inviting me to appear before this hearing to give you an update on Northwest Airlines' Y2k readiness. I'd like to begin by assuring the committee that Northwest Airlines expects to offer its passenger and cargo customers a full, regular and normal schedule of services as we begin the new century. As always, of course, we will make adjustments as necessary to ensure the safety and integrity of our operations and the convenience and comfort of our passengers. Ensuring safe operations is the number one priority at our airline and it is the basis on which we have built our Y2k program.

Northwest Airlines recognizes the importance and magnitude of making the necessary changes required for operating successfully in the 21st century. Northwest is working both internally and with external entities worldwide to ensure a smooth transition to Y2K compliant systems by the year 2000.

I'll give you a brief overview of how we at Northwest have approached the Y2k challenge, our collaborative effort within the industry, the current status of our Y2k program, and what we expect to do during the remainder of 1999.

Northwest's Y2k Program

Northwest's efforts on a Y2K transition program began in January 1996 and employs a staff of 26 who are dedicated to leading the more than two hundred Northwest people assigned to Y2k related tasks. Our estimated costs for Y2k related activities is \$45 to \$55 million of which over \$30 million has been spent.



The objectives of Northwest's Y2k program are clearly defined and focused: to ensure that all Northwest computers and computer-related systems will function properly on January 1, 2000 and beyond; to assess the Y2k compliance status of the external organizations on which Northwest relies; and to develop workable contingency plans which will enable Northwest to maintain safe, reliable air transport of passengers and cargo.

To effectively address the Y2k issues, Northwest Airlines adopted the methodology prescribed by the Government Accounting Office's (GAO) Assessment Guide on the Year 2000 Computing Crisis. The phases of awareness, assessment, renovation, validation and implementation outlined in this document have served us well in dealing with the complex and interdependent nature of this problem in the airline industry. In a similar way, Northwest has followed the GAO's Business Continuity and Contingency Planning guidelines published last year. Assessment and evaluation of all supporting documentation and compliance to GAO methodology is subject to independent verification by Northwest's Audit and Security department.

Within this context Northwest identified 531 internal information services (IS) systems, approximately half of Northwest's IS systems, which required conversion or replacement to be Y2k compliant. All business areas within Northwest were tasked with identifying and assessing their critical operations components and suppliers for Y2k compliance, again following the GAO guidelines.

Assessing domestic and international airport and air traffic control system readiness has been undertaken with a cooperative and jointly funded collaborative effort with the Air Transport Association (ATA) and the International Air Transport Association (IATA), and other industry trade associations. Member airlines, in addition to their own Y2k programs, have invested \$44.5 million in funding the Y2k programs of these associations.

Northwest has worked closely with both Boeing and Airbus to assess and test our fleet of more than 400 aircraft and our fleet of 20 flight simulators, which must function identically to actual aircraft to be suitable for the training and certification of pilots.

To assess the readiness of worldwide infrastructure systems, Northwest initiated a collaboration with the Gartner Group that is being used by many airlines.

Finally, a Northwest cross-department steering committee was charged with identifying and developing contingency plans for processes considered essential for maintaining the airlines' normal operations and where the potential for failure is high.

Northwest's Y2k Status

At present, Northwest has completed approximately 98 percent of its application renovations and has completed testing of more than 90 percent of its highest priority applications. The remaining renovation and testing are on target to be completed within the third quarter of 1999.

Minor modifications have been made to bring Northwest's aircraft fleet into Y2k compliance. No Y2k safety of flight issues were ever documented within Northwest's aircraft fleet.

Northwest's reservation systems were successfully renovated and capable of booking and selling tickets through all distribution channels, including Northwest's Internet site, since February 4, 1999. To date more than 75 of Northwest's major internal systems have successfully passed initial failure dates.

As ATA reported to the President's Council on Year 2000 Conversion on July 1, 1999, U.S. and Canadian airlines are 95 percent finished with their Y2k remediation efforts. The nation's airports are on schedule with their own Y2k efforts, and the FAA has met its June 30, 1999 completion date for Y2k remediation, and that final independent verification by outside contractors and government agencies is pending.

A status report presented by the International Civil Aviation Organization (ICAO) to the United Nations National Y2k Coordinators Meeting on June 23, 1999, reports substantial progress in all critical areas of air transport and in the development of contingency plans for all contracting states of ICAO.

Remaining Activities

Mr. Chairman, most of what I've discussed up to this point has shown how Northwest Airlines and the aviation industry are addressing Y2k readiness. For the remainder of 1999, Northwest plans to focus on what we're calling Transition Management. This consists of executing contingency plans (as necessary), developing alternative flight schedule scenarios, and dealing with events as they actually occur through the transition.

As the year progresses and more information becomes available on the status and readiness of any of our destinations, Northwest will make and announce changes to our flight schedule. You can rest assured Mr. Chairman, that should any adjustments to Northwest's schedule be deemed necessary, those changes will be promptly communicated to the traveling public.

Northwest will continue to be actively engaged with industry activities to complete remediation and to reassure the public that they can plan to travel during the transition period with full confidence that the same standards for safety, the hallmark of the aviation industry, have been rigorously applied to our Y2k remediation work.

In conclusion, I want to again assure you and the Committee, that Northwest Airlines is on track with its Y2k program, that we are working closely with our industry associations to complete readiness and contingency planning initiatives, and we expect to have normal operations at the start of the year 2000.

I'd be happy to answer your questions now...

Mr. HORN. Thank you very much. We will now go to questions. Mr. Knollenberg.

Mr. KNOLLENBERG. Thank you, gentlemen, for the testimony. I am particularly pleased that we have the big three—I guess it is the big three still—in the audience—getting bigger, each one.

And it is no surprise, Chairman Horn, that they would be here. They do not call this MoTown for nothing, it is motor town, it is vehicle town. And with no apologies to anybody and certainly now we have multi-national connections and obviously all three of you represent those multi-national connections. So I am delighted you are here.

I have heard from each of you about how close you are to compliance and what you have got in place to get there before D-day. About these suppliers, for example, you have hundreds, thousands of them, and you have them in foreign countries. When it comes to the percentage of those—and I think, Mr. Surdu, you mentioned was it 10 percent have not responded? How critical are those 10 percent and what percentage of the criticality of the automobiles that are being made depend on their contribution? Is that something that we could focus on for a moment? And if there is a problem there and they do not respond, do you have backup suppliers?

Mr. SURDU. First of all, the 10 percent is an overall number at this point. That number is, I believe—and I would have to verify it—less than 2 percent in terms of our critical suppliers. For those that have not formally responded through the AIAG process, we have had onsite visits to validate where they are at, so in terms of all of our critical suppliers, we are very, very confident on where they are at. The other suppliers, as I mentioned, that have not responded to date, we are taking a look at them, we have got other actions in terms of additional onsite visits very similar to what Mr. Costantino mentioned from General Motor's plan, and we need to validate, you know, their state of readiness, not assuming that they are in bad shape. But if you take a look at the percentages, the percentages for failure are consistent for us around the globe. So as we take a look at the state of readiness of our suppliers in North America versus other parts of the globe, the numbers are fairly consistent.

In terms of our business contingency planning, of course, that has come into play. We have been mapping that, we do have alternative sources if need be, but we have no plans on doing that. We feel very, very strongly about the relationship we have with our supply base and what impact they would have on our facilities are all a function of our contingency plans.

Mr. KNOLLENBERG. Could I pose the same question to Mr. Costantino and of course Mr. Buck. Mr. Costantino, if you would.

Mr. COSTANTINO. With respect to the supplier base, I would say right now that out of our critical suppliers—we have obviously got thousands of suppliers, many of which would not really impact us if they did not operate on that date. When you get down to the absolutely critical number, you are probably down in the 3,000 to 4,000 range. We have probably got, I am going to say, 400 to 600 of them that we are watching closely right now that we have probably not only had site visits but actually have put people out there to help them remediate.

Mr. KNOLLENBERG. Let me pose this question, are most of the suppliers who have not responded or who are dragging their feet, are they in North America or are they overseas?

Mr. COSTANTINO. I would say right now that the majority of the ones that we are currently working on are not in the United States, they are basically outside, off shore. And our teams overseas are now working with them. Anyone on that list has been visited, everyone on that list will have a contingency plan put together, including, if need be, our going in to provide technical assistance if in fact there is no alternative to ensure the supply chain.

Mr. KNOLLENBERG. Mr. Buck.

Mr. BUCK. Yes, our about 15 percent that we are trying to wrap up with, we are meeting personally face to face with them. They are having to come into Auburn Hills and meet with our buyers. Basically by the end of this quarter, if we cannot be satisfied that they are ready, then we will have a contingency plan with them, which could go as far as banking parts. That is how we are assessing that situation.

Mr. KNOLLENBERG. Thank you.

Let me go to the question about—I think it was Mr. Parker who mentioned the Gartner Group who is addressing or working with several airlines to address your problems. Was there a single group, for example, with the automotive companies, that you sought help from to contribute to eliminating or alleviating your problems, or did you do it internally?

Mr. BUCK. We worked together at the Automotive Industry Action Group since February 1997 and they are having a common problem with our suppliers, so our suppliers would not have to do a GM way or a Ford way or a Chrysler way, now DaimlerChrysler way of determining what they needed to do. And the first thing we did was put together joint sessions. We invited our top 5,000 suppliers between us to a session, a half day session. We invited the chief executive officers in May 1997. We brought them in and said, you know, you probably know you have got this problem with your computer systems, but you also have a problem on your shop floor. We went through and showed them that our plans—

Mr. KNOLLENBERG. When you say we, you mean all three of you?

Mr. BUCK. It was a joint program. And actually we used our audit firms of Deloitte & Touche and Coopers to put this program together. We have a common year 2000 Office for our suppliers, actually several other auto companies have joined that also. We offered it to the world. And we have been sharing information. Basically we talk all the time, “Gee, did you know that when we did this, this happened at one of our sites?” That has really made us take action in making sure that we had the problem handled.

Mr. KNOLLENBERG. So you have worked in a fairly unique fashion then, as I see it.

Mr. SURDU. Consistent with the Automotive Industry Action Group practices, it is really an opportunity for companies like Ford, GM and DaimlerChrysler to get together on common issues, and certainly this was a common issue for us.

Mr. KNOLLENBERG. Here is a common issue as well, the big three, as you are seated there, have over the years and recently produced automobiles that have a great deal of amenities, one of

which is the on-board computer. I understand some of these computers are used for the purpose of fuel injection and navigation. What can you tell me about—have you communicated to the consumers, to the customers, just what the potential problems might be if there are any? Have you reassured them that there will not be problems? Are you doing that now?

Mr. SURDU. Let me begin and we will—I think you will probably hear very similar programs.

But first of all, we have communicated to our entire population, we have responded to every inquiry, several thousand inquiries in terms of the readiness not only of Ford Motor Co. but of its vehicles, both past and present. And we have sent communications out through our dealer body as an example. So there have been very many different mechanisms that we have communicated our readiness and our status. And in particular your question about vehicles, the interesting thing about the technology that is in the vehicles is that the chips themselves are not like the chips you find on a PC. They do not have a system date, they do not carry that kind of functionality. And so there is no date-related functions in the chips themselves. We verified that through our chip manufacturers, our subassembly manufacturers, we have done internal testing. We have even gone so far as to do a global all-employee message or inquiry as to any past or present thoughts that our entire work force might have in terms of our vehicles and researched all of those. And all of those findings came out zero.

You could theoretically put some functionality from a software standpoint into your vehicle that might be date-related, but if you think about the functionality in the vehicles themselves, and certainly in particular in our vehicles, we do not care about the date. If I am looking for maintenance, and the example I like to give our customers is that if you park your Ford vehicle in the garage for 6 months, you do not want the on-board computer to say that it is time for maintenance. We care about things like engine cycles, we do have counters which get reset every time the vehicle is started. So there are no date-related functions that care about the year, that affect either the safety or the performance of our cars.

Mr. COSTANTINO. From our perspective, we are doing the same thing, we have a great deal of communication through the Internet even to try to assure all of our customers, current, future, that we have found no problems in past or current vehicles and we have done the same level of extensive testing on those vehicles. I think our focus has been even more on the dealerships to ensure that they clearly understand this and ensure that they are ready because, quite frankly, they are the face to the public and we want them to be fully operational come the transition period as well.

Mr. KNOLLENBERG. Mr. Buck.

Mr. BUCK. For DaimlerChrysler, it is the same situation. In our vehicles, we have not found anything that would impair or affect in any way running that vehicle. And we have communicated it through the means mentioned. Also, I believe all three of our companies have a statement that is on the National Transportation Safety Board site that also says the same thing. So it is out on the Internet available to the public.

Mr. KNOLLENBERG. I think Y2K may have hit me already, I have a car that has an on-board computer and it tells me I need an oil change, the dealer says it does not need an oil change. I will work that out but I think it may be the fact that somebody did not reset it or some such. So I am not going to blame that on Y2K yet.

Mr. Parker, just in regard to—and I will close with this question—with regard to the airlines, you just heard the automotive people are working together to share information and I remember your saying again that Gartner has worked with several airlines. Is there any communication between the various airlines on this matter, that may go beyond Gartner or maybe in addition or worked in with Gartner?

Mr. PARKER. Yes, it is very substantial. When I was referring to the Air Transport Association and the International Air Transport Association, there are upward of 120 airlines that are working to share information about—if I can draw an analogy to the supplier network in the automotive industry—we share airspace control and airport control functions around the world and so we have been very active from the very beginning sharing information, finding out the state of the programs of the different agencies that control those and share that. That is the majority of where our cooperative effort has been focused.

Mr. KNOLLENBERG. Do you feel good about the year 2000, January 1, 2000?

Mr. PARKER. I do.

Mr. KNOLLENBERG. Are you going to travel?

Mr. PARKER. I would travel. I will be with my programming staff at our data center.

Mr. KNOLLENBERG. So you are going to have your critical employees that will be available during that timeframe, that December 15–January 15 timeframe?

Mr. PARKER. Yes. We have—we will have, much like you have heard earlier, we have canceled all of our vacations for our technical staff. They will be positioned either at our data center or at our major sites such as our major hub airports. We also will have our executives and other decisionmakers in a command center type program, similar to what you have heard from my colleagues, ready to make decisions and reaction to events as they occurred.

Mr. KNOLLENBERG. Is this called insurance, pretty much just in case.

Mr. PARKER. Yeah.

Mr. KNOLLENBERG. But you feel good about where you are. And I guess I am hearing that from all of you, but you also want to make sure that there is no glitch at the end and you are going to be available to handle customer problems.

Mr. PARKER. Yes.

Mr. KNOLLENBERG. Thank you very kindly for your testimony, gentlemen. And Mr. Chairman, thank you. Back to you.

Mr. HORN. Thanks a lot, Joe. Good to see you.

We appreciate having Mr. Knollenberg with us this morning. Since he is getting a little car advice, let me ask Mr. Surdu.

I have been a quite happy customer of Mercuries for a long time, and the reason I bought my 1988 Mercury was one reason and that was that dashboard. And now I do not see anybody using it. It was

terrific, you can know what the speed is with a 1 inch numeral and I love it. A little bit of the electronics went out and I really do not care about that part of the dashboard, but what happened? Why are we back to those crazy needle things that you can hardly see in any car that I have seen?

Mr. SURDU. You know, I wish I could answer that question. Being a systems professional for the company, I cannot answer an engineering question, but I think it has to do with customer needs and customer wants and customer interests. We still have, by the way, some of those dashboards with big dials. I can put you in a vehicle that has one, if you would like.

Mr. HORN. I just wondered, do I have to buy a Lincoln or something to get that dashboard back? Is that the motive?

Mr. SURDU. I will take that back with me. How is that?

Mr. HORN. OK. But I always wondered what happened, because you go in, and really those dashboards with that crazy little needle, you cannot even see it and usually the steering wheel is blocking it and that wonderful dashboard of 1988, which I still have that car and it has worked great for 11, going on 12 years. But I did not know if that was obsolescence or all the other things we hear, but it is a great board, get back to putting it in and I think we will all be happy.

Let me ask you a couple of the questions I did the previous panel, just for the record.

When did Northwestern start undertaking the year 2000 bit?

Mr. PARKER. We began looking at it in 1995 and funded the program in January 1996.

Mr. HORN. And when did Chrysler start that?

Mr. BUCK. Both Chrysler and DaimlerChrysler began in 1995, both sides of the company.

Mr. HORN. I see. So even though you had not merged at that point, why your brains were thinking along that line?

Mr. BUCK. Yes.

Mr. HORN. Well that is great. How about General Motors?

Mr. COSTANTINO. I would say in earnest, 1996.

Mr. HORN. And how about Ford?

Mr. SURDU. June 1996.

Mr. HORN. In June 1996?

Mr. SURDU. Right.

Mr. HORN. Because your leadership under Mr. Peterson was a very international oriented leadership that did a lot for Ford and I just wondered if you would be ahead of that or not, based on that international executive experience you had there.

Mr. SURDU. Well, we seem to think that we certainly have this well under control. You know, you asked the question earlier on in terms of what would we do differently, obviously I would parrot back "more time".

Mr. HORN. Yeah.

Mr. SURDU. But certainly we have learned a lot from this program, there is a lot of positive that has come out of this for us. We understand more than we ever did before the technologies that we have in place on a global basis. And if I would say we would like to start earlier, it would be to take advantage of the things that we now know in terms of some of the things that we are moving

forward with. So it has been a very worthwhile, at the end of the day, experience for us, one I would not like to do too often, but certainly it has been of real value to us.

Mr. HORN. Well, you raise an interesting point. What about your foreign competitors in those days, both Europe and Asia, were they into this earlier than you or after you, or what?

Mr. SURDU. Well, I certainly cannot speak for our competition. I can tell you what—and we have kept very, very close to organizations like the Gartner Group and Forrester and others and our own internal, if you will, intelligence in terms of where the globe is in this Y2K issue. And generally speaking, we agree with all the documentation that Europe has been behind North America, in particular, and other parts of the Far East and South America are working very hard to catch up.

We, within Ford Motor Co., when we initiated the program in 1996, it was a full global program, so we put a full court press on for us internally and began working, as the panel here has indicated, from the big three, with our supply base very, very early on a global basis. But I cannot speak for the other automotives.

Mr. HORN. One of the interesting things is when you look at the global picture, it is mostly in developing countries that the problem exists. And as you know, the United Nations held two conferences on this, and they had a great turnout at the last one just 2 weeks ago, I think 173 countries were represented, whereas the one in the preceding period had been about 120 countries. So the message is getting through, but as you look at the globe, it is the developing countries that frankly do not have the money to do some of this, and the World Bank, I gather, is trying to help them on that. But some of you have plants in these developing countries. Is that a different situation when you are surrounded by people who have not really corrected the tapes and all yet and would that affect you or are there any interactions between your plants and the surrounding economy? I mean, does it make a difference when you are in those developing countries?

Mr. COSTANTINO. Oh, the answer is, I think, it does. But I think we are treating each one of those as we would the United States. In all of our operations, we put the Y2K teams in place. The supply base, I think for all of us, is really global in nature. So in many cases, those suppliers that are actually supplying a Brazilian operation could very well be supplying a North America operation as well. So I think the desire to basically ensure those suppliers are ready is there for not only the international, but also domestic.

I think the piece that we have added is to really take a hard look at the utility situation in those countries, because we may find ourselves where a supplier is ready, but our intelligence tells us that the chances for outages of 2 or 3 days is imminent and therefore, you need to do something from a contingency standpoint to protect your supply chain and also that supplier. And that is an effort that is going on right now.

Mr. HORN. You heard your colleague from Ford say time would have been helpful on this. What was your experience, if you had to do it again now, what is it that you wish you had done?

Mr. COSTANTINO. One thing I wish we had done is kept a better inventory. It took a lot of effort, way more than I think people

thought it would take, to really get an understanding of all of the plant floor equipment, et cetera. And now that we have this information, I hope that we maintain it so if we ever needed it again, we could move more quickly.

Mr. HORN. Was that in relation to the codes in particular processes?

Mr. COSTANTINO. It is everything. I mean just simply knowing where you have 1.4 million devices and how to get to them all took an awful lot of effort and I think the Gartner Group has underestimated in some cases the front end of the work that had to be done.

In addition, for General Motors, we had the complication of being kind of diverse and therefore, we do not have singular systems in many cases, which made the job even more difficult. Again, opportunities in the future though to take advantage of what we have learned.

I am not sure on the time, I think we are where we need to be right now and I think it is the right time. The concern I have is one I was reading last year, people saying they are ready for Y2K. Then they must have an industry that is making no changes because one of the most difficult things we will all face in the next 6 months is managing change, because the world around us, the computers, the things they want to change fast, the systems want to change fast, the plant floor wants to change fast. If you go and think you are done a year and a half ago, you are not done, because I doubt you could shut down change. So I think we are kind of in a good position there because we know the changes have to come but we want to try to manage them.

Mr. HORN. Well, on that matter, as you went through this process for the year 2000, were you able to get rid, able to combine some of your systems that you had to look at and rather than just adapting them, getting rid of them?

Mr. COSTANTINO. I am not sure this is good or bad news, but we eliminated probably between 3,500 and 4,000 systems already.

Mr. HORN. Yeah, well it makes a lot of sense.

Mr. COSTANTINO. Oh, yes.

Mr. HORN. How about DaimlerChrysler?

Mr. BUCK. Just to change the question slightly. Instead of what have I learned, what would I do different; what have I learned that is going to make me do something different in the future. When we ran what we call time machine tests of our manufacturing plants, we found a bug that would have shut our plants down for one shift. And so we are now looking at, you know, what if this had occurred, what could we have done on January 1st and 2nd so we would have caught this in time and not shut our plants down. We are seriously right now looking at operating a plant Saturday night, January 1st, a third shift operation, running for 4 hours, then running all the systems behind that as though it was a normal work day, giving us a day to fix any bugs that we have missed.

You know, we all run tests, but the real world where you are going through a telecommunications company that is in the year 2000 and you are going to suppliers who are bringing in just in time material, and you are doing everything, so that we have some reaction time so that on Monday, the 3rd, we would have a higher degree of certainty that we are ready.

Mr. HORN. Mr. Parker, how about Northwestern, if you had to do it over again, what is it that stands out that you wish you had done first?

Mr. PARKER. Interestingly enough, I think that we allocated enough time to the overall effort. I think starting earlier would have made the whole program a little bit cheaper because it would have been less of an auxiliary effort and more of a mainstream effort. But there are probably three things I would have done differently. I would have liked to have educated the business community inside Northwest, to understand that it was not just an IT problem, to get them involved with business process changes and contingency planning and things much earlier in the cycle. I think we would have been much more aggressive about retiring older systems than—as opposed to fixing them, because we could use this as an opportunity to build for the future better than perhaps we did. And I think we also could have encouraged our industry associations to begin digging for information much sooner than we did.

Mr. HORN. Now when Northwestern began its efforts was about what?

Mr. PARKER. It was in January 1996.

Mr. HORN. Yeah, January 1996. By the way, Mr. Willemsen, come on up and join the panel for the last couple of questions. He is our worldwide expert. We have a chair for you.

What I am interested in is what else needs to be done, if anything, by the Federal Government on the awareness side and what do you wish had been done by the Federal Government in that respect—not that it is doing your work, but what could it have done to be helpful. They finally got around to it. I think they are doing a pretty good job now and it is happening, but it took years to get them to face the music. They ignored it—well, they ignored everything up until, as I said, April 1998. That is when they finally got Mr. Koskinen in there to do the job.

So anything else we could have done on our side on awareness, whatever?

Mr. PARKER. I think on the—from the airline industry, having more visibility into the program sooner, having the—particularly the FAA and other government agency programs started sooner and made aware of the progress to us sooner would have helped. Because we had to start our programs with assumptions that we would have at some point run into some additional work because the assumptions did not hold.

Mr. HORN. I take it on verification, some of you have used inside verifiers, others have used outside verifiers, on the fact that your codes have been adjusted and so forth. What has been the practice at Ford on that, did you have an outside team do it? I remember you mentioned a few accounting consultant firms.

Mr. SURDU. We actually have addressed this in two fashions. Internally, we used both internal and external resources to assist us in the remediation testing and initial verification. We actually did verification work prior to testing. It turns out it simplifies the process to find the problems up front before you get into testing and it facilitates testing. So we used both internal and external resources for that.

Same thing on the auditor side, our general auditor's office has been engaged from the very beginning on this program, and we have used Coopers Price Waterhouse as well.

On the pure verification now, we are taking another pass at it and that is all using external resources.

Mr. HORN. How about General Motors, somewhat similar?

Mr. COSTANTINO. Very similar, actually almost exactly the same. We have multiple testing obviously inside and again, we use EDS which brings in additional outside resources, although they are a prime supplier. But many of our critical systems have been going through independent verification with a totally outside third party.

Mr. HORN. How about Chrysler—Daimler?

Mr. BUCK. At DaimlerChrysler, when we had finished 99 percent of our business systems at the end of last year, we raised the tier or the measurement of completeness to doing integration testing with stand-alone main frames or stand-alone servers, and this sign-off with not only the IT individuals, but with our customers—we are involving all of our customers in our testing and they have to sign off on critical applications. We are using Deloitte & Touche to do independent verification.

Mr. HORN. Mr. Parker, how about your situation in Northwestern?

Mr. PARKER. We follow a similar program, we do an internal IT testing and validation; we then go to our business units and have them sign off for completeness after user acceptance testing. We have an internal auditing department which validates the results and we have also used Ernst & Young as our external audit group. We are also using Price Waterhouse Coopers in our contingency planning efforts, which is an umbrella that sits above virtually all of the program and they have looked at it as well.

Mr. HORN. For the workers you have on America's assembly lines and on the airlines, how have your companies trained employees to recognize and address possible year 2000-related problems? Are they sensitized to that?

Mr. COSTANTINO. In our case, basically we are just taking our normal practices which say that every single plant we have, for example, has procedures—and I am sure it is true for both gentlemen here—to handle any kind of situation such as a power outage or a supplier issue. I mean we deal with these things every day. Y2K is really almost an extension of what we do deal with. So we are back in there just doing two things—making sure everybody is following and understands those procedures and is prepared, and also if there is any uniqueness with respect to potential Y2K ones, how to deal with it. But in many cases, we will also have some technical teams, if we run into a problem that is beyond our capability, that we will then send out to handle any technical problems.

Mr. HORN. How about Ford, about the same way?

Mr. SURDU. Yeah, the one other item in response to your question is we have gone out with numerous all-employee communiques in terms of not only the year 2000 challenge but where the company was and what the company was doing. In addition to that, they have been personally engaged as a result of our end-user computing process. Every desktop owner, we have provided a tool, we have provided training on how to use the tool, and they actually

personally go through a compliance and analysis and a validation phase through the things that they develop. So there is a rich amount of awareness within Ford with our employee base.

Mr. HORN. How about DaimlerChrysler?

Mr. BUCK. In addition to the, what we call incident management teams at each site and what we call our PC rollout where everyone who has a PC has to run a program and assess whether they have created anything that is not compliant, we have put posters all over our company, both an English version and German version, telling the employees here are the types of things we found going wrong. If you know of anything that you think is not compliant, here is who you contact. So we have tried to do everything we can to get down to the employee level, to make sure that if there is something that we have missed, that they are asking the questions. And they are, they are asking the questions. Their interest is growing as we near the year 2000.

Mr. HORN. If you have got an extra set of those posters, I would like it filed with the subcommittee and its chairman in particular, to see if my German has any relationship to my English.

Mr. BUCK. Sure.

Mr. HORN. How about Northwestern?

Mr. PARKER. We have a formal communication plan that includes all of our constituencies. As it relates to the employees, what we have found with the front line employees is that most of what they need is a consistent way to answer customer questions, passenger questions. So what we have done is given them some documentation both in written form and on their systems that they can access to be able to answer those questions. And we have also instructed them to point our customers to our Website which contains kind of our formal communication to our customers.

At a leadership level, we have worked with the different departments throughout the organization to ensure that they have a consistent way of communicating to the work force. And then from a decisionmaking standpoint, those people that are required to make decisions that would recognize Y2K events and make decisions to modify the airline plans, we have gone to a much more formal area and we have attached that in our command center approach with our existing command center and lengthened the time window to be able to accomplish that. So it is more of a formal plan than a communication plan.

Mr. HORN. Well, thank you.

Mr. Willemsen, what needs to be asked of this panel that I have not asked?

Mr. WILLEMSSEN. The one thing that I think that I would like to emphasize is to extend on some of the remarks that were made earlier. I think it is especially important for the companies here to continue publicizing verified facts to the public. That is the best way to combat any rumor or potential panic down the road. I think one comment was made about making sure that the dealerships, since they are the face to the customer, have that information in hand. I think that is especially important, because as we roll into the fall, there are going to be a lot more questions raised about Y2K than have been raised cumulatively to this point. So I think it is especially important that the companies continue putting the

word out, here are the facts of the situation and here is what we know about our products and services and their compliance status.

Mr. HORN. Yeah, I agree with you that is very important, because as we get closer to January 1st, you are going to have people selling their books, selling their solution and all the rest of it. And there is going to be a lot of fear mongers, shall we say, in those wonderful little tabloids as you go through the grocery store line—that kind of thing. So they will turn to that and we just need to head them off by, as you say, getting the facts out there for the public to know.

And I think on the previous panel of public people with the bills they send to the citizens, they might want to put a little information in there about what is happening on the utilities and the water and the electricity and so forth. And we are getting to the electric panel.

One question has come here from the audience—is there another one? Just one. It is for both Northwest and the General Accounting Office. What is the preparedness of other countries like Jamaica in terms of air traffic control? Northwest got any feelings on that?

Mr. PARKER. We do. I cannot specifically speak to Jamaica, but we keep a very close eye on all of that. We would agree, I think, with the assessment that I heard earlier that the United States is in better shape than the rest of the world. Europe is somewhat lagging behind, Asia would probably fall into that area and then a lot of unknowns still remain in the rest of the world.

As you look at the rest of the world, there are really—that part that is the unknowns, there are really two states of being. One is their systems are so old and their normal processes are so inconsistent, that it will just be like a regular day if they were to have a Y2K problem. And we know how to deal with that, we deal with that every day.

The other part is where they have made some modernization of their systems, but we do not know how far they are going to be going into the remediation effort.

Our general read on things now is that it will be safe to fly. Air-worthiness, flight safety issues will be addressed, but some passenger convenience things like moving sidewalks or elevators or HVAC systems, heating and cooling systems, may not be ready and may run into some problems in the smaller countries.

Mr. HORN. Mr. Willemsen.

Mr. WILLEMSSEN. I think there is reason for concern in other countries in the air traffic control system, not necessarily because of what we know, but because of what we do not know. Later this fall, the State Department working with the Transportation Department, plans to issue travel advisories to the citizenry where they have real concerns about the systems within those countries. I think that is a reasonable step from a public information perspective.

Mr. HORN. Yeah, I agree with you. I have a lot of faith in the American Federal Aviation Agency and the Administrator that runs it now. They sort of dragged their feet for awhile and then when she got in there, she started to clean house a little. So I think that is going to happen, at least in the American sweep, but obviously our planes are flying all over the world. And there are some

situations where I am sure they are going to have to really clean up and the ICAO, International Civil Authority ought to be working on that right now with the developing countries.

You have raised a good question. We have not particularly satisfied all the answers; but in terms of the U.S. situation, the Administrator has the power in law from Congress to ground any planes that are in any unsafe situation. So I think there is a lot of effort going on in the towers of this country, and by the way, at L.A. International 4 years ago, they had a few vacuum tubes still, and they had post-its on the windows and things like that. We are getting a little beyond that now hopefully and I long ago suggested to FAA when I was on the Aviation Subcommittee, why do you not go look and see what Lufthansa is doing and 2 years ago, I had a chance to go over there and look and guess what, Ratheon equipment, all over the tower in Berlin. The FAA, in 1993–1994 had blown \$4 billion to try and accomplish the same thing Ratheon had already done with Lufthansa. So hopefully we learn from these experiences.

All of you have given some very important testimony and we appreciate your doing it and we are glad to see people working together, because I know we passed that Good Samaritan Act so competitors could work together without somebody saying it is an antitrust violation, and I have been delighted to see all over this country firms that are pretty—very competitive and did not particularly like their colleagues, are working together to solve this problem. And I think that is good news for the American public. So thank you very much for coming.

We will move to panel three now. Panel three is Mr. Roosen of Detroit Edison; Mr. Lozano of Michigan Consolidated Gas; Mr. Johnson of Wayne State University; Mr. Potter of the Southeast Michigan Health and Hospital Council and Mr. McDougall of the Southeast Michigan Information Center, United Way.

OK, we have got everybody, if you would stand and raise your right hands.

[Witnesses sworn.]

Mr. HORN. The clerk will note six witnesses affirmed the oath. We will begin with Mr. Jim Roosen, the Y2K program manager for Detroit Edison. Glad to have you here.

STATEMENTS OF JIM ROOSEN, Y2K PROGRAM MANAGER, DETROIT EDISON; RAYMOND LOZANO, MANAGER OF STATE-WIDE COMMUNITY RELATIONS, MICHIGAN CONSOLIDATED GAS, ACCOMPANIED BY TOM MOTSINGER, DIRECTOR, INFORMATION AND TECHNOLOGY MANAGEMENT; JAMES JOHNSON, VICE PRESIDENT OF COMPUTING AND INFORMATION TECHNOLOGY, WAYNE STATE UNIVERSITY; DON POTTER, SOUTHEAST MICHIGAN HEALTH AND HOSPITAL COUNCIL; AND DAN McDOUGALL, DIRECTOR, SOUTHEAST MICHIGAN INFORMATION CENTER, UNITED WAY

Mr. ROOSEN. Thank you, Mr. Chairman. My name is Jim Roosen with Detroit Edison Co. and I am one of several Y2K program managers working in our program office. I had submitted some formal testimony and I would like to make some additional comments, if I may.

Mr. HORN. Right, and you have all heard that your statement goes in the minute we introduce you. We would like you to summarize it, do not read it, 5 minutes, and then we can have more dialog.

Mr. ROOSEN. Correct.

The scope of Detroit Edison's Energy year 2000 Program is quite fast. Just for purposes of the audience and the committee, we serve 2.1 million customers in southeastern Michigan in 13 different counties and have 9 power plants and 36,000 miles of distribution line.

We are keenly aware of the seriousness of the year 2000 issue and we are committed to providing a safe, reliable flow of electricity well into the millennium. We began working on our Y2K program in 1996. We, subsequent to that work in our Information Technology Group, we established an enterprise-wide year 2000 program office to oversee all of the year 2000 activities. We have a dedicated team of five executive managers, who have over 125 years of utility experience and they have been assigned to the project. They have both IT experience and operating experience. We have committed over 450 employees to the effort over the last 2½ years.

We have a rather structured program that reports directly to the office of the president of DTE Energy, and we regularly report to the audit committee of the Board of Directors.

Additionally, we have issued a call to action memo to all of our employees in July 1998, to advise them that we would—not to arrange for vacations during the rollover, that there are certain needs that we will have in order to carry out our contingency plans and to be prepared for the unknown.

Where are we? We are on track after 3 years of the program, and the intricate planning and implementation to address the Y2K issues.

In summary, our inventory and assessment considered over 140,000 individual assets and that is complete. Our compliance testing of those assets was completed and of those assets that were determined to be not ready, about 2 to 3 percent of the total assets, 99 percent of that equipment is ready for the year 2000. Everything has been remediated, we are now in the testing phase of that remediated code. And the final system, which has nothing to do with delivering electricity, but it is the back office, the billing systems and some of the support systems, will be moved into production no later than October 1st.

However, the systems that are necessary for the generation, the transmission and distribution of power are ready as of January 30th. In fact, we have sent letters to the North American Electric Reliability Council, who have been asked by the Department of Energy to provide oversight of the national grid, we have sent letters to them informing them that all of our facilities, all of our systems that are necessary for generation, transmission and distribution are in fact complete by the June 30th date.

Additionally, we have sent a letter to the Nuclear Regulatory Commission with regard to our nuclear plant, Fermi 2, that it is ready, has complete Y2K readiness and was complete by June 30th. So those have been completed.

We are in the process now of moving from that asset phase, the individual assets, to what we call a business process approach where we look at it from an integrated standpoint enterprise end-to-end, to make sure that those systems when all hooked together will continue to provide the level of service to our customers that they expect and deserve. We have operated five of our generating units successfully into the millennium mode and some of them are still operating with a millennium year 2000 clock.

We developed some rather detailed business continuity plans and they basically are extensions of our present readiness plans, but with the kind of Y2K twist to them. We are continuing to communicate and to integrate our efforts with others, as other witnesses have said today. We have participated in depth in utility consortium to exchange information and strategies and solutions and testing procedures through the Electric Power Research Institute and other agencies, EEI, the Edison Electric Institute, and others.

We are in the process of assessing and have really completed the assessment of our key mission-critical vendors. There are over 1,200 mission critical vendors and we pared that down to 20 and have worked with each of those vendors to make sure that the supply chain will continue on an acceptable basis through the millennium.

We have been conducting a lot of meetings with the local and State governments and particularly with emergency management organizations here in Michigan, including FEMA in some of the meetings, working with the State police and other agencies to ensure that everyone in southeastern Michigan is working together for infrastructure types of things like electricity and water.

We did participate also in some national tests that were indicated to be held by the North American Electric Reliability Council. One was in April, and there is another one scheduled for September and we will be participating in that. Those tests are not of the grid, those are tests of communication systems that are necessary in the case some unknown event occurs and electronic communications is not available.

Mr. HORN. Let me ask you at this point, are there any tests for the grid?

Mr. ROOSEN. The actual electric grid itself is up and running and the risk of testing it while it is up and running is too great. Simulation tests have been conducted and we have high confidence, because of the lack of a lot of computer operation of the grid, it is basically a manual operation and has a lot of manual backup, that there is very low risk of any Y2K induced interruption of the grid.

Mr. HORN. Based on the New York blackout, the regional blackout, San Francisco had a blackout in the last few months, what have we learned from that, anything that applies to the Y2K situation?

Mr. ROOSEN. Those were all equipment failures. Equipment fails mainly due to overload. And during the heavy load periods during the summer, you will have equipment failures, and they happen every day. In fact, you could not testify today that there are no customers out in Detroit Edison's territory, there will be customers out. But we are used to that, that is our normal operation, and our approach is as fast a response as possible to restore to normal.

The New York one is a particularly interesting one because they have an all underground system and they had some cable failures and it particularly interfered with getting them back because everything is under the street and it takes a long time to restore. Those are the only particulars I have.

We have similar systems, although not as extensive as New York, but we are prepared to respond in a reasonable period of time. Normally a 3-day outage is what we advise our customers to prepare for and we have a fairly good track record of sticking to those 3-day outages. There are the exceptions, of course.

Mr. HORN. Well, thank you, I just wanted to get that on the record right now.

Mr. ROOSEN. Right.

One other thing in terms of integrating our efforts, we have been hosting forums with our partners in gas, water, telecommunications, to make sure that we are all well aware of our remediation status or our compliancy status.

In summary, we anticipate no widespread or sustained interruptions of service as a result of the turn to the new millennium. We cannot, of course, give 100 percent guarantee, like I said, even on a normal day-to-day operation like today, but we can give the guarantee that we will be prepared to respond in the manner that we have become accustomed to because our response systems are well tuned to this kind of an emergency.

That prompt response to unusual circumstances is really our day-to-day job. We will be doing continuous monitoring and coordinating communications with all the emergency management organizations and we will have an emergency communications center manned and be participating both with the Federal and local government.

Mr. HORN. Well, thank you very much, we appreciate that.

Our next witness is Raymond Lozano, the manager of Statewide community relations for Michigan Consolidated Gas and he is accompanied by Mr. Tom Motsinger, director, information and technology management.

[The prepared statement of Mr. Roosen follows:]

Testimony Given to the U.S. Congress Subcommittee on
Government Management, Information and Technology

July 9, 1999, Detroit, Michigan

Good morning, my name is Jim Roosen and I represent the Detroit Edison Company. I would like to share Detroit Edison's Y2K Program status with you. By now, I trust each of you has had the "problem" described to you, so I won't cover that ground again. I have included a pamphlet from one of our trade groups which outlines the situation and provides a general overview, which you can peruse at your leisure.

What I prefer to spend our time on is what we are doing, where we are, and where we are going during the remainder of 1999.

If you would, please refer to Page 1 of the two-page multi-colored attachment.

We have a comprehensive enterprise-wide effort focused on the Year 2000 situation.

Basically, our effort can be thought of in four pieces:

- Asset focus in *Green*
- Process focus in *Blue* and *Salmon* and
- Management focus in *Grey*;
- With a continuous effort of awareness/commitment in *Yellow*.

Life cycle cost for Detroit Edison's effort is expected to exceed \$80 million dollars.

Moving directly to the mission-critical asset focus section, Green; we have processed over 140,000 assets throughout our overall phases. An asset is all systems, hardware, software or equipment, such as a meter, a computer system (e.g. customer care system) or a relay. To date, we have attained the following current status:

Inventory: 100% complete

Assessment: 100% complete

Compliance Testing: 100% complete

As the Company receives new assets, they are put through the same process with the same rigor as those in the original inventory.

Remediation: 99% complete

Our remediation phase includes post-remediation testing. The only mission-critical assets for which testing is still in progress are several business systems which will be complete by September of 1999.

The above status includes the efforts of our Fermi 2 nuclear plant team. No shut down has been required for any Y2K specific work. The balance of the Fermi 2 assets was completed in June. On June 30, 1999 a letter was sent to the Nuclear Regulatory Commission stating that the plant's Y2K readiness program is complete for those systems required for the operation of Fermi 2.

From an overall perspective in this asset-focused piece, 99% of our assets are in a ready state for Y2K as I speak. On June 30, 1999 the Company officially informed the North American Reliability Council (NERC) by letter that critical systems essential for the

Testimony Given to the U.S. Congress Subcommittee on Government Management, Information and Technology, July 9, 1999, Detroit, Michigan
Page 3

generation, transmission and distribution of power are ready for the change to the new millennium. However, we are not resting on our laurels, while completing this painstaking work is a tribute to the numerous dedicated employees' and partners' relentless efforts, we are acutely aware of the remaining work to be done in 1999. Complacency could become our worst enemy.

Please refer to page 2 of the two-page attachment. I would like to point out another key aspect of our program, Clean Management. This effort is targeted at not reintroducing Y2K problems into our environment once we have "cleaned" them. This effort touches every aspect of our normal, daily business as we continue to connect customers, maintain our infrastructure, and introduce innovative solutions that increase operation efficiencies and customer satisfaction. Clean Management is introducing a new discipline into our culture that will change how we perform our business activities long into the future.

Now, let me move to the management perspective or the Grey area of the chart. The story here is not as well depicted by the bar graphs. The tenets of our management strategy are rigor and thoroughness, formal project management principles and substantial Senior Management involvement to ensure adequate resource allocation and attention to the effort.

Detroit Edison's program management team driving this effort consists of five full-time senior executives with more than 125 years of combined experience in utility operations. We met weekly with various project members to review nearly 100 individual, detailed

and resource-loaded plans for progress and deviation from the plan. The team reports directly to the Office of the President and is championed by Robert J. Buckler, President of DTE Energy Distribution. Additionally, we are guided by a steering committee comprised mainly of officers of the corporation including the Chairman, CFO, CIO, President of DTE Energy Resources, Legal and the Controller. Regular updates are also scheduled with the appropriate committees from our Board of Directors. Each and every employee has a specific Y2K goal as part of his or her 1999 work goals.

From a quality perspective, we are applying the principals of ISO 9000 standards to our policies and procedures. Independent, periodic reviews of our effort in addition to frequent self-assessments are also conducted.

Moving into the Blue and Salmon areas of the handout, you will note three areas of focus, Integration Testing, Business Continuity Planning, and Emergency Operations. This is where we move from an "asset" perspective to a "process" perspective. By process, we mean the series of steps or activities used to conduct our everyday business. This includes such things as Customer Connections, Revenue Collection, and Electric Grid Operations.

In the integration phase, we are going the extra step and actually testing the assets associated with the specific business process in a "Millennium Mode." To date, we have run many of our generating units successfully in this mode. We have also, to a more limited extent, tested the communication aspects of scheduling and delivering power at

the Michigan Electric Power Coordination Center (MEPCC) with our partners from Consumer's Energy. We have experienced no situations which would threaten normal operations. We will continue this type of process-focused testing throughout the third quarter of this year to increase our confidence in our ability to operate successfully in the Year 2000. Additionally, we will participate in the next NERC national drill scheduled for September 9, 1999.

Moving our focus to the last section, both Business Continuity Planning and Emergency Operations, you'll notice this phase extends well into the fourth quarter of this year. These efforts are recognition that there are always unknowns. In these phases, we continue to modify our existing plans and procedures to comprehend Y2K specific scenarios.

Let me speak for a moment about existing plans and offer some insights into the Emergency Management perspective of our efforts. Currently over 5,000 of our employees have emergency management assignments, have been formally trained for their assignments and, in fact, been mobilized and performed successfully in actual emergency situations such as storms. Recently, we received national recognition for our emergency response plans. We expect no less of our employee and management performance in a Y2K-related incident, if the need arises to "mobilize our troops". This is an example of where we modify existing plans for the Y2K scenario. We are also engaged with the State Emergency Management Organization through the Michigan State Police and local units of government to ensure appropriate coordination of necessary

Testimony Given to the U.S. Congress Subcommittee on Government Management, Information and Technology, July 9, 1999, Detroit, Michigan *Page 6*

response efforts in the event of an unknown failure. Additionally, we have hosted four governmental/community events across our service territory to highlight the Y2K issue and generate broad community cooperation in the planning efforts. As a final point in this section, we plan to initiate our emergency organization during the last quarter of this year and engage the team in the performance of Y2K specific drills.

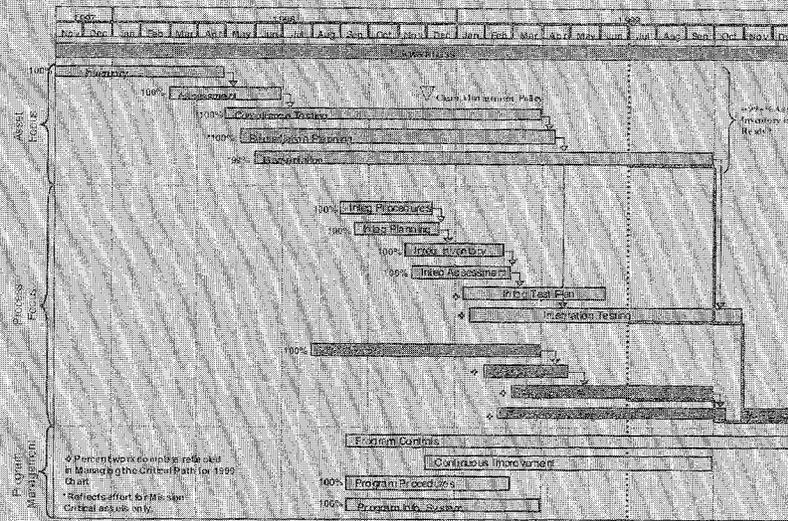
Also attached to this testimony is our latest press release on the Y2K issue.

In closing, let me assure you that Detroit Edison's commitment to providing a safe, reliable flow of electricity in the new millennium is on track. We are keenly aware of the crucial link we provide to almost every aspect of society. We recognize the need to serve our customers in our every day work as well as when faced with the challenge of meeting the Year 2000 issue.

Thank you for your time and attention.

Appendix - Page 1

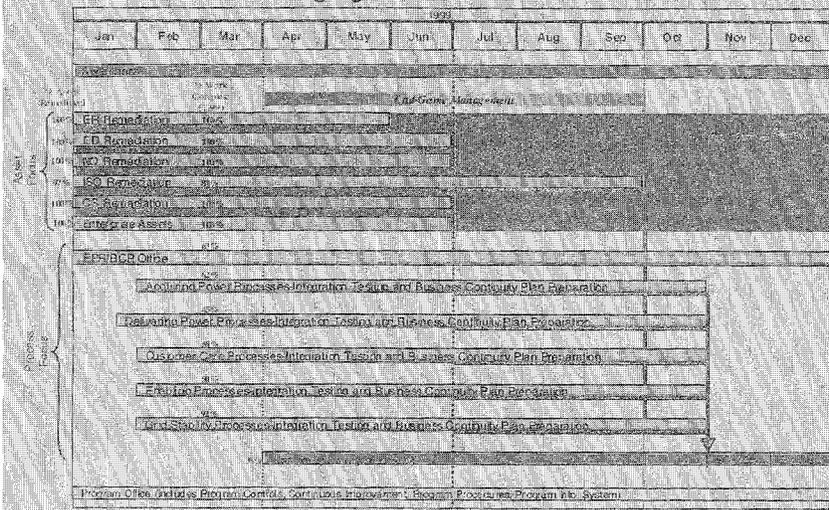
Managing the Overall Process



Source: 12R Prime Controls

Appendix - Page 2

Managing the Critical Path For 1999



Appendix - P2K Project Summary

June 30, 1999

For Further Information:

Scott L. Simons
(313) 235-8808

Lewis K. Layton
(313) 235-8809

DETROIT EDISON TELLS GOVERNMENT GROUPS IT'S Y2K-READY

DETROIT – Detroit Edison – after three years of painstaking work in connection with Year 2000 (Y2K) computer issues – today sent letters to the North American Electric Reliability Council (NERC) and the Nuclear Regulatory Commission (NRC) that it has all mission-critical systems ready for the change to the new millennium.

"Detroit Edison believes that the company's primary functions related to production and delivery of electricity will continue reliably through Y2K dates," said Robert J. Buckler, president of DTE Energy Distribution, in the letter to NERC. "Recognizing, however, that no company can make absolute guarantees about something as complex as Y2K, Detroit Edison is developing ... contingency plans to address potential problems caused by Y2K."

A similar letter to the NRC stated the Y2K readiness program is complete for those systems required for operation of the Fermi 2 nuclear power plant. In addition, the letter noted that contingency plans have been developed to mitigate the impact of Y2K-induced events at key rollover dates.

Since the inception of its Y2K Program in 1996, Detroit Edison has committed itself to providing a safe, reliable flow of electricity come Jan. 1, 2000. As many as 700 people have worked on the program, with current staffing at about 400. The program cost is expected to exceed \$80 million.

Detroit Edison, in its mission to become Y2K-ready, has inventoried, assessed, repaired or replaced, and tested about 140,000 critical software programs and susceptible devices involved in the utility's operations to generate and distribute electricity. At power plants for example, generation equipment has been tested six ways, including setting computer clocks forward to Jan. 1 and leap year at steady operation, increasing power and decreasing power.

The utility's focus now is on completing business continuity planning and contingency plans to prepare to respond promptly to unknown occurrences which may interfere with electric service to customers.

"We are confident that any "unknowns" that surface during the changeover to 2000 will have no major impact on our ability to generate, transmit and deliver power to our customers," said Paul A. Childs, manager, Year 2000 Program. "Working in our favor is that customer demand for electricity is low at that time of year, so if there is a situation at a power plant, we'll have other plants to turn to. As an electric utility, storm restoration management and crisis response is part of our everyday operations. Y2K contingency planning just adds a new twist to our existing skills.

"These achievements, along with progress being made by our other major suppliers, is providing us with a higher degree of confidence that Y2K will look like any other date rollover," Childs added. "We believe that this tremendous progress should also help allay the fears of our customers and give them confidence that Jan. 1 will be like any other day for reliable electric service."

Detroit Edison also has taken a lead role in the Southeast Michigan Y2K Utility Forum, recognizing that electric, gas, telephone, and water and sewerage utilities are interdependent. All utilities in the area have joined forces to support each other and share information, and will be in communication with each other through the rollover to 2000.

In addition, the company has been working with major utility industry associations and organizations, as well as customers, vendors and key units of government to gather and share information on Y2K issues. Detroit Edison also is in close contact with suppliers critical to company operations and is continually assessing their progress on Year 2000.

Detroit Edison successfully tested its backup communications systems in April, and will participate in a drill Sept. 9 that will involve electric utilities in North America.

For more information about Detroit Edison's Y2K program, call toll-free, (888) 464-3376, or visit Detroit Edison on its Website - <http://www.detroitedison.com>.

Mr. LOZANO. Mr. Chairman, good morning. Thank you for the opportunity to testify here.

As mentioned, I am Ray Lozano, manager of statewide community relations.

In summary, MichCon provides natural gas service to about 1.2 million homes throughout the State in terms of factories, businesses and institutions throughout Michigan. On any given day, we deliver gas to about 4.5 million residents.

We want to fully assure the committee today that—and all of our customers, that come January 1st, we are expecting that natural gas will continue to flow to our homes and businesses that we serve. Very simply, we are committed to delivering the gas service that we have been delivering throughout our 150-year history.

We have been working, in terms of replacing our business systems, since early 1995 and established a corporate-wide Y2K office in 1997 that reports to a vice president that in turn reports to the chairman of our parent company, MCN, and to its Board of Directors.

We have, in fact, inventoried our systems and developed a schedule for prioritizing and assessing any concerns. We have identified all of our partners with whom data is shared, to prevent the disruption of information flows. And we have worked with our suppliers and established milestone to track this progress.

In summary, we have focused on five mission-critical processes—the incoming calls from our customers, our gas supply, gas storage and transmission operations, gas leak and emergency response capability and appliance service requests. In fact, this effort addresses all aspects of our business, including our customer information systems, our communications equipment that includes telephone, radio and emergency systems, the control equipment that we employ for gas handling, storage and meter reading, and of course interfacing with our suppliers, partners and financial institutions.

I would like to report that we are on schedule, we fully expect to be year 2000—that we will be ready by the end of September on Y2K issues, and most of our systems already are. Those that are not currently ready are being modified or replaced.

Even though we had expected everything to be ready by the end of September, we developed contingency plans also and we have been testing these plans since last December. As with Edison, we are working in coordination with other utilities and the Michigan State Police Emergency Management Division and other EMD departments throughout the State. Also involved with the AGA and its member utility companies in terms of the DOE coordination of member utilities.

Probably nowhere have we sensed more a sense of partnership than with our major gas suppliers and transmission pipelines. The cooperation that we have had from them in this effort is dedicated to keeping adequate supplies of gas flowing in our system. The safety of our customers and our employees is our major concern and we think with this sense of partnership, we have even more ensured this capability.

Our goal, of course, is to keep gas flowing to our customers and continue to dispatch technicians, even if we are to lose all commercially provided electricity, even if every piece of electronic control

and measurement equipment in our transmission and distribution system, and even if our current telecommunications links were to be interrupted. Right now, we fully expect that we will be able to maintain critical services even in the event of the loss of those scenarios.

Even in the unlikely event of this kind of a system failure, we are prepared to operate our systems manually. In fact, our major gas handling systems are designed to function in emergency situations without electricity or computer controls. In this AGA combined effort that we have doing, it has been reported that less than one in five Americans think that the Y2K problem will affect their natural gas service and we think that is a remarkable level of confidence.

We would like to thank you again for this opportunity to be here and invite any questions.

[The prepared statement of Mr. Lozano follows:]

464

Statement
of
Raymond Lozano
Manager of Statewide Community Relations
Michigan Consolidated Gas Company

Field Hearing
of
Subcommittee on Government Management, Information & Technology
U.S. House of Representatives

Detroit, Michigan
July 9, 1999

(These statements are informational and should not be construed as MCN Energy Group Inc.'s warranty of Year 2000 readiness. This information is a Year 2000 Readiness Disclosure. Therefore, MCN Energy Group Inc. claims the full protections established by the "Year 2000 Readiness Disclosure Act" for Year 2000 Statements and Year 2000 Readiness disclosures.)

Good morning.

My name is Ray Lozano. I am Manager of Statewide Community Relations for Michigan Consolidated Gas (MichCon). With me today is Tom Motsinger. Tom is MichCon's director of Information and Technology Management. He heads up our Year 2000 Project Office. I have asked Tom to join me today to address the technical questions that you may have.

We want to thank you for the opportunity to address you about this important matter.

MichCon provides natural gas service to 1.2 million homes, factories, businesses and institutions across Michigan. On any winter day, the gas we deliver helps to warm more than 4.5 million Michigan residents.

Lozano – Y2K, July 9, 1999

2

As January 1, 2000, approaches, we expect our customers' interest in this topic to increase greatly. Prompted by growing media attention, our customers' interest already has increased.

We want to assure you -- and all our customers -- that come January 1, we expect natural gas to continue to flow to the homes and businesses we serve.

Very simply, we are committed to delivering the critical services that our customers have come to expect during our 150-year history.

Does that mean that every computer system will function perfectly? Frankly, I wish I could be 100 percent certain, but Tom assures me I can't.

I CAN assure you, however, that we are doing everything we can to be Year 2000-ready. In fact, we have been preparing since early 1997.

Upon establishing a corporate-wide project office to manage the effort, we have followed an aggressive, disciplined approach ... an approach that is widely accepted as the standard for organizing Year 2000 efforts.

In brief, we have:

- Inventoried and assessed our systems ...
- Developed a schedule prioritized to address any concerns ...
- Identified partners with whom data is shared to prevent the disruption of information flows ...
- Worked with suppliers, and ...
- Established milestones to track our progress ...

Lozano – Y2K, July 9, 1999

We have focused on five "mission-critical" processes:

- incoming calls from customers,
- gas supply.
- gas storage and transmission operations,
- gas leak and emergency response capability and
- appliance service requests.

The scope of this effort addresses all aspects of our business, including:

- Our Customer Information System ...
- Our communications equipment, including telephone, radio and emergency systems
- The control equipment we employ for gas handling, storage and metering ...
- And, of course, our interfaces with suppliers, partners and financial institutions.

I am happy to report that we are on schedule. Bottom-line, we fully expect we will be Year 2000-ready by the end of September. Most of our systems already are. Those not currently ready are being modified or replaced.

Even though we expect our systems to be ready by the end of September, we have developed contingency plans. We have been testing these plans since last December.

In addition, we are participating in contingency planning efforts led by the Michigan State Police Emergency Management Division, local E-M-D activities here in southeast Michigan and the federal Department of Energy program through the American Gas Association.

Nowhere is this sense of partnership more evident than in the efforts with our major gas suppliers and gas transmission pipelines. Together, we are dedicated to keeping adequate supplies of gas flowing into our system.

Lozano - Y2K, July 9, 1999

This effort builds on a long-standing tradition of partnership and mutual support among members of the natural gas industry and most especially among utility companies here in Michigan.

Our fundamental goal, of course, is to keep gas flowing to our customers and to continue to dispatch our technicians ... even if we were to lose all commercially provided electricity ... even if every piece of electronic control and measurement equipment in our transmission and distribution system failed ... even if our current telecommunications links were to be interrupted.

Right now, we fully expect that we will be able to maintain critical services even in the event of these scenarios.

In the unlikely event of these kinds of system failures, we are prepared to operate our systems manually. In fact, our major gas-handling systems are designed to function in emergency situations without electricity or computer controls.

As the American Gas Association recently reported: Less than one in five Americans think a Y-2-K problem will affect their natural gas service. That's a remarkable level of confidence.

We at MichCon have been working hard to justify that confidence and trust.

Thank you.



YEAR 2000 Update

Period ending 3/31/99

YEAR 2000 INFORMATION AND READINESS DISCLOSURE ACT - These statements are informational and should not be construed as MCN Energy Group Inc.'s warranty of Year 2000 readiness. This information is a Year 2000 Readiness Disclosure. Therefore, MCN Energy Group Inc. claims the full protections established by the Year 2000 Information and Readiness Disclosure Act for Year 2000 Statements and Year 2000 Readiness Disclosures.

BACKGROUND

As a result of computer programs being written using two digits rather than four digits to define the year, any programs that have time sensitive software may recognize a date using "00" as the year 1900 rather than the year 2000. This Year 2000 issue, if not addressed, could cause computer systems to malfunction and have a material adverse impact on MCN's operations and business processes. The effects of the Year 2000 issue could be exacerbated as a result of companies' dependence on partners, operators, suppliers and government agencies.

PLAN AND STATE OF READINESS

MCN, aware of the Year 2000 potential impact, initiated a business systems replacement program in 1995. Additionally, MCN established a corporate-wide program in 1997 under the direction of a Year 2000 Project Office. The Year 2000 project is overseen by a vice president of the company who reports regularly to the MCN Chairman and Board of Directors. MCN has also retained the services of expert consultants to evaluate its Year 2000 program and to independently assess and validate its processes. MCN has implemented a four-phase Year 2000 approach consisting of: i) inventory - identification of the components of MCN's systems, equipment and facilities; ii) assessment - assessing Year 2000 readiness and prioritizing the risks of items identified in the inventory phase; iii) remediation - upgrading, repairing and replacing non-compliant systems, equipment and facilities; and iv) testing - verifying items remediated. MCN is generally on schedule to have its mission critical business systems and measurement and control systems (including embedded microprocessors) Year 2000 ready by mid year 1999. The extension of the program to September 30 reflects MCN's determination that additional testing and remediation is appropriate for some critical business and control systems for both MCN and its partners and vendors. MCN's business systems primarily consist of general ledger, payroll, and customer billing and inventory control systems and their related hardware. MCN's measurement and control systems primarily consist of the "SCADA" system, which measures and monitors the transportation and distribution of gas, as well as regulators, pressure controls and meters. The estimated completion status of these systems and the projected status for the future follows:

Business Systems	Inventory	Assessment	Remediation	Testing
March 31, 1999	100%	100%	80%	45%
June 30, 1999	100%	100%	95%	85%
September 30, 1999	100%	100%	100%	100%

Measurement and Control Systems	Inventory	Assessment	Remediation	Testing
March 31, 1999	98%	98%	93%	88%
June 30, 1999	100%	100%	98%	98%
September 30, 1999	100%	100%	100%	100%

MCN also has visited essential partners, operators and suppliers to review their Year 2000 issues and share information. To the extent that any of these parties experience Year 2000 problems in their systems, MCN's operations may be adversely affected. The majority of MCN's key partners, operators and suppliers have represented to MCN that they have completed their Year 2000 inventory and assessment phases. MCN is continuing to monitor the progress of these key partners, operators and suppliers toward their completion of the remediation and testing phases.

YEAR 2000 Update

Period ending 3/31/99

COST OF REMEDIATION

Costs associated with the Year 2000 issue are not expected to have a material adverse effect on MCN's results of operation, liquidity or financial condition. The total costs are estimated to be between \$5 million and \$6 million, of which approximately \$3.9 million was incurred through March 1999. This estimate does not include MCN's share of Year 2000 costs that may be incurred by partnerships and joint ventures.

The anticipated costs are not higher due in part to the ongoing replacement of significant older systems, particularly MichCon's customer information system. MCN has made a substantial investment in new systems that are in process of being installed, as well as those installed over the past few years. The replacement of these systems, and the customer information system in particular, was necessary to maintain a high level of customer satisfaction and to respond to changes in regulation and increased competition within the energy industry. While the system replacements were not accelerated due to Year 2000 issues, MCN expects the new systems to be Year 2000 ready.

RISK AND CONTINGENCY PLANNING

MCN anticipates a smooth transition to the Year 2000. However, the failure to correct a material Year 2000 problem could result in an interruption in or a failure of certain business activities and operations such as: i) delivery of gas to customers; ii) control and operation of the distribution system by electronic devices; iii) communication with customers for purposes of service calls or inquiries; and iv) timely billing and collection. The risk and impact of such failures is largely dependent on critical vendors and the external infrastructure that includes telecommunications providers, gas suppliers and project partners. The most reasonably likely worst case scenarios would be the extended inability to deliver gas due to the failure of embedded systems in the distribution process or the extended inability to communicate with and respond to customers due to the loss of telecommunications. Such failures could have a material adverse effect on MCN's results of operations, liquidity and financial condition. Due to the uncertainty inherent in the Year 2000 issue, resulting in part from the uncertainty of the Year 2000 readiness of key partners, operators, suppliers and government agencies, MCN cannot certify that it will be unaffected by Year 2000 complications. MCN has addressed the Year 2000 risks of its business by prioritizing such risks based on the worst case scenarios and their impact on the business. Focusing first on the safety and welfare of MCN's customers and employees, the following two mission-critical processes were identified: gas supply and distribution, and leak management emergency response.

While MCN believes it will be able to remediate and test all internal systems that support these processes, it fully recognizes its dependence on partners, operators, suppliers and government agencies. In order to reduce its Year 2000 risk, MCN is developing contingency plans for mission-critical processes in the event of a Year 2000 complication. Through failure scenario identification, MCN's approach is to develop reasonable and practical contingency plans to maintain operations in case of non-performance. Contingency planning teams have been established to address specific scenarios and mission critical functions identified in support of the safety and welfare of customers and employees. External suppliers have been contacted for their participation in the contingency planning efforts for gas supply and transportation, and materials management. Contingency plans for several essential gas transmission facilities continue to be tested under a "power outage" scenario and have achieved excellent results. Contingency plans will continue to be refined throughout 1999 as MCN works with partners, operators, suppliers and governmental agencies.

Mr. HORN. Well, we appreciate you coming.

Let me just ask you a question before I forget it. We have been worried about what is happening in eastern Europe with the Russian natural gas supply and a lot of that is what keeps the industry and the homes warm in January in particular when this date situation is going to occur, and the problems they have found in east Europe is some microchips in the refineries' operation, in the ships' operation if they are bringing anything in to a refinery and in the pipelines. And I just wondered, your source is really domestic United States, I take it, in terms of natural gas, so you do not have any of those worries that the Russians might be having?

Mr. LOZANO. Right. Most of our supplies are domestic, and even Michigan provides a source and we have over 40 billion cubic feet in our own storage reserves that fully can take us through a normal winter.

Mr. HORN. How long would that last if it was run down for one reason or the other?

Mr. LOZANO. I am sorry?

Mr. HORN. How long would that supply you have in your inventory right now—how many days would that give everybody in Michigan a chance—

Mr. LOZANO. That normally takes us through a normal winter.

Mr. HORN. A normal what?

Mr. LOZANO. Winter season.

Mr. HORN. Normal winter. So you could last with that inventory over a month?

Mr. LOZANO. An extended period of months, yes.

Mr. HORN. When does it run out?

Mr. LOZANO. It depends really on weather conditions and the usage that customers are using, but it—40 billion cubic feet takes us through our normal heating season which begins in October and runs through April.

Mr. HORN. So you really could do it without further supplies between October and April?

Mr. LOZANO. I think we could take it through a critical period. I cannot say that we are not getting additional supplies during that time period, there are purchases on the spot market.

Mr. HORN. Well, that is interesting to know, you have a very long span then, just based on what is in the pipeline and everything else.

Mr. LOZANO. Yes.

Mr. HORN. OK. Well that thought had not really reached Washington, DC, so it is going to reach it now. We thank you for that.

Mr. James Johnson is the vice president of computing and information technology for Wayne State University. Glad to have you here.

Mr. JOHNSON. Thank you very much, Mr. Chairman, for the opportunity to testify today. I would also like to thank you for holding these hearings. I think it is very critical that we have an awareness of the year 2000 problem through our institutions and through our society.

Wayne State University has been dealing with the year 2000 problem for approximately 4 years. Universities are not notorious

for being early to the game, but in this case, we have been fairly early to the game.

We have gone through a metamorphosis of probably three stages, I would say. The first stage was awareness that we had a computer problem with large administrative systems. The second awareness was the awareness that we have embedded systems throughout the University running the gamut from building heating systems and elevators to distributed laboratory equipment in the medical school. I think the third stage of awareness has been our concern about critical suppliers. I would like to just mention briefly where we are in each of those three areas.

We have been at the administrative game with the large administrative systems for registering students, handling financial records and handling human resource records, for about 3 years. We did our last test over the July 4th weekend. We did encounter a problem, even though we had tested extensively when we put the system into production; we had one glitch that caused us to be unable to register students for 3 days. The lesson there is you can test all you want, but until you put something in actual production, there is always something that is going to catch you somewhere.

In embedded systems, we have identified about 10,000 pieces of laboratory equipment, about 2,000 of them have date-sensitive chips in them. We have already tested and evaluated 1,000 of them and we are finding about 1 percent of the embedded chip systems have year 2K problems that are going to have to be remediated or overlooked, as the case may be. We have 9,000 personal computers throughout the campus, 90 percent of them are compliant.

One area we have been surprised in as we have looked at the core administrative system is that a lot of our departments have their own spreadsheets and systems as well. We have identified 3,300 departmental systems and of the 3,300, 56 percent are non-compliant, and so we are in the process of remediating those at this time.

Suppliers, we are in a little different position than the large automakers in the sense we do not have this same level of clout with suppliers. And I think that that concern runs from utility service—we have been tested last week in that arena, having on successive days lost power and the lost water. We call that pre-year 2000 planning.

With the suppliers, we have had a lot of difficulty getting them to indicate whether they were compliant or not. In some instances where they have said they have been compliant, they have not when we have tested the system. In other cases where they said they would become compliant, they come back to the table and say ah, but you have to get a new version of our software at a cost of \$100,000 or something like that. So that is our concern right now is in that area.

Last, but not least, we do expect problems and therefore, we have a contingency plan in place. Our employees will not have vacations as with most IT employees. We have also involved public safety in the program as well.

We have carried out a lot of the practices that have been recommended by the General Accounting Office in terms of getting compliance throughout the University. As you well know, univer-

sities are very decentralized with people having different sources of funds and they do not always respond well to orders. We have had a lot of success with report cards, with holding individual departments responsible rather than the IT area responsible, by having sponsors in every department, in every school, and by having training and workshop programs.

One innovative program we have put in place is a student awareness program, which makes our students aware of how year 2K may affect their lives and their interactions with the university. I do not know of other schools that have done that.

What has been a large help to us has been publicity, through efforts such as yours, which has made the campus aware that there is a problem. And the other thing that has been very helpful, are tool kits that we used, particularly from the Department of Education. Which was surprising.

In closing, I would like to say there is a bright side to this. I think we have really sharpened our skills in dealing with crisis and recovery. We have really improved and enhanced communication between areas of the University. We have been forced to put new systems and processes in place sooner rather than later, from which we will gain benefits in efficiency down the road.

That concludes my comments, thank you.

[The prepared statement of Mr. Johnson follows:]

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

U.S. HOUSE OF REPRESENTATIVES

JULY 9, 1999

Testimony on Year 2000 Computer Problem Submitted by: James W. Johnson, Vice
President for Computing and Information Technology, Wayne
State University

My name is James Johnson, Vice President for Computing and Information Technology, and responsible for Wayne State's Year 2000 computer problem assessment and remediation effort. I am pleased to report on Wayne State's year 2000 compliance effort and our concern about major external service disruptions on that effort. I want to convey to you that the year 2000 problem is pervasive, serious, and tractable. I also want to impress upon you the idea that the year 2000 problem becomes more pervasive, more serious, and less tractable if basic services fail or perform inadequately.

Wayne State is a Carnegie Research I University located in the cultural center of the nation's automotive capital: Detroit, Michigan. With approximately 31,000 students enrolled in 14 schools and colleges, Wayne State is the 17th largest university in the nation, containing the 4th largest graduate school, with a commitment to excellence in teaching, national prominence in research, and a deep involvement in community service. Wayne State produces most of the area's doctors, lawyers, teachers and engineers.

I want to underscore one point. Wayne State as an urban, Research I university, is in a highly competitive, global environment. If we are disadvantaged by year 2000 problems, we will lose our ability to serve our students and conduct cutting edge, often life-saving, research.

Recognizing an absolute and competitive vulnerability, the Wayne State University President and Board of Governors have undertaken a very aggressive year 2000 computer compliance program at a cost of millions of dollars, knowing that the cost of non-compliance would be greater.

Wayne State is replacing some outdated basic systems such as financial accounting with year 2000 compliant systems. It has contracted with Compuware, Inc. to remediate other systems such as human resources, payroll, and purchasing. These systems have been fixed and tested as year 2000 compliant. Wayne has replaced the operating system on its mainframe computer and has assured that all local data networks will operate. Public safety and security systems for fire and access have been certified as year 2000 compliant. Our purchasing office will not allow acquisition of equipment or software that is not year 2000 ready. Wayne's facility systems ranging from building energy management systems to elevators will be year 2000 compliant. Desktop computers and office equipment that are not year 2000 ready are being replaced or fixed. Replacement, repair and testing of major computer based systems is 90% complete with 100% completion scheduled for October 1, 1999.

Laboratory equipment, a most critical element, is being checked for year 2000 compliance. Our experience to-date is that about 1% of equipment with embedded computers (chips) are non-compliant, with further research needed on 10%.

In the depth and breadth of its efforts, Wayne would rank in the top 20 percent of U.S. universities in addressing the year 2000 computer problem. It is in the top rank because it was early, because it addresses departmental as well as central university problems, and because it looks at laboratory and facilities equipment that rely on computer "chips" as well as computer programs. (See <http://y2k.wayne.edu> for further information).

A key component in the University's program to minimize our year 2000 computer problem exposure has been to inform each school, college and division of its responsibility in dealing with the problem. As part of this program we have appointed year 2000 sponsors to oversee, coordinate, and report on year 2000 efforts in each unit. The sponsors are responsible to you and the University to identify and correct problems that may affect your unit and make contingency plans for problems that appear after the year 2000 begins that were not anticipated.

Even with such an aggressive program, Wayne realizes it will not catch all problems. So it is putting into place a contingency plan to deal with failures as they occur. This means that key employees will be on-call, if not on-site, during the New Year period.

Wayne State is satisfied, although still uneasy, with our efforts to overcome any internal problems associated with the year 2000 computer problem. We are, however, increasingly concerned with our dependence on external agencies that may or may not have adequate year 2000 remediation efforts and contingency plans. The problem is clouded by lack of information that would indicate what possible points of failure we should focus on. Exculpatory clauses are the order of the day, rather than informed assessments of probabilities of failure and sharing of plans to deal with disruptions in service.

If basic services such as electricity fail or perform poorly in the year 2000, Wayne State and all of society will face great problems. It will also make it more difficult to recover from other year 2000 computer problems because we cannot deal with them as they occur over time, but as utilities are available.

A positive aspect of the year 2000 effort at Wayne State has been a realization of our dependence on computer based and computer controlled systems. As a result we have made our systems more fault tolerant and more redundant, and have sharpened plans to deal with internal failures and external service disruptions.

Thank you for the opportunity to report to you. If we are diligent and not complacent, I believe the year problems will be mitigated.

Y2K Site Map

WSU Y2K Home Page

- **General Information**
 - [Charter](#)
 - [Methodology and Organizational Structure](#)
 - [Contacts](#)
 - [Oversight Committee](#)
 - [Implementation Committee](#)
 - [Advisory Board](#)
 - [Support Coordinators](#)
 - [University-Wide Contacts](#)
 - [S/C/D Sponsors](#)
 - [S/C/D Leaders](#)
 - [Downloads](#)
 - [Frequently Asked Questions \(FAQs\)](#)
 - [Related Sites](#)
- **University-Focused Activities**
 - [Facilities](#)
 - [Communications - Voice and Data](#)
 - [Libraries](#)
 - [Purchasing](#)
 - [University-Wide Applications](#)
 - [Public Safety](#)
- **School/College/Division-Focused Programs**
 - [Desktop Computers](#)
 - [Methodology](#)
 - [Frequently Asked Questions \(FAQs\)](#)
 - [Contacts](#)
 - [Databases \(Restricted\)](#)
 - [Other Sites](#)
 - [Downloads](#)
 - [Lab equipment](#)
 - [Methodology](#)
 - [Frequently Asked Questions \(FAQs\)](#)
 - [Contacts](#)
 - [Databases \(Restricted\)](#)
 - [Other Sites](#)
 - [Downloads](#)
 - [End-User Applications](#)
 - [Methodology](#)

Y2K General Information

This page provides general information about the Y2K process being followed at Wayne State University. For more detailed information about specific areas, please visit the links available from the Y2K Home page.

Charter for the Year 2000 effort at Wayne State University

- | | |
|--|---|
|  | Organizational structure of the Y2K effort at Wayne State University |
|  | Committees and database of S/C/D Project Sponsors and Project Leaders |
|  | Project Leader Training materials |
|  | Frequently asked questions about the Year 2000 Problems |
|  | Lists of other sites related to Y2K |

Copyright ©1999 Wayne State University

*This web site is maintained by WSU's Y2K Implementation Committee
Please [contact us](#) with any comments or suggestions
Last modified on January 25, 1999*

Mr. HORN. Well, we thank you for that. Let me just ask a couple of questions. On the 3,300 systems at the departmental level, are a lot of those faculty personal computers that can tie into the University in one way or the other?

Mr. JOHNSON. No, those are mainly the PCs, individual systems. What I was talking about was essentially business systems such as spreadsheets in departments. We have used Focus as a report generator, so there are a lot of Focus programs we have had problems with and so on down the line.

Mr. HORN. You have a very fine medical school, have you got a hospital that goes with that?

Mr. JOHNSON. No, the hospital is separate, that is the Detroit Medical Center, which has the affiliation with Wayne State University.

Mr. HORN. So you do not have a problem on worrying about an emergency room or anything.

Mr. JOHNSON. No, I have had that in a previous incarnation, but fortunately not in this one.

Mr. HORN. And you got into another incarnation fast, huh?

Mr. JOHNSON. That is right.

Mr. HORN. I can understand that.

Mr. JOHNSON. Actually, before we looked at like the operating room and we found 320 embedded devices in there.

Mr. HORN. Yeah. Well, my impression is, and we will hear from Mr. Potter, to see if my impression is right, is that there has been very good cooperation in terms of a national Website and all that in equipment. So Don Potter, Southeast Michigan Health and Hospital Council, you are going to bring all the knowledge to us in this area.

Mr. POTTER. I will be glad to do so, Mr. Chairman, thanks very much for having me here this morning and thank you for coming to town to gather the information that hopefully will be helpful to you and your colleagues in Washington as we tackle this challenge together.

Mr. HORN. It will be.

Mr. POTTER. My hope this morning is to provide a sense of what our hospitals and health systems in southeast Michigan have done, are doing and will do to combat the dreaded millennium bug to ensure that their operations are uninterrupted come New Years Eve 1999. I would also like to provide thanks for what you and your colleagues in the Congress have done to date to ease this effort and to provide recommendations on what you can and should consider for future assistance to our hospitals as they complete their efforts on this major issue.

By way of background, you should know that the hospitals and health systems in southeast Michigan are a relatively consolidated group with more than 90 percent of our 55 hospitals as part of broader health systems, so that centralized talents and capabilities have assisted in developing consistent programs, able to deliver consistent results with inherent economies in the Y2K issue.

Our hospitals are all organized as not-for-profit entities with community service as their primary missions. And they have been involved in Y2K planning from about 1997 forward, is our informa-

tion at this stage, and feel very confident that things have been moving along well.

The focus of their activities of course has had to be internal on the information systems they have, their medical equipment and devices and their facilities, with the external focus on suppliers and device manufacturers, insurance companies, certainly the Medicare program at the Federal level has been a concern just in terms of basic cash-flow for our hospitals to make payroll, and we are confident that you have taken care of a number of those concerns at the Federal level.

We have heard and had some meetings locally with our utilities, collective activity on the part of all of our hospitals and health systems through our hospital council, but we of course have police and fire and ambulance services and other external publics that are important as well.

By way of contingency plans, please know that our hospitals and health systems are in the business of dealing with emergent conditions and the unexpected on a routine basis. They are used to mobilizing quickly in the face of natural disasters and human carnage. They routinely hold drills to ensure that such mobilizations are successful and that no stone is left unturned in appropriate preparation for disasters that seldom happen. There is no reason to believe they will not be ready for the year 2000, whether or not every medical device in their facilities is Y2K compliant. Further, patient safety is the highest priority for our hospitals and health systems and their ultimate contingency plan is to have caregivers at the bedside of all patients as they do 24 hours a day, 7 days a week, 365 days a year.

Should a medical device turn out to be non-compliant even after testing, it is very likely that the ramifications will be limited, because it is the hospital's people who take care of patients, not a hospital's medical devices.

In many ways, it is fortuitous that the Y2K millennium bug dilemma is focused on New Years Eve 1999. This is a time of the year when the hospital census is the lowest and only the sickest patients remain in our hospitals. All of our hospitals and health systems have advised our office that they are examining a range of options, but all have told their employees, as others you have heard from this morning, not to plan vacations for this coming holiday season, as they have in the past. They are planning to have staff at the bedside of every patient where a medical device is in use and the manpower pool will be significant.

Remaining concerns that our hospitals have in becoming Y2K compliant include a reliance on manufacturers of products and the role of the FDA in assisting them. Our hospitals have historically and continue to rely on manufacturers for representation of the fitness and safety of their products. The FDA's Y2K guidance to manufacturers emphasizes the responsibility of manufacturers for their products' Y2K compliance and safety. The FDA has also stressed that the technical know-how for determining the compliance status of devices rests with the manufacturers.

A challenging question that hospitals face is whether to undertake independent testing of their medical devices and equipment. And this is a decision that must be made with the judgment of

those at each hospital and health system, based on whether clear and complete information on the device's Y2K compliance status has been obtained from the manufacturer. External guidance from national resources suggests that the testing a provider can accomplish is superficial and may provide false assurances about compliance in a wholly different set of problems.

Although a few hospitals nationally have identified discrepancies between what some manufacturers have reported in their own tests of medical equipment, the numbers of these occurrences is reportedly very small and none are mission critical.

The FDA has taken a leadership role nationally in working with the manufacturers to encourage their provision of complete lists of individual products that are Y2K compliant. It is critical that the FDA continue to monitor the reporting of manufacturers about these devices and equipment because they have the expertise, resources and authority to ensure that their products are safe and reliable.

At the same time, our national association is encouraging the FDA to play a rumor-control role, monitoring such arenas as the Internet and the media to make sure that information that circulates about the effects of Y2K on medical devices and equipment is accurate and corrected when it is wrong.

Liability matters are another concern for our hospitals. A dubious distinction that has haunted our hospitals and health systems in southeast Michigan for a number of years is that they pay some of the highest, if not the highest, medical liability insurance premiums in the country. The history and the culture of Detroit as the home of the auto manufacturers has resulted in an extremely active plaintiffs' bar and a very high propensity of the public to bring suit to seek redress for any wrong they perceive to have occurred.

Our hospitals are not able to ultimately face the Y2K challenge alone, they rely on medical device manufacturers as well as vendors and suppliers who have ultimate influence over the manner in which their services are provided to the people they serve.

Our hospital Y2K compliance programs have resulted in thousands of letters being sent to manufacturers, vendors and suppliers to ascertain whether their services and equipment are Y2K compliant. Unless the hospitals are provided the necessary and truthful information from these external sources, they will be in a position of facing uncertain circumstances, which could result, unfortunately, in patient harm, though that is clearly not a high probability.

Nonetheless, in spite of all that is being done, problems could still arise and our hospitals understand and appreciate the desire to avoid litigation. Resources diverted from serving patients are resources lost to the mission of our hospitals. That is of utmost importance. It is therefore important that our hospitals remain on a level playing field when defending personal injury cases. They must retain all of their current rights to take legal action against a vendor or a manufacturer whose product is involved in a claim. It is our hope that proposals entertained by Congress to address the liability matter relative to Y2K issues not create a disadvantage for our hospitals because it is essential that if a hospital is sued by a patient for a Y2K-related event, explicit language must

be included in any congressional proposal to ensure that the hospital has the same recourse against a vendor or a manufacturer that it has today. H.R. 775 recently passed by the House does this and we encourage you to maintain that posture.

Our third concern is the issue of costs. Our hospitals in southeast Michigan have expended close to \$150 million thus far on Y2K compliance. It appears that nearly half of those expenditures have been devoted to upgraded equipment, which will result in enhanced efficiency on their behalf. Nonetheless, the unplanned nature of this expenditure at a time when our hospitals are facing unprecedented challenges from all who purchase and pay for health care is presenting great challenges.

With respect to the role of Congress, we would like to thank you and your colleagues, Mr. Chairman, for the passage of the good samaritan legislation that has shielded from liability those who would work together, and we have competing hospitals and health systems working together locally on this in part as a result.

As I have previously alluded, we would encourage you to provide the FDA the resources and impetus necessary to enforce its requests for information from medical device manufacturers and to serve a rumor-control function regarding those devices. Further, we support a recent proposal by John Koskinen, chairman of the President's Council on Y2K Conversion, that mentioned the possibility of creating a contingency fund which States, in the case of Medicaid programs for example, or hospitals, could draw moneys needed to continue operating in case of Y2K disruption.

And finally, Medpac, the congressionally developed oversight body for the Medicare program, has included in its recommendations for fiscal year 2000 funding an additional one half of 1 percent payment increase to hospitals to cover their Y2K compliance costs. We would encourage you and your colleagues in Congress to support that as well.

Thank you very much for the opportunity to be here. I think I can convey that our hospitals and health systems have been aggressively working on this problem for at least 2 years and are feeling relatively confident about their positions today.

[The prepared statement of Mr. Potter follows:]



SOUTHEAST MICHIGAN HEALTH & HOSPITAL COUNCIL

DONALD P. POTTER, PRESIDENT

Testimony
of the
Southeast Michigan Health and Hospital Council
before the
Subcommittee on Government Management, Information and Technology
Committee on Government Reform
of the
United States House of Representatives
on
The Impact of the Year 2000 Computer Problem on Hospitals and Health Systems
July 9, 1999

Mr. Chairman, I am Donald Potter President of the Southeast Michigan Health and Hospital Council, the trade association representing the interests of the more than 50 acute care general hospitals and health systems located here in southeast Michigan and which serve nearly half of the people of the state of Michigan. It is a pleasure to have you and your colleagues here in Detroit today and I am honored to appear this morning on behalf of our hospitals. We are delighted that Congress has shown the concern that you have shown in the Y2K matter and welcome your further insights and assistance.

- My purpose here today is two fold:



SOUTHEAST MICHIGAN HEALTH & HOSPITAL COUNCIL
24725 W. Twelve Mile Road • Suite 104A
Southfield, Michigan 48034-8345
(810) 358-2950 • Fax (810) 358-1098

- To provide a sense of what our hospitals and health systems in southeast Michigan have done, are doing and will do to combat the dreaded "millennium bug" to insure that their operations are uninterrupted by the calendar change that will take place on December 31, 1999.
- To provide thanks for what you and your colleagues in Congress have done to date to ease this effort and to provide recommendations on what you can and should consider for future assistance to our hospitals as they complete their efforts on this major issue.

1) Hospital Preparation and Progress to Date:

By way of background, you should know that the hospitals and health systems of southeast Michigan are a relatively consolidated group with more than 90% of our hospitals as parts of broader health systems so that centralized talents and capabilities have assisted in developing consistent programs able to deliver consistent results with inherent economies. Our hospitals are all organized as not for profit entities with community service as their primary missions. They have all been involved in Y2K planning for some time already and significant efforts have been put forth across the board here in southeast Michigan to ensure that no stone remains unturned in their attempts to ensure a smooth transition for their patients and communities they serve into the new millennium.

A) Steering Committee Formation:

Our information from our members points out that nearly all began the formation of Y2K steering committees as early as January of 1998 and program planning and development has been ongoing since then.

B) Outside Assistance:

Our hospitals have received significant assistance from their American Hospital Association nationally and the Michigan Health and Hospital Association as well as the Catholic Hospital Association and other groups of hospitals with which they have relationships on a national or statewide basis. Manufacturers of medical devices have in many cases been more than helpful in assisting our hospitals in their Y2K compliance planning. And, it is no secret that the marketplace has developed numerous opportunities to engage consultants to assist in Y2K planning and many of our hospitals and health systems have engaged external consultants for such assistance.

C) General Approach:

In working with our hospitals and health systems to promote cooperative endeavors, we have learned that each of their programs for Y2K compliance has been developed with inclusion of the following steps or some variation thereof:

- Inventory
- Risk identification
- Compliance assessment
- Planning
- Remediation
- Testing/validation
- Contingency planning
- Communications planning

D) Focus of Compliance Programs

Once again with the assistance of external parties and developing approaches to Y2K compliance programs, our hospitals and health systems have generally developed their programs around the following foci:

(1) Internal Focus:

- A) Information Systems
- B) Medical Equipment/Devices
- C) Facilities - Heating and Cooling,
Telecommunications, Elevators, Security, etc.

(2) External Focus:

- A) Suppliers/Manufacturers
- B) Insurance Companies - HMOs - Medicare/HCFA
Financial Institutions
- C) Utilities

- D) Ambulance Companies
- E) Police and Fire

(3) Contingency Plans:

Please know that our hospitals and health systems are in the business of dealing with emergent conditions and the unexpected. They are used to mobilizing quickly in the face of natural disasters and human carnage. They routinely hold drills to ensure that such mobilizations are successful and no stone is left unturned in appropriate preparation for disasters that seldom happen. There is no reason to believe that they will not also be ready for the year 2000 whether or not every medical device in their facilities is Y2K compliant. Further, patient safety is the highest priority for our hospitals and health systems. Their ultimate contingency plan is to have care givers at the bedside of all patients - as they do 24 hours a day, seven days a week 365 days a year. Should a medical device turn out to be non-compliant even after testing, it is very likely that the ramifications will be limited because it is a hospital's people who take care of patients not a hospital's medical devices.

In many ways it is fortuitous that the Y2K "*millennium bug*" dilemma is focused on New Year's Eve 1999. This is the time of the year when the hospital census is the lowest and only the sickest of patients remain in our hospitals. All of our hospitals and health systems

advised that they are examining a range of options and all have advised their employees not to plan vacations for this coming holiday season as they have in the past. They are planning to have staff at the bedside of all patients who are reliant on medical devices to ensure that no malfunctioning device will result in impeded medical care.

In May of 1999, our Council hosted a Y2K readiness meeting with our members and representatives from the utilities operating within our region. A dialogue has been developed with all major utilities and efforts are merging community-wide to ensure that hospitals are provided priority for electricity, water and natural gas should any problems develop with our utilities and their ability to supply the overall region. The utilities have expressed confidence that their Y2K planning is moving along nicely and our hospitals all have back up power systems in place to enable them to address any electrical failure.

(4) Communication Plans:

Each of our hospitals and health systems has as part of their Y2K compliance plan a communication plan for all internal and necessary external publics to enable them to be aware of contingency plans and of work done to date.

E) Remaining Concerns:**(1) Reliance on Manufacturers/Role of the Food and Drug Administration**

Our hospitals have historically and continue to rely on manufacturers for representation of the fitness and safety of their products. The Food and Drug Administration's Y2K guidance to manufacturers emphasizes the responsibility of manufacturers for their product's Y2K compliance and safety. The FDA has stressed that the technical know-how for determining the compliant status of devices rests with the manufacturers. A challenging question that hospitals face is whether to undertake independent testing of their medical devices and equipment? This is a decision that ultimately must be made with the judgment of those at each hospital and health system based on whether clear and complete information on the device's Y2K compliance status has been obtained from the manufacturer. External guidance from national resources suggests that the testing a provider can accomplish is superficial and may provide false assurances about compliance and a wholly different set of problems. Although a few hospitals nationally have identified discrepancies between what some manufacturers have reported in their own tests of medical equipment, the number of these occurrences is reportedly very small and none are mission critical.

The Food and Drug Administration has taken a leadership role nationally in working with manufacturers to encourage their provision of complete lists of individual product models that are Y2K compliant. It is critical that the FDA continue to monitor the reporting of manufacturers about their medical devices and equipment because they have the expertise, resources and authority to ensure that the products are safe and reliable. At the same time our national association is encouraging the FDA to play a "*rumor control*" role monitoring such arenas as the Internet and the media to make sure that information that circulates about the effects of Y2K on medical devices and equipment is accurate and corrected when it is wrong.

(2) Liability Matters:

A dubious distinction that has haunted our hospitals and health systems in southeast Michigan for a number of years is that they pay some of the highest medical liability premiums in the country. The history and the culture of Detroit as the home of the auto manufacturers has resulted in an extremely active plaintiff's bar and a very high propensity of the public to bring suit to seek redress for any wrong they perceive to have occurred. Our hospitals are not able to ultimately face the Y2K challenge alone. They rely on medical device manufacturers as well as vendors and suppliers who have ultimate influence over the manner in which their services are provided to the people they serve. Our

hospital Y2K compliance programs have resulted in thousands of letters being sent to manufacturers, vendors and suppliers to ascertain whether their services and equipment are Y2K compliant. Unless the hospitals are provided the necessary and truthful information from these external sources they will be in a position of facing uncertain circumstances, which could result unfortunately in patient harm, though that is clearly not a high probability. Nonetheless, in spite of what all is being done, problems could still arise. Our members understand and appreciate the desire to avoid litigation. Resources diverted from serving patients are resources lost to the mission of our hospitals. That is of the utmost importance. It is therefore important that our hospitals remain on a level playing field when defending personal injury cases. They must retain all of their current rights to take legal action against a vendor or manufacturer whose product is involved in a claim. It is our hope that proposals entertained by Congress to address the liability matter relative to Y2K issues do not create a disadvantage for our hospitals because it is essential that if a hospital is sued by a patient for a Y2K related event, explicit language must be included in any Congressional proposal to ensure that the hospital has the same recourse against a vendor or manufacturer that it has today. H.R.775 recently passed by the House does this and we encourage you to maintain that posture.

3) Costs:

An informal survey of our members suggests that they have expended approximately \$150 million in their Y2K compliance planning to date. The good news is that nearly ½ of those expenditures has been devoted to the purchase of upgraded equipment to replace that which is not determined to be Y2K compliant. In most cases this equipment has enhanced the efficiency and effectiveness of the services they offer. Nonetheless, the unplanned nature of this expenditure at a time when our hospitals are facing unprecedented challenges from all who purchase and pay for health care is presenting great challenges.

2) Role of Congress:

As I have described, our hospitals and health systems have been diligent and extremely serious in the planning and preparation for the Y2K millennium bug challenge. They are steadfast in their view that patient care is their mission and patient care will not be compromised by this particular dilemma and they will be prepared when the time comes to welcome the new year with minimal - and we hope *no* disruption. I have alluded in my comments today to further roles that congress can play in assisting our hospitals in ensuring this outcome. On behalf of our hospitals I would like to thank you and your colleagues Mr. Chairman for the passage of the "*Good Samaritan*" legislation that will shield from

liability, those who would share information in good faith to work together on the Y2K issue. It has enabled our hospitals and health systems to sit down together at their Hospital Council meeting table with no concern for anything but the welfare of those they serve.

As I have previously alluded, we would encourage you to provide the Food and Drug Administration the resources and impetus necessary to enforce its requests for information from medical device manufacturers and to serve a "*rumor control*" function regarding those devices.

Further, we support a recent proposal by John Koskinen, Chairman of the President's Council on Year 2000 Conversion, that mentioned the possibility of creating a contingency fund from which states (in the case of Medicaid for example) or hospitals could draw monies needed to continue operating in case of Y2K disruption.

Finally, Medpac, the Congressionally developed oversight body for the Medicare program, has included in its hospital prospective payment system update recommendations for FY2000 an additional 0.5% to cover hospital' costs of becoming Y2K compliant. In light of the expense that has been incurred by our hospitals and the continuing pressure on their costs, we would respectfully request that you and your Congressional colleagues increase the mandated

hospital update factor by 0.5% to reflect this recommendation from this important body.

Conclusion:

I have had the pleasure and the honor of serving as the President of the Southeast Michigan Health and Hospital Council for the past 16 years. The great people who lead and work in our hospitals and health systems in this region have been most serious and diligent in taking the "millennium bug" as a serious matter and making it a matter of highest importance to the continuation of their missions of serving the health care needs of the people of our region. I am advised that most hospitals and health systems have Y2K compliance planning reports routinely on their board meeting agendas and the dialogue that we have been able to engender with utilities and other external forces suggests to me that this effort has been nothing short of miraculous in engendering cooperation among often otherwise competing entities. The assistance that we have received from you and your colleagues in Congress, from the Administration, from our manufacturers, suppliers, and vendors has been unprecedented in my experience. I join you in the hope that what we are dealing with is minimal or non-existent when new year's eve comes this year. I hope that as you move across the country with your hearings that you will recall that southeast Michigan hospitals are but one group of the nation's five thousand hospitals that have taken this matter seriously and devoted significant time, effort and resources to ensuring that patient safety and care remains uncompromised. In recent months our hospitals and health systems have noted what they

believe erroneous information reported in the popular media about their preparation for Y2K and would hope that as you gather information from other groups in your efforts, that you would work as well to dispel any notion that our hospitals are not up to speed and diligently preparing for this hopeful non-event. Thank you for coming to our fine city and thank you for the opportunity of presenting these remarks to the subcommittee today.

Mr. HORN. Now the hospitals have a Website, do they not, where they can check out equipment against it in terms of the manufacturer's name, the model number and all that, so they do not have to be repeating this all over America?

Mr. POTTER. This is being assisted by the FDA in their gathering of information from the manufacturers, but also by the American Hospital Association as well. My information is that about 70 percent of that equipment is easily accessible in terms of information right now.

Mr. HORN. That is very helpful.

Our last witness on this panel is Dan McDougall, who is the director, southeast Michigan information center for United Way.

Mr. MCDOUGALL. Thank you for the opportunity to speak today, and especially today on the last panel, because I think I represent an industry that is very different than the industries you have heard from earlier today, and that of course being the human services sector that provides support services to people in our community.

I thought what I would do today is talk to you not so much about how our individual United Way is dealing with Y2K internally, but how the human services sector in southeast Michigan is dealing with the Y2K issue and kind of what we see as some of the possible solutions, and I will try to summarize my report.

Clearly, the non-profit sector does not have the dollars and the resources behind it that some of the corporations that we have heard from today do. Our first—at United Way, our first attempt at addressing the issue among the smaller non-profits in our area was to send a letter out to non-profits in September of last year, kind of outlining the Y2K issue and asking folks to start looking at it in their individual organizations.

In addition to that, we worked with George Surdu from Ford Motor Co., who was here earlier today, to develop a Y2K handbook for non-profit organizations. We have heard a lot of people talk about the Good Samaritan Act and I keep thinking of that when I talk about our relationship with Ford Motor Co., because it is only because of Ford Motor Co. that we have been able to address the Y2K issue in the non-profit sector locally here.

Since September though, unfortunately what we have found is that non-profits just are not looking at the issue serious—the Y2K issue seriously. And part of this has to do with the culture of the small non-profit community. Non-profits are expected to operate with budgets far less than the for-profit sector, and very often the funding distribution to non-profit organizations stipulates that money cannot be spent on capital, things such as computer equipment. The result is that most non-profits are operating with computer systems that are the castaways from the for-profit sector. So although we love it when the big corporations give us their old computers, what is happening now is that the corporations are giving us their computers that are going to crash in January. [Laughter.]

We like to take things from everybody, but unfortunately, this one is not helping.

So unfortunately, we have this cyclical nature of the non-profit sector not getting the funding to deal with the issue and then also

non-profits just being too burdened by the day-to-day tasks that they have to really look at the Y2K issue. It is just not in our culture to deal with technology very much.

Late last year, the Nonprofit Times and Gift in Kind International did a national survey of the non-profit sector in technology, with a little bit of focus on the Y2K issue and what they found is that non-profit organizations with an annual budget of less than \$1 million are the most susceptible to issues with respect to Y2K and that is because most of these organizations are dealing with this loaned equipment or donated equipment and they are usually processors that are 386 level or below. Sixty-three percent of the non-profits in that survey said that they have absolutely no money budgeted for technology or technology training, no budget at all. So they are really depending on Board members who give their old computers and who come and teach classes to their staff.

And then also, 40 percent of the respondents in that survey stated that their biggest roadblock to Y2K issues was money. And of course we always want to focus on the equipment aspect of the Y2K issue for non-profits but it is also training and technology planning. So we are really seeing that the problem is more than just hardware for us.

In terms of our local picture, in the seven-county area that we call southeast Michigan for the purposes of United Way, there are a little over 6000 registered non-profits and those are of the size that they are a million budget or less, which is the focus that we have. If we were to say that one—if we looked at the trends in terms of the kinds of computers that smaller non-profits have, replacing one computer for each organization would cost a little over \$1.3 million and that does not include training and updating of software and things like that.

So in our mind, it is really an issue of focusing on a cadre or a mosaic of services and hardware issues that non-profits have. And so what I would like to do is talk about a program that we have locally that we think works, but of course is not big enough.

We work with a national project called Team TECH which is a collaborative arrangement between IBM, United Way and the Corp. for National Service. We use AmeriCorps volunteers at United Ways throughout the country to distribute IBM hardware and also provide technical training and technical planning. In Detroit, this has made a huge impact on the ability of small non-profits with one and two staff members to start looking at technology in new ways and to address the Y2K issue in their organization. And so one of the things that we are looking at is because of the Y2K issue, we have had organizations like Ford and IBM come to us and want to provide us technical assistance so that we can help non-profits do things better. And so for us, coming from a culture of not using technology very much, we are seeing this issue as an opportunity and we would like to say that we would like to take the Y2K lemon and try to make some technology lemonade out of it for non-profits.

So what we are looking forward to is the results of this hearing helping us bring together some of the other good samaritans in our community to help the non-profit sector.

I will conclude my testimony there.

[The prepared statement of Mr. McDougall follows:]

**Prepared Statement to
The House Task Force on the Year 2000**

Dan McDougall
Director,
Southeastern Michigan Information Center
United Way Community Services
1212 Griswold
Detroit, Michigan 48226
(313) 226-9272
dmcdoug@uwcs.org

July 9, 1999

Good morning. My name is Dan McDougall, and I am the Director of the Southeastern Michigan Information Center, a program of United Way Community Services, here in Detroit. I appreciate the opportunity to discuss the Year 2000 issue today – especially as it relates to the non-profit sector. At United Way, our efforts focus on human service organizations – a group that is traditionally behind in the use of technology, and is woefully ill-prepared for the Year 2000.

I'd like to utilize my time today to summarize our understanding of the impact of the Y2K issue on human service organizations, and to briefly outline the success of one local project that brings together the Corporation for National Service, the United Way, and IBM to address the issue of technology among non-profits.

In September of last year, United Way Community Services CEO Virgil Carr and Chief Operating Officer Geneva Williams issued a letter to area nonprofits about Year 2000 (Y2K) computer issues. In that letter they emphasized the potential impact of Y2K on the ability to serve our clients, volunteers, and donors, and conduct "business as usual." Realizing informing nonprofits of the looming problem was only the beginning of the remedy; a Y2K handbook was created with the assistance of Ford Motor Company and Comerica that accompanied the letter. Additionally, three community forums were held to educate nonprofits and provide a detailed plan for dealing with the dilemma.

Nearly ten months later there are still concerns that nonprofits are ill-prepared for Y2K. The Associated Press wrote recently that, "big business and government may be well on their way toward fixing the so-called Y2K computer bug. But it's likely to be a bumpier ride for cash-strapped nonprofit agencies." Nonprofits tend to be short-staffed, have limited resources, are overworked, and are mission driven. If Y2K is not an immediate threat to putting food on a shelf or beds in a homeless shelter, nonprofits tend to continue focusing on what they are doing now and deal with Y2K later. In addition to not rushing to deal with Y2K problems in their computers, many nonprofit agencies haven't begun thinking about how Y2K could create extra demand for their services. Nonprofit social-

service agencies, which provide for the nation's neediest citizens and could be called upon to help others if Y2K disasters occur, may be among the most vulnerable to Y2K.

The Nonprofit Times/Gift In Kind International - Nonprofit Sector Technology Survey attempted to assess, nationally, nonprofit readiness for Y2K. The study revealed that there is much disparity in the degree of preparedness. The nonprofits that have yet to take action are smaller generally in size. The nonprofits with budgets under \$1 million are especially vulnerable because these social service organizations are most likely to have 386-level and older computers as their primary computing systems.

The most significant roadblock to becoming Y2K compliant experienced by most nonprofits is the lack of technical expertise to assess the organization's computer and office equipment systems; conduct the review necessary to determine vendor and other external operations problems, and; find and install new equipment and train staff. Sixty-three percent of nonprofits have no money budgeted for computer training, and lack of funds was identified as a major roadblock to Y2K compliance by 40 percent of the nonprofits in the national survey. Cost restrictions imposed by funders often prevent organizations from making required upgrade purchases, and obtaining the technical expertise to manage the process, test office equipment, and train staff.

The price tag for Y2K compliance by nonprofits has yet to be determined; however, there is no question that the bill will be substantial. The factors effecting the cost burden to nonprofits are numerous. It is natural to focus on the issue of replacing antiquated hardware. This is a significant issue among non-profits, which often rely on antiquated cast-away computers from the corporate sector. The cost of the Y2K dilemma, however, does not end after upgrades and the purchase of new computers. Staff will have to be trained to use the updated equipment and must quickly learn new software that is essential to the operation of the organization.

Again, the Nonprofit Times' survey reveals that those non-profits most vulnerable to the Y2K issue are those with budgets less than \$1 million annually. In addition, the survey identified trends in the level of hardware antiquity among these nonprofits. When these trends are applied to the more than 6,000 nonprofits of this size in the seven-county region surrounding Detroit, the Y2K issue seems massive.

Even if we allow that each such organization has only one computer, the cost for evaluation, upgrading and replacement of computer systems vulnerable to the Y2K "bug," is more than \$1.3 million. This is a conservative estimate of only the hardware-related issues for non-profits in southeastern Michigan. It does not address issues related to training and technical assistance.

A Local Model for Success

While these numbers are daunting, there are many local and national efforts designed to improve the way that non-profits utilize technology – especially in the face to the Year 2000 issue. I'd like to close by highlighting one such project: Team TECH.

Team TECH is a national initiative bringing together the United Way, IBM, and AmeriCorps*VISTA. This project is a model of how a collaborative, public/private effort can address the technology issues plaguing the human service sector.

Team TECH places teams of AmeriCorps*VISTA volunteers throughout the nation at United Way offices. Throughout the 15 Team TECH sites, AmeriCorps*VISTA volunteers help provide technical planning and assistance, training, and hardware and software upgrades to non-profits. In Detroit, the project has had a significant impact on the ability of smaller non-profit organizations to utilize technology to improve the lives of people in our community. Beyond the Y2K issue, this project has truly altered the way that local, small non-profits view the use of technology in their day-to-day work.

Based on the lessons learned in the Team TECH project, I'd like to suggest that the plan for helping non-profit organizations face the Year 2000 issue – and the broader technology issue – must go beyond simple hardware replacement. Non-profit organizations lack the basic technology training and planning skills necessary to sustain any "quick fixes" that come along as a result of the Y2K crisis. A coordinated response that includes hardware and software, technology planning, and technical training is the responsible answer to the crisis at hand. Rather than putting a hardware band-aid on the problem, we at United Way Community Services are hoping that the result of hearings like this one will be the taking of the Y2K lemon, and making technology lemonade.

Mr. HORN. Well, thank you very much. Let me ask the panel generally a couple of questions. Let us just say when did it start, some of you told me and I just want to get it on the record. Mr. Roosen, when did you start this Y2K adaptation and awareness and all the rest of it?

Mr. ROOSEN. 1996.

Mr. HORN. 1996? And then when, early in 1996 or later?

Mr. ROOSEN. We started, as I recall, in our Information Technology Department somewhere in mid-1996.

Mr. HORN. OK, we will say June then.

Mr. ROOSEN. That would be fair.

Mr. HORN. When did the gas company find time to start on it?

Mr. LOZANO. We started replacing our business systems back in 1995, but instituted our Y2K office corporate-wide in 1997.

Mr. HORN. 1997, 1995.

And then how about the Wayne State University, when did you start?

Mr. JOHNSON. We started in 1996 with awareness and we were budgeted in fiscal year 1997 which starts October 1st.

Mr. HORN. And then how about the Health and Hospital Council, when did they start on this, roughly?

Mr. POTTER. Speaking collectively on behalf of all the hospitals in the region, Mr. Chairman, we are seeing late 1997 and early 1998 for the system-wide formation of steering committees to actually take on the matter.

Mr. HORN. How about the non-profits with the United Way?

Mr. MCDUGALL. Well, it varies from non-profit to non-profit. Our United Way started focusing on our internal systems in late 1996, but we just started working with assisting other non-profits in middle to late 1998.

Mr. HORN. Now that you have a lot of experience in this area, we can start down the line again, what do you wish you had done that you did not do and what would be No. 1 for you next time around, if we ever had this experience? Mr. Roosen, what do you think?

Mr. ROOSEN. I think as one of the earlier witnesses said, the inventorying your assets and knowing what you have makes it a lot easier to do something with them and I would say that would be the one large learning if you had to do it over again.

Mr. HORN. How about you, Mr. Lozano?

Mr. LOZANO. With me is Tom Motsinger, director of technology and information systems, and we had a discussion about this and we just echo that sentiment, that inventorying—

Mr. HORN. Well, you are the expert, Mr. Motsinger, what do you think?

Mr. MOTSINGER. That is correct, the inventory has been our biggest issue. As was said earlier by the auto industry, the—you are definitely surprised by the number, the count of pieces of equipment and how much is out there that you really do not know about.

Mr. HORN. Does that mean that sort of in the future everybody is going to have a going, running inventory.

Mr. MOTSINGER. Ongoing.

Mr. HORN. Yeah, ongoing. How about it, Mr. Johnson, what has been Wayne State's experience with—

Mr. JOHNSON. Well, first, I would replace probably another core system rather than remediate it. I would echo what everyone else said; the other factor I would mention is keeping up to date with software because when you bring in the compliant software, if you are not up to date, you have got to bring it up to date and then go from there. And the third I think would be a broader national awareness. It has been pretty late for people to discover the year 2K problem is a much broader problem than an information technology problem. And it has only been recently that we have really been able to get the attention of the skeptics that there is a problem and they need to do something about it.

Mr. HORN. Yeah.

Mr. JOHNSON. One thing fueling that was obviously some Federal agencies saying you have to assure compliance for funding.

Mr. HORN. We urged the President to do just that in 1997 and he did give the speech to the National Academy of Sciences in the summer of 1998, I believe, and of course they were the last people that needed to be educated, they already knew about it. And I think there are three speeches that have been given, so the bully pulpit has not been used very much, as Theodore Roosevelt called the Presidency, and it is too bad. But you are right, general awareness.

And what would you say on the issue that you would rather do first next time and you did not do it for one reason or the other?

Mr. POTTER. I think our inventory has turned out to be relatively solid, thank goodness, in our hospitals and health systems. The big issue that jumped up was really the cost issue. Health care reform did not die in Congress in 1995, it switched its colors and our hospitals here in Detroit have had 5,000 layoffs in the last year just to live with the dollars they have. So to factor \$150 million out of their patient care dollars has not been an easy proposition, to be spending money on upgrading information systems when they could be taking care of patients.

So probably the surprise, at least in the short run, was what it did cost ultimately for them to update their systems and how to accommodate that in the short run.

Mr. HORN. That is a very interesting point. In terms of Medicare, is there sort of an administrative base that is recognized as part of your cost structure?

Mr. POTTER. Yes, we are under Federal price controls and Medicare pays hospitals a given amount to take care of a patient of a given diagnosis and that amount is updated on an annual basis. In my testimony, I alluded that there is this group called MedPac that Congress appoints to make recommendations through the appropriations process to determine what should be the annual change, if any, in prices. Unfortunately, it is going down rather than up right now, by virtue of the Balanced Budget Act of 1997.

Mr. HORN. Yeah. Well, it is interesting because you have had an extra expense you did not know several years before, you would have, because very few people did. And has there been an adjustment in that base?

Mr. POTTER. The recommendation has been made, but it is not clear to me that the appropriations process has accommodated it this year. There is a lot of reluctance in Congress, as you well

know, to tamper with anything that came out of the Balanced Budget Act, but the Balanced Budget Act, if you may recall, cut Federal spending by \$122 billion over 5 years and \$116 billion of that came from Medicare, which is only 13 percent of the budget. And 95 percent of that came from health care service providers, not in cuts of eligibility or benefits to Medicare enrollees. So it is the providers who have got the problem.

Mr. HORN. You have made a good point and I will ask the staff to follow it up and see what is happening with the Appropriations Committees on this.

Mr. POTTER. I appreciate that.

Mr. HORN. This point has not really been raised before and so I think that is a real contribution.

Now let me ask those of you that represent various utilities, you send out sometimes monthly billings to large clientele. To what extent have you used some of that sheet that tells them what they have got to pay to educate them on the Y2K situation and to sort of reassure the citizenry that you are on top of these things, because there is a lot, as I have said numerous times, a lot of scare-mongers out there for their own delights and their own money-making, who will try to scare a lot of your customers that gee, we are not doing this, we are not doing that. You have got a lot of tort lawyers also that are sitting there salivating. And I was just curious, to what extent have you tried to educate your clientele, our fellow citizens, with this information. Mr. Roosen.

Mr. ROOSEN. Well, from Detroit Edison's standpoint, there are really three approaches. You are right, the bill stuffer is one approach, but as we all know, when we are paying our bills, a lot of times we throw that stuff away. I know I have that habit.

We have used the bill stuffer and we have done it, I believe, three times since last summer. Annually, we send out notices to our customers, we have a lot of storms in the spring, starting in about March, so we took advantage of the early storm tips to also put in a Y2K twist.

And then we have 18 offices and we have some advice to customers on preparation. We have booklets that we have made available to them.

And then third, we have a speakers corps and any time any—whether it be a garden group or a church or whatever, any time that they ask us, we volunteer a speaker to go out and do something on Y2K.

Mr. HORN. How about it, Mr. Lozano, what has been the approach?

Mr. LOZANO. Mr. Chairman, we have similar efforts as does Edison. We have had one bill stuffer that has gone out to customers and most of ours has been more responsive to the community groups and the individuals that call either through our public affairs offices or through the Y2K office, responding to individual requests for information or just verbal information or speaking before groups. As we are located throughout the State, we have been involved in multiple presentations throughout the entire State and usually in a panel type of situation involving the communication industry and local municipalities.

Mr. HORN. I do not think—let us see, did the rest of you really have that kind of communication going on? Well, hospitals send bills too, but I do not know if they want it read on anything but the bottom line when the poor patient gets it. Was that not the reason we always get rolled out of a hospital in a wheelchair, because they show you the bill on the way out? [Laughter.]

Mr. POTTER. We really do have a problem, Mr. Chairman, on this one. I learned it just a couple of weeks ago when my 73 year old mother-in-law told me there are two places she was not going to be on New Year's Eve, one was on an airplane and the other was in a hospital. And I asked "Where does this come from that it is part of the public thinking?" Whether she watches day time television or what, she at the same time asked me if I would like to go halves with her on a generator after she had purchased three cases of canned goods to put in her basement.

So we have got a real problem with the general public that needs to be dealt with and it is something that we are kind of looking at collectively in our hospital council to see what we can do as an industry.

Mr. HORN. Did you ever find out where she got her information?

Mr. POTTER. It turns out there is a—she lives in west Michigan and there are some very high profile kooks out there stirring up the pot and holding meetings and individuals are going, almost like the old time revivals. And there is this cult that has developed, of which I am afraid she is on the fringe, and Lord knows what it is going to take, but she wants to know everything I know about Y2K. And I will even give her a copy of my testimony today and see if that will help, but it has not thus far.

Mr. HORN. When we were in Topeka the other day holding a hearing our staff director happened to pick up the Kansas City Star and Ann Landers had a column in there on the scams that are being worked on senior citizens with the Y2K being it. They phone up the senior citizen and say we are the bank and we need to move your money from your account to this bond account and all. And you know, utter baloney. But people are going to be hurting senior citizens just like they do on other scams. So we need to help head that off, and the Attorney General of each State needs to really be leading that front.

Mr. Willemsen, why do you not sit in one of the Commissioners chairs here, it is a cushy one, better accommodations than you have had in most hearing rooms.

What do you make of all this and what should we discuss to get it on the record?

We are going to have to wire you for sound wherever you go.

Mr. WILLEMSSEN. Thanks, Mr. Chairman. A couple of thoughts that I thought I would raise to you that may be a little bit unique that we had not talked about at the other field hearings. One having Wayne State here, you may want to inquire about the extent of coordination that they have had with the Department of Education on their data exchanges on student loans and student grants.

And also with a representative from the hospital association, I think it is useful to point out that beyond the Website that the Food and Drug Administration has, they also plan to begin some

independent efforts on a sample of critical care life support biomedical equipment items, to independently check behind the compliance certifications of the manufacturers and see what evidence is behind that, for those critical care and life support items.

So I thought I would just raise those couple of points.

Mr. HORN. Well, those are excellent questions. Let us deal with the student loan one and student grant, the Pell grants. We are the first Congress that ever got them paid to the highest mark you possibly could have in Pell grants. So I am curious what the Department of Education is doing in relation to Wayne State University.

Mr. JOHNSON. They have an awareness program and they are one of our suppliers that assures compliance with the year 2000. We have not tested it yet.

Mr. HORN. Now they have intermediaries, do they not, that do a lot of the—

Mr. JOHNSON. Yes.

Mr. HORN. It is not directly Department of Education.

Mr. JOHNSON. It is not always done directly, the transfers, that is right.

Mr. HORN. And it is the same as Medicare in that sense, they have intermediaries between the hospitals and Medicare providers.

Mr. JOHNSON. Right. It is a very dispersed problem.

Mr. HORN. Yeah. So what has been your experience then on this situation with grants and loans, I did not quite hear that.

Mr. JOHNSON. I am not aware of a problem of non-compliance. I will not confess to being infinitely wise in this area.

Mr. HORN. Yeah, if you would ask your director of financial aid, it might be interesting and we will put it in the record at this point, if you want to write us a letter as to what the experience is.

Mr. JOHNSON. OK, I will do that.

Mr. HORN. That would be very helpful.

[The information referred to follows:]

WAYNE STATE UNIVERSITY
COMPUTING & INFORMATION TECHNOLOGY
5925 WOODWARD AVENUE
DETROIT, MICHIGAN 48202

August 9, 1999

Honorable Stephen Horn, Chairman
Subcommittee on Government Management,
Information, and Technology
Committee on Government Reform
House of Representatives
Congress of the United States

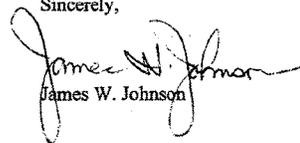
Dear Congressman Horn:

At your hearing entitled, "Oversight of the Year 2000 Technology Problem: Lessons to be Learned State and Local Experiences" held on July 9, 1999, you asked me about (p.114) the year 2000 of financial aid service providers for the Department of Education. I offer the following statement:

I have discussed the ability of the Department of Education data exchange services to operate beyond the year 2000 with Wayne State University's Director of Financial Aid, Adalberto Andino. He reports that the third party data exchange provider has tested the data exchange software for student financial aid data between the agency and Wayne State and has found the system year 2000 compliant. Any problems associated with the data exchange are not the result of the year 2000 computer technology problem.

I hope this fills in the record. I have also enclosed the edited transcript of my testimony.

Sincerely,


James W. Johnson

Mr. HORN. OK, Mr. Potter, on the Medicare/Medicaid intermediary, is there a problem there at all with the hospitals and the interactions on the computing with the State government and the Federal Government and its intermediaries?

Mr. POTTER. We have just solved another problem because we have the third intermediary—

Mr. HORN. You want to move the mic a little closer, I cannot—

Mr. POTTER. I am sorry. Our hospitals in Michigan are dealing with the third Medicare intermediary that has been used for the last 5 years. So we have just worked through another change, it is now in Wisconsin, but the technology of the day has made life a lot easier and although Medicare does not pay enough, the dollars are flowing and there are no major concerns at this point.

Mr. HORN. How about on the Food and Drug aspect of equipment that Mr. Willemssen mentioned?

Mr. POTTER. I appreciated that insight, that is new news to me and it is good news, because we do have some manufacturers that have been reluctant to even respond to mailings, and if they have, they have done so in such a manner so as to guarantee absolutely nothing. And the FDA's control over these device manufacturers is an extremely important tool to our hospitals because as I said in my testimony, they do not have the expertise to go into this machinery and remediate it and if you really do get to the point where you cannot do that and no one is responsive, then once again, you have to go buy a new piece of equipment, perhaps unnecessarily. So I am very glad to hear that.

Mr. HORN. Yes, it is a very important point and between GAO and our staff, hopefully we can get that sorted out with FDA as to what degree is this a problem, because I think that is an excellent point that Mr. Willemssen has made.

Any other thoughts, Joel?

Mr. WILLEMSSEN. I think you summed it up very well, Mr. Chairman.

Mr. HORN. Well, I want to thank each one of you. Do you have any comments you might want to make based on your colleagues' testimony?

[No response.]

Mr. HORN. It does not look like you do, so I want to thank you very much. We really appreciate it.

And I thank all that have been involved in preparing this. On our own side, we have got J. Russell George, our staff director and chief counsel is here. He is holding up that Corinthian column there that I am looking at. And Matthew Ryan is to my left and your right. He is the senior policy director involved in this type of hearing. And Grant Newman, our faithful clerk, who has probably broken his back lugging stuff around this country. Where are you, Grant? There you are in the back, the well-dressed young man. I do not think our interns are here, but they helped, and that is Lauren Lufton and John Phillips, Justin Schleuter, they are back at the office.

And then for Wayne County, we particularly appreciate the cooperation we have had from your Assistant County Executive, Suzanne Hall, she was an excellent witness a few weeks ago in Washington; and Sue Hanson, deputy director, Y2K Program Office; Al

Montgomery, clerk of the Commissioners; and Mr. Cavanaugh, county commissioner, and—Mr. Christopher Cavanaugh. We really appreciate them, and we appreciate, as we said earlier, George Cushingberry, Jr., county commissioner, and his help.

And then we had also your Wayne County manager of information technology for the Commission, and that is Orlando Gloster, and we appreciate all that he has done.

And last but not least, because he has got the big workout in one of these hearings, is Bill Warren, the court reporter that took all this down. I still do not understand how they can do it that fast and listen to the next word, but that is OK, the transcript comes out fine and we appreciate it.

So with that, this committee, which began in Topeka and was also in Naperville, IL outside of Chicago in recess, and it was recessed to Detroit and it is over now and so we will adjourn this meeting. Thank you.

[Whereupon, at 12:14 p.m., the subcommittee was adjourned.]

