AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

# THE YEAR 2000 PROBLEM, INDIANAPOLIS: A LOCAL RESPONSE

## HEARING

BEFORE THE

## COMMITTEE ON GOVERNMENT REFORM

## HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

FIRST SESSION

APRIL 19, 1999

**Serial No. 106–15**

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
57–495 CC WASHINGTON : 1999

COMMITTEE ON GOVERNMENT REFORM

DAN BURTON, Indiana, *Chairman*

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

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

---

BERNARD SANDERS, Vermont (Independent)

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

# CONTENTS


| | Page |
|---|---|
| Hearing held on April 19, 1999 | 1 |
| Statement of: | |
| Cottey, Jack L., sheriff, Marion County, IN; John Spahr, deputy fire chief, Lawrence Township Fire Department; J. Gregory Garrison, CBS legal analyst; and Kate Ekins, manager of public affairs, St. Vincent Hospital and Health Services | 137 |
| Redick, Dennis R., mayor, Noblesville, IN; Charles G. Henderson, mayor, Greenwood, IN; and Carlton Curry, councilman, Indianapolis, IN | 116 |
| Willemssen, Joel, Director, Civil Agencies Information Systems, General Accounting Office; Peter Beering, deputy general counsel, Indianapolis Water Co.; Robert Miller, Indianapolis Water Co.; John Edwards, project manager, year 2000 compliance, Citizens Gas and Coke Utility; Joseph Gustin, vice president, information services, Indianapolis Power and Light; Frank Mitchell, media relations manager, year 2000, Ameritech; and Don Sloan, legislative director, AT&T | 15 |
| Letters, statements, etc., submitted for the record by: | |
| Beering, Peter, deputy general counsel, Indianapolis Water Co.; Robert Miller, Indianapolis Water Co.; John Edwards, project manager, year 2000 compliance, Citizens Gas and Coke Utility; Joseph Gustin, vice president, information services, Indianapolis Power and Light; Frank Mitchell, media relations manager, year 2000, Ameritech; and Don Sloan, legislative director, AT&T, presentation of | 66 |
| Burton, Hon. Dan, a Representative in Congress from the State of Indiana, prepared statement of | 3 |
| Cottey, Jack L., sheriff, Marion County, IN, prepared statement of | 139 |
| Curry, Carlton, councilman, Indianapolis, IN, prepared statement of | 130 |
| Ekins, Kate, manager of public affairs, St. Vincent Hospital and Health Services, prepared statement of | 159 |
| Garrison, J. Gregory, CBS legal analyst, prepared statement of | 152 |
| Henderson, Charles G., mayor, Greenwood, IN, prepared statement of | 125 |
| Horn, Hon. Stephen, a Representative in Congress from the State of California, prepared statement of | 7 |
| Mitchell, Frank, media relations manager, year 2000, Ameritech, prepared statement of | 49 |
| Redick, Dennis R., mayor, Noblesville, IN, prepared statement of | 118 |
| Spahr, John, deputy fire chief, Lawrence Township Fire Department, prepared statement of | 144 |
| Willemssen, Joel, Director, Civil Agencies Information Systems, General Accounting Office, prepared statement of | 18 |

# THE YEAR 2000 PROBLEM, INDIANAPOLIS: A LOCAL RESPONSE

**MONDAY, APRIL 19, 1999**

HOUSE OF REPRESENTATIVES,
COMMITTEE ON GOVERNMENT REFORM,
*Indianapolis, IN.*

The committee met, pursuant to notice, at 9 a.m., at Indiana University-Purdue University at Indianapolis University Place, room 132, 850 W. Michigan Street, Indianapolis, IN, Hon. Dan Burton (chairman of the committee) presiding.

Present: Representatives Burton, Horn, and McIntosh.

Staff present: Bill O'Neill, director of procurement policy; Lisa Smith-Arafune, deputy chief clerk; Matt Ryan, senior policy director, Subcommittee on Government Management, Information, and Technology; Michael Yang, minority counsel; Michael A. Delph, district director; Jim Atterholt, senior policy advisor; and Tim Davis, special assistant.

Mr. BURTON. Quorum being present, we will start this hearing.

Normally, my colleague Steve Horn would be chairing this hearing, but in deference to the chairman of the full committee, he has allowed me to start off this morning. Steve is the man who is the real expert on the Y2K problem. He will be carrying most of the heavy work up here for us. Right?

Mr. HORN. Anything you say, Mr. Chairman. Subcommittee chairmen learn to keep on the good side of the full committee chairman.

Mr. BURTON. Right. Right.

Well, I want to welcome everyone this morning to discuss one of the most pressing issues that our Nation faces as the millennium approaches. The promise of a new century also brings the possibility of chaos, due to the year 2000 computer problem. As you know, the Y2K bug is the software lines of computer code that, if not fixed when the millennium comes, has the potential to wreak havoc worldwide.

Virtually every governmental and private-sector organization is affected by this most pressing problem. I am quite pleased to have my good friend from California, Steve Horn, who chairs the Government Management, Information, and Technology Subcommittee with me at today's hearing. Chairman Horn is recognized as the leading expert in the Congress on Y2K, and is cochairman of the House task force on the year 2000 problem. He has been holding hearings on this issue for over 3 years, and has been instrumental in raising public awareness of the potential problems we face if we don't take action and take it quickly.

A significant milestone in the Federal Government's effort to update its computer systems for the year 2000 has just been passed. On March 21st, the President's deadline for all mission-critical computers to be year-2000 compliant, 92 percent of the government's departments and agencies reported that their 6,123 mission-critical computer systems are ready for the new millennium. Only 3 short years ago, several agencies were unaware of the programming glitch that could shut down or corrupt their computer systems on January 1, 2000.

The Federal Government has made tremendous progress in its effort to be Y2K compliant; however, 8 percent of the government's mission-critical systems failed to meet the President's March 31st deadline. These systems found within 11 Federal agencies are vital to the health and well-being of millions of Americans. They must be fixed before we can focus on end-to-end testing.

As there are numerous interactions between Federal and non-Federal computer systems, the purpose of this hearing is to assess the level of preparedness of non-Federal entities. Today we will examine the local response to the Y2K problem. We will hear testimony from local government officials, emergency response agencies, and utility concerns on how they are working to resolve their Y2K problems.

The public depends on the uninterrupted flow of service from their utility providers. They expect the phone to ring, and the water and electricity to flow. When there is a problem, they expect their police and fire departments to respond and to be able to obtain health care services. The public needs to be assured that these services will continue. If this is not the case, they need to know what is being done to correct this now, and what contingencies are planned in case of interrupted service.

This forum is of perfect opportunity to see how America's heartland has prepared to meet the challenge to become Y2K compliant. The citizens of Indianapolis have a right to expect that their local government and service providers are doing all that they can to make sure that they enter the millennium Y2K compliant.

We have an excellent panel of witnesses, and I look forward to hearing their testimony on the challenges that they all face, solutions they have implemented and the lessons they have learned in working on this vital issue. I would like to say the reason we are having this here in Indianapolis is because we wanted to find out what major cities, like Indianapolis, across the country are doing to be Y2K compliant.

I thought since Indianapolis is the 11th or 12th largest metropolitan area in the country, and since I am chairman of the committee, that this would be the best place to do this. But my colleague Steve Horn has been all over the country having these hearings. And with that, let me yield to him for some opening remarks.

[The prepared statement of Hon. Dan Burton follows:]

**Statement of the Honorable Dan Burton**

**Chairman**

**Committee on Government Reform**

**April 19, 1999**

**"Year 2000 Computer Problem**

**Indianapolis: A Local Response"**

I want to welcome everyone this morning to discuss one of the most pressing issues that our nation faces as the millennium approaches. The promise of a new century also brings the possibility of chaos due to the Year 2000 computer problem. As you know, the Y2K bug is in the software lines of computer code that if not fixed when the millennium comes, has the potential to wreak havoc worldwide. Virtually every governmental and private sector organization is affected by this most pressing problem.

I am quite pleased to have my good friend from California, Steve Horn, who chairs the Government Management, Information, and Technology Subcommittee, with me at today's hearing. Chairman Horn is recognized as the leading expert in the Congress on Y2K, and is co-chairman of the House Task Force on the Year 2000 problem. He has been holding hearings on this issue for over three years and has been instrumental in raising public awareness of the potential problems we face if we don't take action.

A significant milestone in the Federal Government's effort to update its computer systems for the Year 2000 has just been passed. On March 31, the President's deadline for all mission critical computers to be Year 2000 compliant, 92 percent of the Government's departments and agencies reported that their 6,123 mission critical computer systems are ready for the new millennium.

Only three short years ago, several agencies were unaware of the programming glitch that could shutdown or corrupt their computer systems on January 1, 2000. The Federal Government has made tremendous progress in its effort to be Y2K compliant. However, eight percent of the Government's mission critical systems failed to meet the President's March 31 deadline. These systems, found within 11 Federal agencies, are vital to the health and well being of millions of Americans. They must be fixed before we can focus on end to end testing.

As there are numerous interactions between Federal and non Federal computer systems, the purpose of this hearing is to assess the level of preparedness of non Federal entities.

Today, we examine the local response to the Y2K problem. We will hear testimony from local government officials, emergency response agencies and utility concerns on how they are working to solve their Y2K problems.

The public depends on the uninterrupted flow of service from their utility providers. They expect the phone to ring and the water and electricity to flow. When there is a problem, they expect their police and fire departments to respond, and the ability to obtain health care services. The public needs to be assured that these services will continue. If this is not the case they need to know what is being done to correct this now, and what contingencies are planned in case of interrupted service.

This forum is a perfect opportunity to see how America's heartland has prepared to meet the challenge to become Y2K compliant. The citizens of Indianapolis have a right to expect that their local government and service providers are doing all that they can to make sure that they enter the millennium Y2K compliant.

We have an excellent panel of witnesses and I look forward to hearing their testimony on the challenges they face, solutions they have implemented, and the lessons they have learned in working on this vital issue.

Mr. HORN. Thank you very much, Mr. Chairman. Last fall we were here in Indianapolis, and the chairman had to be in Washington dealing with the Attorney General on one of our major national scandals, and how we do something about it. The year 2000 "millennium bug" has turned into a metaphor for the potential computer problems that are associated with January 1, 2000, around the world. And they go back to the 1960's.

Some of you will remember rooms such as this with mainframe computers from one end to the other and very little capacity. Your personal computer has more capacity than most of those mainframes. So when you get to the year 2000, what happens is that to get more space, they said, why do we have to put 19 in when we put in 1967? Let's just put 67. And that became the standard throughout the industry.

The result is, when you get to January 1, 2000, you end up with a zero-zero, not a 67 or a 1967. And so computers all over the world have to be adjusted that way. And even when you have yours set up and adapted, the facts are that you might be polluted again by computers that are not adapted to a situation where they will know it is the year 2000, because it will think it is the year 1900. And computers are only as good as we program them. So this is a massive reprogramming situation.

We started on this in April 1996 when the Federal Government was doing absolutely nothing about it. The Social Security Administration had done it on its own from 1989, and it took them 10 years to be 100 percent compliant. They weren't compliant until this year. But you can tell all your friends the Social Security checks will be around.

And the same will be, I think, with Medicare; they are coming along.

But we do have some real problems in the Federal Government.

The Federal Government at this point has spent $8 billion to fix its computer system. The original estimate of the Gartner Group was that we would be spending $30 billion. My guess was we would spend $10 billion, and I think my guess—and I have absolutely, complete ignorance on this subject, and I don't claim to be an expert, but my instincts are pretty right on this one—they might well go to $10 billion. And it is considered a $600 billion worldwide problem by the Gartner Group, which is one of the leading consultant services.

So what we wanted to do, as the chairman said, is start seeing what the major cities have done at this point, and so that is why we are in Indianapolis. We have also visited Dallas, New York, and New Orleans. The bottom line is, any one of the entities that make up the modern major city, be it utilities, the government, whatever, that affects our lives, can have a very difficult impact on citizens. What we want to avoid is some of the panic scare that some people have already done, and you will see a lot more of it. That is why we think we ought to go out and see what is going on.

The danger comes when somebody is trying to sell a book, which a lot of them have. I have a closet full of them from all over America, where people have tried to scare the living daylights out of people.

And that doesn't mean you can't be prudent. You can be prudent, and it isn't a panic to say it. Make sure you've got your records in case some bank didn't adapt, but the banks have done very well. Mr. Greenspan, I discussed that with him 2½ years ago, and Governor Kelly of the Board of Governors has been in charge of that effort, and they have done a fine job. We have checked them with the banks, the clearinghouse, the stock markets; all of those were working on this 3 years ago. So I think we are safe on that bit.

But there are some places in the United States where they don't quite get the message. This is not one of them, because we had a very good hearing here last fall.

But with the computers to work, we need power, for example. That is why we are going to talk to various entities in the electrical power, whether it be hydro or wind or solar, or whatever it is, because if that power goes down, the business, say, of the strike at Flint, MI, a few months ago, that will be a drop in the bucket.

It would put the whole Midwest out. And after a few days, if there wasn't some way, it would come back on, you would be letting go thousands of workers. That is what we want to avoid. So we think rational business will do it.

I think we have a lot of other things we could say on this, Mr. Chairman, but I would just like my statement to be put in the record as if read.

Mr. BURTON. Without objection, so ordered.

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

**"Oversight of the Year 2000 Problem: Lessons to Be Learned from State and Local Experiences"**
**Opening Statement of Chairman Stephen Horn**
**Subcommittee on Government Management, Information and Technology**
**April 19, 1998**
**Indianapolis, Indiana**

Thank you Mr. Chairman for holding this hearing today in the lovely city of Indianapolis. Just last September we were here in Indianapolis to learn of the city's progress in grappling with the Year 2000 "millennium bug," a now common metaphor for the potential computer problems associated with clocks around the world turning to January 1, 2000.

We are here today to discuss the Year 2000 computer problem. As just about everyone knows by now, many computers and microchips must be fixed in order to recognize the date change to January 1, 2000, and beyond. This is a race against time: we are facing a deadline that cannot be moved. The checkered flag has been waived and we are on the last lap. We must work together, share information, mobilize our resources, and cross the finish line in time.

Almost three years ago, our Government Reform subcommittee held the first Congressional hearing on the Year 2000 problem, and since that time, we have held almost 30 hearings and issued 7 "report cards" to assess the status of the Federal Government's Year 2000 computer fixes.

We know that the Year 2000 computing problem affects just about every aspect of Federal, State, and local governmental operations. Furthermore, it also affects private sector organizations and could affect 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.

The Federal Government alone has already spent about 8 billion dollars to fix its computer systems. No single organization, city, State or even country can solve the Year 2000 problem alone. 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 has data that contains pertinent payment information for those citizens that are eligible for social security payments. 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 their own network of computers.

The bottom line is: If any one of these entities fails, from the Federal Government to the local bank, 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.

But, for computers to work, we need power. One of the first questions concerning the Year 2000 challenge is, "will the lights stay on?" Without electricity, our modern society would be in the proverbial "stone age" again.

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 pose potential serious threats at local levels as well, from the potential interruption to 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.

Accordingly, the testimony we receive today will help our understanding of the full extent of the Year 2000 computer problem. One thing is for sure, there are only about 255 days until January 1, 2000, and the clock is ticking.

I welcome our witnesses Mr. Chairman and look forward to their testimony.

Mr. BURTON. I would like to welcome our colleague, Mr. McIntosh. He is chairman of the National Economic Growth, Natural Resources, and Regulatory Affairs Subcommittee of the Government Reform Committee.

David, do you have some comments you would like to make?

Mr. MCINTOSH. Just very briefly.

Chairman Burton, let me say thank you for holding this hearing here. In particular, I welcome our colleague Mr. Horn, who has frankly done more than anybody that I know of in the government to make sure that we are focusing on this issue; and he did it far before the rest us even really understood the problem and the potential problem. And so we owe him a debt of gratitude for leading that effort in his subcommittee.

I want to thank you for that, Steve.

Mr. HORN. Well, I thank the gentleman. He is a fellow subcommittee chairman, and he has done an outstanding job. And you can see how we get in Congress when we say nice words about each other.

Mr. MCINTOSH. That is right.

Mr. HORN. Somebody has got to say nice words to us.

Mr. BURTON. Mutual admiration.

Mr. MCINTOSH. Exactly. But so everybody puts it in context, Steve really has spent the last several years focusing on an issue that many in Congress said, that is down sometime in the future, we don't have to worry about it. And he has. We have all been helped as a result of it.

I want to thank the panelists today for coming. I have talked to many of them about it; just asking, Are we ready? You will be favorably impressed, Steve, that the business community here in Indianapolis has gotten ahead of the curve and has done a good job. But with that Chairman Burton, thank you very much for having this hearing here today.

Mr. BURTON. Thank you. Before I go to the first panel, let me just say that one of the main purposes of this hearing is to try to allay some of the fears that people have. My brother and a lot of other people have been getting information that leads them to believe that they should buy generators and have them close to their home, and have gas supplies and everything else, because January 1st there may be a glitch that closes down the electricity. Some people are even buying guns and everything else to protect themselves against their neighbors.

So one of the things that I think is important is that the public be well informed about the situation so that they don't get hyper. I think you touched on that, Steve. And for that reason, I think what we are talking about today hopefully will be discussed all over this country, so people will not go off the deep end and start doing crazy things, and wasting a lot of money that they don't have to.

Our first panel—and I want to say, I am glad we have one of our major supporters in getting this information out to the people, Greg Garrison, who is on television and radio quite a bit; has his own radio show here. He has been telling the people about the Y2K problem. I appreciate you being here, Greg, and testifying as well

so that you can get the message out to the hinterlands about what the real situation is.

Mr. GARRISON. My pleasure.

Mr. BURTON. Our first panel is Mr. Joel Willemssen. We normally swear you folks in, but I am not going to have you all stand up at one time and swear you in, because I know you are going to tell the truth, and I don't want you to turn the table over.

So we have Mr. Joel Willemssen. He is the Director of Civil Agencies Information Systems at the General Accounting Office. Are you out of Washington?

Mr. WILLEMSSEN. Yes, sir, Mr. Chairman.

Mr. BURTON. Welcome to Indiana. And also on our panel is Mr. Peter Beering, Deputy General Counsel at the Indianapolis Water Co.

Are you related to Mr. Beering up at Purdue?

Mr. BEERING. Yes, sir, I am.

Mr. BURTON. Your father?

Mr. BEERING. He is.

Mr. BURTON. Well, tell your father we said hello.

Mr. BEERING. I will do that.

Mr. BURTON. Mr. Robert Miller of the Indianapolis Water Co.; Mr. John Edwards, project manager for the year 2000 compliance at Citizens Gas and Coke Utility; Mr. Joe Gustin, vice president, information services at Indianapolis Power and Light. We had dinner together last night.

Did you get a good night's sleep?

Mr. GUSTIN. Yes, sir.

Mr. BURTON. Frank Mitchell, year 2000's media relations manager at Ameritech; and, Mr. Don Sloan, legislative director at AT&T.

And I think that about covers it.

Would you like to start off with a brief overview?

Mr. WILLEMSSEN. Yes, I will.

Mr. BURTON. Mr. Willemssen.

**STATEMENTS OF JOEL WILLEMSSEN, DIRECTOR, CIVIL AGENCIES INFORMATION SYSTEMS, GENERAL ACCOUNTING OFFICE; PETER BEERING, DEPUTY GENERAL COUNSEL, INDIANAPOLIS WATER CO.; ROBERT MILLER, INDIANAPOLIS WATER CO.; JOHN EDWARDS, PROJECT MANAGER, YEAR 2000 COMPLIANCE, CITIZENS GAS AND COKE UTILITY; JOSEPH GUSTIN, VICE PRESIDENT, INFORMATION SERVICES, INDIANAPOLIS POWER AND LIGHT; FRANK MITCHELL, MEDIA RELATIONS MANAGER, YEAR 2000, AMERITECH; AND DON SLOAN, LEGISLATIVE DIRECTOR, AT&T**

Mr. WILLEMSSEN. Thank you, Mr. Chairman, Subcommittee Chairmen Horn and McIntosh. Thank you for inviting the GAO to testify today. And, as requested, I will give a brief overview on where the Federal Government stands, and then briefly touch on, as requested, some of the lessons learned to date from the leading organizations in dealing with Y2K.

Mr. BURTON. Let me interrupt.

Mr. WILLEMSSEN. Certainly.

Mr. BURTON. I hope that the panelists will try to limit their remarks. We have about 3 or 3½ hours here, and if we could limit our remarks to around 5 minutes, that would be very helpful, and then we will get the questions and answers later.

Mr. WILLEMSSEN. Yes. Mr. Chairman, as you noted, the Federal Government has made notable progress in addressing Y2K, now standing at a reported 92 percent of mission-critical systems being compliant.

A lot of the reason for this improvement has been congressional oversight. Chairman Horn was on this issue 3 years ago, before it was a nationally known issue. He has been out there spurring top agency leadership to move forward on Y2K by holding agencies accountable through hearings, through his report cards, and through other mechanisms. So I think you are right by giving Chairman Horn and other committees within the House and Senate credit for much of the improvement that has been made within the Federal Government.

Nevertheless, despite that improvement, there remains a lot of work to be done. In particular, there are some critical agencies and systems within those critical agencies that are not yet compliant. Notable among those are the Federal Aviation Administration, and the Health Care Financing Administration, which administers Medicare. Many of those systems are not yet compliant. Beyond that individual system compliance, we then have to think about end-to-end testing of multiple systems supporting a key business process. So even when those individual systems have been deemed compliant, there is still a lot of hard work left to be done.

The bottom line on the Federal Government is that while a lot of progress has been made, by no stretch of the imagination are we done with the work that needs to be done.

You also asked me to briefly comment on some of the lessons learned to date from leading organizations. We have put together about 100 reports and testimonies on Y2K covering a wide range of Federal agencies and also State and local governments, and other key economic sectors. Based on that work, and based on what we have seen from some of the leading organizations, I thought I would offer in summary form some of the key elements of key "best practices" we have seen of the leading organizations in addressing Y2K.

One, it goes without saying, top agency organization leadership needs to be intimately involved with Y2K. Y2K needs to be viewed as a business problem, not a systems or technical problem. To the extent that that is done, the organizations we have looked at are way ahead of the game in understanding that this is not something that can be shoved off just on the information technology part of the organization, but is truly part of the business and is critical to making sure that those business processes will work as necessary.

That brings us to the second critical point that we have seen. Increasingly, we have needed to focus on the business functions, as opposed to information technology systems. And that is a bit of a learning curve, especially in the Federal Government. And now the Federal Government is moving more to a program orientation rather than a system orientation. For example, we don't think that the average citizen really cares if a Medicare system works or not.

What they care about is that the benefit comes through. And that is where a lot of the focus needs to move.

Third, another critical element is focusing on your partners and your data exchanges. To just focus on your individual business and your individual systems is not good enough. In fact, you could have the best program of any organization, but to the extent you haven't dealt with those critical data exchanges, you run the risk that bad data could come in, infiltrate your systems, and all of that good work that you have done on your systems could go for naught.

Fourth, one of the most important areas within Y2K, testing. The leading organizations are spending between 50 to 70 percent of the total amount of time on Y2K in testing both on individual systems and from an end-to-end perspective. And if organizations today, to the extent that they are not deeply into the testing and through with much of the testing for their individual systems, they are behind the eight ball, and they do need to get moving quickly.

Fifth, another critical component is independent verification and validation. This is essential as another set of eyes to give organizations exactly what the ground truth is on what is going on.

And then to sum up, another critical element: business continuity and contingency planning. No matter how good an organization's efforts are, you have got to have that backup plan in place, so that we can assure the citizens that benefits and services will continue to be provided, even if there are system failures.

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

Mr. BURTON. Thank you. I presume, Steve, that they have given you something in writing on all this?

Mr. HORN. Yes, if I might say, Mr. Chairman, some people in the room might not be familiar with the General Accounting Office. It is part of the legislative branch of the United States, not the executive branch. It reports to the Controller General of the United States. We have a new one that just took office. It is a 15-year term to isolate them from any political pressures by any party. And they do a superb job.

We have several thousand real professionals over there that deal not simply with fiscal matters, but increasingly, as a result of the congressional acts of 1946—but had never been permitted for many years—is the program reviews, and we are looking at all agencies in the Federal Government to have a business plan, have strategic goals, to get a balance sheet. That is the first time that has happened in 210 years of the American Congress and the American executive branch; so they are our eyes and ears.

Mr. BURTON. Thank you, Steve. I would like to have a copy of your report turned in as well.

[The prepared statement of Mr. Willemssen follows:]

United States General Accounting Office

GAO

Testimony

Before the Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at
9 a.m.
Monday,
April 19, 1999

# YEAR 2000 COMPUTING CRISIS

## Readiness Improving But Much Work Remains to Ensure Delivery of Critical Services

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

GAO/T-AIMD-99-149

Mr. Chairman and Members of the Committee:

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

Because of its urgent nature and the potentially devastating impact it could have on critical government operations, in February 1997 we designated the Year 2000 problem as a high-risk area for the federal government.[2] Since that time, we have issued over 90 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 remaining challenges in correcting its systems; identify state and local government Year 2000 issues; and provide an overview of the available information on the readiness of key public infrastructure and economic sectors.

---

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

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

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

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

THE PUBLIC FACES RISKS OF
YEAR 2000 DISRUPTIONS

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

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

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

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

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

---

[5] FAA Systems: Serious Challenges Remain in Resolving Year 2000 and Computer Security Problems (GAO/T-AIMD-98-251, August 6, 1998).
[6] Defense Computers: Year 2000 Computer Problems Threaten DOD Operations (GAO/AIMD-98-72, April 30, 1998).

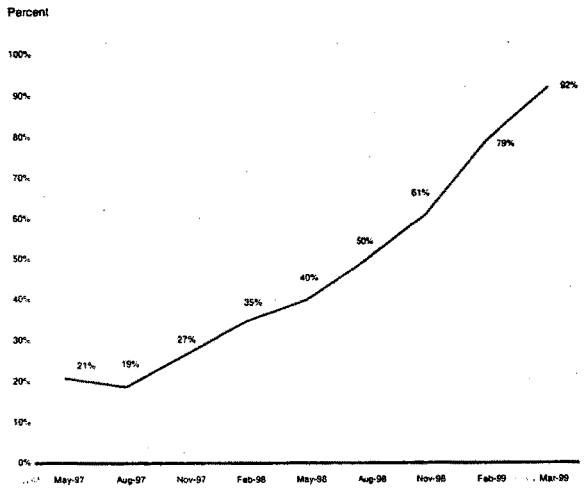
## IMPROVEMENTS MADE BUT MUCH WORK REMAINS

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, OMB directed the major departments and agencies to submit quarterly reports on their progress, beginning May 15, 1997. These reports contain information on where agencies stand with respect to the assessment, renovation, validation, and implementation of mission-critical systems, as well as other management information on items such as business continuity and contingency plans and costs.

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 the 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, 92 percent of these systems were reported to have met this goal.

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




Source: May 1997 – February 1999 data are from the OMB quarterly reports. The March 1999 data are from the President's Council on Year 2000 Conversion and OMB.

While this progress is notable, 11 agencies did not meet OMB's deadline for all of their mission-critical systems.[7] In addition, as we testified last week, some of the systems that were not yet compliant support vital government functions.[8] For example, among the

[7]The 11 agencies were the Departments of Agriculture, Commerce, Defense, Energy, Health and Human Services, Justice, State, Transportation, Treasury; the National Aeronautics and Space Administration; and the U.S. Agency for International Development.

[8]Year 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).

systems that did not meet the March 1999 deadline were those operated by Health Care Financing Administration (HCFA) contractors. As we testified in February 1999, these systems are critical to processing Medicare claims.[9]

Additionally, not all systems have undergone an independent verification and validation process. For example, the Environmental Protection Agency and the Department of the Interior reported that 57 and 3 of its systems, respectively, deemed compliant were still undergoing independent verification and validation. In some cases, independent verification and validation of compliant systems have found serious problems. For example, as we testified this February,[10] none of HCFA's 54 external mission-critical systems reported by the Department of Health and Human Services 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 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. The following are examples of the results of some of our recent reviews.

- In March 1999, we testified that the Federal Aviation Administration (FAA) had made tremendous progress over the prior year.[11] 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 are adequate, (2) implementing multiple systems at numerous facilities, (3) completing data exchange efforts, and (4) completing end-to-end testing. In addition, last week we testified[12] that 10 of FAA's 52 noncompliant mission-critical systems are among the systems that it 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 – should their Year 2000 repairs experience schedule delays or should the systems not be operational on January 1, 2000. Because of the risks associated with FAA's Year 2000 program, we

[9] Year 2000 Computing Crisis: Medicare and the Delivery of Health Services Are at Risk (GAO/T-AIMD-99-89, February 24, 1999) and Year 2000 Computing Crisis: Readiness Status of the Department of Health and Human Services (GAO/T-AIMD-99-92, February 26, 1999).
[10] GAO/T-AIMD-99-92, February 26, 1999.
[11] Year 2000 Computing Crisis: FAA Is Making Progress But Important Challenges Remain (GAO/T-AIMD/RCED-99-118, March 15, 1999).
[12] GAO/T-AIMD-99-144, April 14, 1999.

have advocated that the agency develop business continuity and contingency plans.[13] FAA agreed and has activities underway which we are currently reviewing.

- Earlier this month, 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.[14] 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 system and completing its contingency plans.

- Our work has shown that the Department of Defense and the military services face significant problems.[15] In March 1999, we testified that, despite considerable progress made in the 3 months before the testimony, Defense was still well behind schedule.[16] We found that DOD faced two significant challenges, it (1) must complete remediation and testing of its mission-critical systems and (2) must have 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 can only be provided if Defense takes 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

[13]FAA 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.
[14]Year 2000 Computing Crisis: Federal Reserve Has Established Effective Year 2000 Management Controls for Internal Systems Conversion (GAO/AIMD-99-78, April 9, 1999).
[15]Defense Computers: Year 2000 Computer Problems Put Navy Operations At Risk (GAO/AIMD-98-150, June 30, 1998), Defense Computers: Army Needs to Greatly Strengthen Its Year 2000 Program (GAO/AIMD-98-53, May 29, 1998), GAO/AIMD-98-72, April 30, 1998, and Defense Computers: Air Force Needs to Strengthen Year 2000 Oversight (GAO/AIMD-98-35, January 16, 1998).
[16]Year 2000 Computing Crisis: Defense Has Made Progress, But Additional Management Controls Are Needed (GAO/T-AIMD-99-101, March 2, 1999).

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).[17]

In January 1999 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.[18] 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 efforts regarding end-to-end testing to demonstrate the Year 2000 readiness of federal programs with states and other partners critical to the administration of those programs.

We are also encouraged by some agencies' recent actions. For example, we testified this March, that the Department of Defense's Principal Staff Assistants are planning to conduct end-to-end tests to ensure that systems that collectively support core business areas can interoperate as intended in a Year 2000 environment.[19] Further, our March 1999 testimony[20] found that FAA had addressed our prior concerns with 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.[21]

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

[17]GAO/AIMD-10.1.21, November 1998.
[18]Year 2000 Computing Crisis: Readiness Improving, But Much Work Remains to Avoid Major Disruptions (GAO/T-AIMD-99-50, January 20, 1999).
[19]GAO/T-AIMD-99-101, March 2, 1999.
[20]GAO/T-AIMD/RCED-99-118, March 15, 1999.
[21]GAO/T-AIMD-98-251, August 6, 1998.

develop contingency plans for all critical core business processes.[22]

OMB has clarified its contingency plan instructions and, along with the Chief Information Officers Council, has adopted our business continuity and contingency planning guide.[23] 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 business continuity and contingency plans in their February 1999 quarterly reports. Accordingly, in their February 1999 reports, almost all agencies listed their high-level core business functions. Indeed, major departments and agencies listed over 400 core business functions. For example, the Department of Veterans Affairs classified its core business functions into two critical areas: benefits delivery (six business lines supported this area) and health care.

Our review of the 24 major departments and agencies February 1999 quarterly reports found that business continuity and contingency planning was generally well underway. However, we also found cases in which agencies: (1) were in the early stages of business continuity and contingency planning, (2) did not indicate when they planned to complete and/or test their plan, (3) did not intend to complete their plans until after April 1999, or (4) did not intend to finish testing the plans until after September 1999. In January 1999, we testified before you that OMB could consider setting a target date, such as April 30, 1999, for the completion of business continuity and contingency plans, and require agencies to report on their progress against this milestone.[24] This would encourage agencies to expeditiously develop and finalize their plans and would provide the President's Council on Year 2000 Conversion and OMB with more complete information on agencies' status on this critical issue. To provide assurance that agencies' business continuity and contingency plans will work if they are needed, we also 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.

On March 31, OMB and the Chair of the President's Council on Year 2000 Conversion 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. OMB also announced that it planned to ask agencies to submit their business continuity and contingency plans in June. In addition to this action, we would encourage OMB to implement the suggestion that we made in our January 20 testimony and establish a target date for the validation of these business continuity and contingency plans.

---

[22] Year 2000 Computing Crisis: Potential for Widespread Disruption Call for Strong Leadership and Parternships (GAO/AIMD-98-85, April 30, 1998).
[23] GAO/AIMD-10.1.19, August 1998.
[24] GAO/T-AIMD-99-50, January 20, 1999.

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.[25]

On March 26, 1999, 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); appendix I lists these programs and 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.

STATE AND LOCAL GOVERNMENTS
FACE SIGNIFICANT YEAR 2000 RISKS

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

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

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

A recent survey of state Year 2000 efforts indicated that much remains to be completed. The states[26] (except for three that did not respond to the survey) reported to the National Association of State Information Resource Executives that, as of April 5, 1999,[27] they had thousands of mission-critical systems.[28] With respect to the remediation of these systems,

- 1 state reported that it had completed between 1 and 24 percent of the activities required to return a modified system or renovated process to production,
- 13 states[29] reported that they had completed between 25 and 49 percent,
- 17 states[30] reported completing between 50 and 74 percent,
- 17 states[31] reported completing more than 75 percent of these activities,[32] and
- almost all states reported that they are actively engaged in internal and external contingency planning but of the 50 states that established target dates for the completion of these plans, 23 (46 percent) reported the deadline as September 1999 or later.

State audit organizations have also identified significant Year 2000 concerns. In January 1999, the National State Auditors Association reported on the results of its mid-1998 survey of Year 2000 compliance among states. This report stated that, for the 12 state audit organizations which 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 13 state-level audit organizations and Guam that discussed the Year 2000 problem and had been issued since October 1, 1998. Several of these 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,

---

[26]In the context of the National Association of State Information Resource Executives survey, the term states includes Guam, Puerto Rico, and the District of Columbia.
[27]Individual states submit periodic updates to the National Association of State Information Resource Executives. For the April 5th report, almost all of the states submitted their data in March 1999.
[28]The National Association of State Information Resource Executives defined mission-critical systems as those that the state has identified as priorities for prompt remediation.
[29]Instead of reporting on its mission-critical systems, one state reported on its processes while another reported on its functions.
[30]Instead of reporting on its mission-critical systems, one state reported on its core business activities, another state reported on projects, and a third state reported on all systems.
[31]Instead of reporting on its mission-critical systems, one state reported on its applications.
[32]Two states did not respond to this question.

- In December 1998, the Vermont State Auditor reported[33] 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 states' external electronic partners.

- In January 1999 the Rhode Island Auditor General reported[34] that testing standards and a test plan had not been developed.

- In February 1999, the California State Auditor reported[35] that key agencies responsible for emergency services, corrections, and water resources, among others, 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 is not completed, the Office of Emergency Services may have to rely on cumbersome manual processes, significantly increasing response time to disasters.

- In March 1999 Oregon's Audits Division reported[36] that 11 of the 12 state agencies reviewed did not have business continuation plans addressing potential Year 2000 problems for their core business functions.

- In March 1999 North Carolina's State Auditor reported[37] that resource restrictions had limited the state's Year 2000 Project Office's ability to verify data reported by state agencies.

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

- In January 1999, the United States Conference of Mayors reported on the results of their survey of 220 cities. The results of this survey of cities found (1) 97 percent had a citywide plan to address Year 2000 issues, (2) 22 percent had repaired or replaced less than 50 percent of their systems, and (3) 45 percent had completed less than 50 percent of their testing.

---

[33]Vermont 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.

[34]State of Rhode Island, Efforts to Resolve the Year 2000 Computer Issue (Office of the Auditor General, January 29, 1999).

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

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

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

- A November 1998 National Association of Counties survey of a sample of 500 counties found that (1) 50 percent of the counties had a countywide Year 2000 plan, (2) 36 percent had completed assessment, (3) 16 percent had repaired or replaced their systems, and (4) 73 percent had no contingency plans.

Status Of State-Administered Federal Human Services Programs Not Clear

About 25 percent of the federal government's programs designated as high-impact by OMB are state-administered, such as Food Stamps and Temporary Assistance for Needy Families. One federal system that did not make the March implementation target is critical to the implementation of several of these programs. This system, the Department of Health and Human Service's Payment Management System, processes billions of dollars in grant payments to states and other recipient organizations for vital programs, such as Medicaid. As we testified in February 1999, the planned replacement system has encountered problems since its inception and, as a result, is still not operational.[38] Consequently, the Department of Health and Human Services decided to repair the existing system, which is not expected to be compliant until June 30, 1999.

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 continued services.[39] 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.[40] 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.

In January 1999, OMB implemented a requirement that federal oversight agencies include the status of selected state human services systems in their quarterly reports. Specifically, OMB requested that the 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. Table 1 summarizes the information gathered by the Departments of Agriculture, Health and Human Services, and Labor on how many state-level organizations are compliant or when in 1999 they planned to be compliant.

---

[38]GAO/T-AIMD-99-92, February 26, 1999.
[39]Year 2000 Computing Crisis: Readiness of State Automated Systems to Support Federal Welfare Programs (GAO/AIMD-99-28, November 6, 1998).
[40]Year 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 Key Federally Supported Programs[a]

| Program | Compliant | January-March | April-June | July-September | October-December | No Report |
|---|---|---|---|---|---|---|
| Food Stamps | 15 | 10 | 12 | 8 | 5 | 0 |
| Unemployment Insurance | 21 | 6 | 13 | 8 | 1 | 1 |
| Temporary Assistance for Needy Families | 7 | 3 | 12 | 4 | 2 | 22 |
| Medicaid – Integrated Eligibility System | 3 | 1 | 8 | 5 | 1 | 33 |
| Medicaid – Management Information Systems | 7 | 7 | 14 | 12 | 2 | 9 |
| Child Support | 4 | 6 | 10 | 3 | 2 | 25 |
| Child Care | 4 | 3 | 8 | 5 | 2 | 31 |
| Child Welfare | 6 | 3 | 8 | 5 | 2 | 27 |
| Women, Infants, and Children | 24 | 8 | 6 | 6 | 6 | 0 |

[a]According to OMB, the Departments of Agriculture and Health and Human Services were still collecting information from the states on the status of the Child Nutrition Program and the Low Income Home Energy Assistance Program, respectively.

Source: Progress on Year 2000 Conversion, (OMB, data received February 12, 1999, issued on March 18, 1999).

Note: OMB reported the status of 5 programs for 50 state-level organizations (Food Stamps, Unemployment Insurance, Temporary Assistance for Needy Families, Child Support, and Women, Infants, and Children). The status of 2 programs was provided for 51 state-level organizations (Medicaid and Child Welfare). The status of Child Care was provided for 53 state-level organizations.

This table illustrates the need for federal/state partnerships to ensure the continuity of these vital services, since a considerable number of state-level organizations are not due to be compliant until the last half of 1999, and the agencies have not received reports from many states. Such partnerships could include the coordination of federal and state business continuity and contingency plans for human services programs.

One agency that could serve as a model to other federal agencies in working with state partners is the Social Security Administration, which relies on states to help process claims under its disability insurance program. In October 1997, we made recommendations to the Social Security Administration to improve its monitoring and oversight of state disability determination services and to develop contingency plans that consider the disability claims processing functions within state disability determination

services systems.[41] The Social Security Administration agreed with these recommendations and, as we testified this February, has taken several actions.[42] For example, it established a full-time disability determination services project team, designating project managers and coordinators, and requesting biweekly status reports. The agency also obtained from each state disability determination service (1) a plan specifying the specific milestones, resources, and schedules for completing Year 2000 conversion tasks, and (2) contingency plans. Such an approach could be valuable to other federal agencies in helping ensure the continued delivery of services.

In addition to the state systems that support federal programs, another important aspect of the federal government's Year 2000 efforts with the states are data exchanges. For example, the Social Security Administration exchanges data files with the states to determine the eligibility of disabled persons for disability payments and the National Highway Traffic Safety Administration provides states with information needed for drivers registration. As part of addressing this issue, the General Services Administration is collecting information from federal agencies and the states on the status of their exchanges through a secured Internet World Wide Web site. According to an official at the General Services Administration, 70 percent of federal/state data exchanges are Year 2000 compliant. However, this official would not provide us with supporting documentation for this statement nor would the General Services Administration allow us access to its database. Accordingly, we could not verify the status of federal/state data exchanges.

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

Beyond the risks faced by the federal, state, and local governments, the Year 2000 also poses a serious challenge to the public infrastructure, key economic sectors, and to other countries. To address these concerns, in April 1998 we recommended that the Council use a sector-based approach and establish the effective public-private partnerships necessary to address this issue.[43] 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.

---

[41] Social Security Administration: Significant Progress Made in Year 2000 Effort, But Key Risks Remain (GAO/AIMD-98-6, October 22, 1997).
[42] Year 2000 Computing Crisis: Update on the Readiness of the Social Security Administration (GAO/T-AIMD-99-90, February 24, 1999).
[43] GAO/AIMD-98-85, April 30, 1998.

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

The January 7, 1999, report summarizes information collected to date by the working groups and various trade associations.[44] The Council acknowledged that readiness data in certain industries were not yet available and, therefore, were not included in the report. Nevertheless, based on the information available at the time, it concluded that

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

The Council's report was a good step toward obtaining a picture of the nation's Year 2000 readiness. However, the picture remains substantially incomplete because assessments were not available in many key areas, such as local law enforcement and the maritime industry. Also, some surveys did not have a high response rate, calling into question whether they accurately portray the readiness of the sector. In addition, in some cases, such as drinking water and health care, the report provided a general assessment of the sector but did not contain detailed data as to the status of the sector (e.g., the average

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

percentage of organization's systems that are Year 2000 compliant or the percentage of organizations that are in the assessment, renovation, or validation phases).

The President's Council on Year 2000 Conversion is to be commended on the strides that it has made to obtain Year 2000 readiness data that is critical to the nation's well-being as well as its other initiatives, such as the establishment of the Senior Advisors Group. However, to further reduce the likelihood of major disruptions, in testimony this January,[45] we suggested that the Council consider additional actions such as continuing to aggressively pursue readiness information in the areas in which it is lacking. 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. The Council's next sector report is expected to be released this month. As discussed below, we have issued several products related to several of these key sectors.

Energy Sector

This month, we reported that while the electric power industry has reported that it has made substantial progress in making its systems and equipment ready to continue operations into the Year 2000, significant risks remain.[46] In response to a November 1998 survey, the nation's electric power utilities reported that, on average, they were 44 percent complete with remediation and testing. However, almost half of the reporting organizations said that they did not expect to be Year 2000 ready within the June 1999 industry target date, and about one sixth of the respondents indicated they would not be ready until the last 3 months of 1999—leaving little margin for resolving unexpected problems. In this report, we suggested that the Department of Energy (1) work with the Electric Power Working Group to ensure that remediation activities are accelerated for the utilities that expect 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. We also suggested that the Nuclear Regulatory Commission, (1) in cooperation with the Nuclear Energy Institute, work with the 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 Year 2000 readiness and (2) publicly disclose the Year 2000 readiness of each of the nation's operational nuclear reactors.

---

[45]GAO/T-AIMD-99-50, January 20, 1999.

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

Health Sector

Last week, we testified[47] that, in response to our September 1998 recommendation,[48] the Food and Drug Administration, in conjunction with the Department of Veterans Affairs, had established a clearinghouse on biomedical equipment. As of April 5, 1999, 4,251 biomedical equipment manufacturers had submitted data to the clearinghouse. About 54 percent of these manufacturers reported having products that do not employ dates and about 16 percent reported having date-related problems such as an incorrect display of date/time. The Food and Drug Administration was awaiting responses from 399 manufacturers.

Our April testimony 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 of them 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 agencies[49] to ensure that the institutions that they oversee are ready to handle the Year 2000 problem.[50] We concluded that the regulators had made significant progress in assessing the readiness of member institutions and raising awareness on important issues such as contingency planning and testing. Regulator examinations of bank, thrift, and credit union Year 2000 efforts found that the vast majority were doing a satisfactory job of addressing the problem. Nevertheless, the regulators faced the challenge of ensuring that they are ready to take swift action to address those institutions that falter in the later stages of correction and to address disruptions caused by international and public infrastructure failures.

In March 1999, we concluded that insurance regulator presence regarding the Year 2000 area was not as strong as that exhibited by the banking and securities industry.[51] We found that the state insurance regulators we contacted were late in raising industry

---

[47]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).
[48]Year 2000 Computing Crisis: Compliance Status of Many Biomedical Equipment Items Still Unknown (GAO/AIMD-98-240, September 18, 1998).
[49]The National Credit Union Administration, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the Federal Reserve System, and the Office of the Comptroller of the Currency.
[50]Year 2000 Computing Crisis: Federal Depository Institution Regulators Are Making Progress, But Challenges Remain (GAO/T-AIMD-98-305, September 17, 1998).
[51]Insurance Industry: Regulators Are Less Active in Encouraging and Validating Year 2000 Preparedness (GAO/T-GGD-99-56, March 11, 1999).

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 too limited.

Transportation Sector

This January we reported on our survey of 413 airports.[52] We found that while the nation's airports are making progress in preparing for the year 2000, such progress varies among airports. 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.

- - - - -

In summary, while improvement has been shown, much work remains at the national, federal, state, and local level 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. To meet this challenge, strong leadership and partnerships must be maintained to ensure that government programs meet the needs of the public 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 Committees may have at this time.

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

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 Labor | Unemployment Insurance |
| Department of State | Passport Applications and Processing |
| Department of Transportation | Air Traffic Control system |
| Department of Transportation | Maritime Search and Rescue |
| 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

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)

(511752)

Mr. BURTON. I understand the panel has a presentation that you would like to make. Who is the spokesman for the panel?

Mr. BEERING. Thank you, Mr. Chairman.

Mr. BURTON. Mr. Beering.

Mr. BEERING. My name is Peter Beering from the Indianapolis Water Co. In the interest of the committee's time, what we have done is, the working group for the year 2000 problem with Indianapolis utilities have a coordinated presentation by each utility that lives within one Power Point Presentation. I believe Ms. Arafune is going to operate the lights for us.

What we will do is, after some brief introductory remarks, each of the organizations represented on the panel, alphabetically, will comment on their specific company preparations, and then we will be happy to field questions you or the committee may have.

As you are particularly aware from the fact that you have represented much of the Indianapolis area for many years, the Indianapolis utilities have a long and distinguished history of cooperative relationships. These cooperative relationships speed our responses to all of the problems that our customers face, whether those are weather-related or computer-related, or related to some other problem. We and my colleagues, who are represented here are a portion of the year 2000 readiness efforts of these utilities, have been meeting for the past number of months, and this consortium includes representatives from engineering, operations and administrative departments to each of the representative utilities.

One utility who is not a direct participant in this panel today, but who has been participating with us, is the White River Environmental Partnership. They deliver wastewater treatment and sewer services for much of this community, and some of the surrounding area; they, too, have been participating.

Recently, we have also expanded participation in this committee to include significant representation from the Department of Public Safety, both police and fire, as well as emergency management, and also our colleagues from public work's side of the municipal government, so that our response to whatever problem may be, if any at all, is completely coordinated across the board.

Each one of the involved organizations has engaged in a series of compliance testing activities. Each of the involved utilities has evaluated and ranked problem systems. Once problem systems have been identified, they are being tested and assessed for compliance. And I am pleased to report that, based on our meetings, that remediation is well under way on the affected systems. Once the remediation efforts have been completed, each of the systems are retested. And an important piece of our testing methodology includes testing for critical dates that may occur prior to the year 2000 event itself.

Although we, as a set of utilities, do not believe that the year 2000 will present any particular service interruptions, we have also engaged in a very elaborate series of contingency planning activities. These contingency planning activities have included, most importantly, the identification of our key facilities and resources, and those locations that we deem to be critical to the uninterrupted service for our customers. These contingency planning efforts, as I mentioned earlier, are being closely coordinated with public safety

and public works officials and emergency communications have been planned both within the utility environment themselves and also with the broader public works and public safety community. Several of these communications systems were tested recently, as I believe Mr. Gustin will mention during his more particular testimony.

The mission-critical functions and facilities and supplies have been identified and procured, and that includes fuel sources, as well as key personnel, from each of the utilities. We have also worked out a number of staffing issues related to how we get personnel to our key facilities in the event that there was a problem. One of our particular concerns is that, as you are aware, this past year we had a significant snow event during the New Year's celebration, and we are working on contingency plans to address even that kind of problem.

Beyond contingency planning, communications is a very important part of our activities. We have all appeared in front of the Indiana Utility Regulatory Commission. We are briefing or staff and our key employees, and we are providing information to those who need it. We are also participating, all of the utilities represented here, in regional and national efforts to assist other utilities in their planning efforts.

Now I believe that Mr. Mitchell from Ameritech will proceed.

Mr. BURTON. Mr. Mitchell.

Mr. MITCHELL. Chairman Burton, and members of the committee, good morning, and thank you for having us.

My name is Frank Mitchell; I am media relations manager for Ameritech for the year 2000. In that capacity, I have conducted hundreds of interviews with various media on the subject of Y2K and Ameritech's preparedness.

Ameritech has a strong year 2000 initiative in place. Since 1996, Ameritech has been pursing one of our most aggressive undertakings ever, to assure a smooth transition to the 21st century for both Ameritech and its customers. We have established a corporate-wide initiative to address and resolve year 2000 issues, and more than 400 professionals from 31 different disciplines are working on a team that is headed by the year 2000 project leader. It involves every business unit in our corporation. We expect to spend approximately $250 million to address the year 2000 issue.

At Ameritech the year 2000 project leader, Fred Cowitz, reports directly to the executive vice president, who in turn reports directly to the chairman. The project leader not only updates his supervisor on a regular basis, but advises our management committee on a monthly basis of our progress. He also meets with the board of directors every 6 months.

The mission-critical systems remediation work at Ameritech is 99 plus percent complete. From our standpoint, we have reviewed more than 2,500 products or services; remediated an IS portfolio of approximately 1,000 applications; upgraded more than 1,400 central office switches that handle phone calls; analyzed and prepared tens of thousands of desktops and office components, such as telephones, computers and fax machines. And we have prepared access and security systems, heating and cooling plants, alarms and elevators, in 12,000 buildings and equipment vaults. Any remaining

remediation activity, testing and deployment has been scheduled and is expected to be completed well in advance of the century date change.

I will talk about our testing strategies in just a few moments. But our contingency recovery and continuity planning process is well under way. Contingency and recovery plans are already part of our ongoing business on a day-to-day basis. Ameritech has launched a team to develop year 2000 business continuity plans. Things we used to do manually, we may have to learn to do again, in the unlikely event of sustained disruption to our systems, infrastructure or key services provided by our vendors.

Ameritech is encouraging cities and businesses to review their own communications equipment to verify they are Y2K ready and to test them. Ameritech's year 2000 readiness plan generally do not cover customer premises equipment; equipment owned by our customers. Customers will need to contact the supplier or manufacturer of such equipment to determine its year 2000 readiness, and to take all necessary efforts to assure the readiness of their own telecommunications infrastructure. However, in support of our customer efforts, Ameritech is working with its suppliers to determine the year 2000 status of customer-provided equipment and make that information available to our customers.

Ameritech is involved in several Y2K partnerships. Ameritech is a member of the Telco Year 2000 Forum, a nationwide group of major telecommunications companies, and a member of the Alliance for Telecommunications Industry Solutions. Both of these organizations have conducted extensive interoperability testing, and the results support our contention that the Nation's telecommunications system will operate without disruption during and after the year 2000 date change.

Ameritech is also a member of the FCC-sponsored Network Reliability and Interoperability Council, an ongoing body, and an Ameritech representative is also chairing a committee sponsored by the International Telecommunications Union that is developing a first alert communication plan.

Some additional information, Ameritech's Internet Web site address is www.Ameritech.com/Y2K. Ameritech is sponsoring a forum in different cities throughout the region over the next several weeks to discuss Ameritech's Y2K initiative with cities—city and county officials, with a particular emphasis and focus on 911 systems. In fact, today some of my colleagues are in Cleveland making that presentation and will be in Indianapolis tomorrow.

Other activities we have done to keep customers informed include customers' visits to our network lab, where testing is conducted at Hoffman Estates, IL. We have produced news releases and quarterly reports that explain our progress, and we have held visits and conference calls about our readiness for telecommunications industry analysts interested in our progress.

On behalf of our year 2000 director, Fred Cowitz, we are pleased to have the opportunity to testify before this committee, and we would like to commend the committee on its efforts to assist in meeting the year 2000 challenge.

[The prepared statement of Mr. Mitchell follows:]

Statement of Frank V. Mitchell
Ameritech Year 2000 Media Relations Manager

Testimony 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

Indianapolis, Indiana
April 19, 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**

Chairman Burton and members of the Committee, I would like to submit the following written testimony on Ameritech's purpose and activities to address Year 2000 issues within our company.

We have devoted considerable effort on keeping interested parties, including the Federal Government, advised of our progress. Beginning in mid-1998, we have testified at a Field Hearing of Congressman Horn's subcommittee, met with representatives from the Federal Communications Commission, the Federal Reserve (both in Washington and Chicago), the GSA, GAO and we participated in 13 seminars developed to assist smaller financial institutions address the Year 2000 and sponsored by the Office of Thrift Supervision, the FDIC and the Federal Reserve .

We have also provided similar information to numerous State regulatory authorities, as well as in connection with the Company's regular securities laws filings, addressed the questions and concerns of our largest 250 customers as well as many thousands of our smaller customers (both business and residential), contacted 1,500 of our financial institution customers, developed a quarterly program summary to serve as a vehicle to help us communicate our progress and opened an internet web site to make our Year 2000 information easily accessible to our customers.

Given that level of activity, we are not sure that we can add significantly to the information that we have provided to other agencies of the government and that we continue to make available to our customers and the general public. Nevertheless, we are pleased to have the opportunity to testify before this committee and we would like to commend the committee on its efforts to assist government at all levels to meet the Year 2000 challenge.

**Challenges of the Year 2000 Issue**

In our opinion, the largest challenge that businesses face as they seek to address the Year 2000 issue has to do with "positioning" the project within their company. I believe that in order to assure the success of a Year 2000 project you need 4 key elements:

- strong executive support
- sufficient funding
- access to strong project management skills
- commitment to Year 2000 goals



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

In order to acquire those elements, senior management of the business must be educated about the seriousness of the Year 2000 issue. Once they understand the scope of the problem and the potential impact to the business of not addressing and resolving the problem, they are quite willing to lend their support to the project. With senior management support, it becomes somewhat easier to acquire the other tools that one needs to develop a successful Year 2000 program including funding, access to internal and external specialized resources and the ability to draw upon the most talented employees.

At Ameritech, we have all of those elements in place and that is why, as you will hear throughout my testimony, we are confident that we will be able to meet our stated objective of making the "Year 2000 transparent to our customers."

**Executive Support and Funding**

As mentioned, executive support and funding are elements critical to the success of a Year 2000 project.

At Ameritech, the Year 2000 project leader (Fredrick Kowitz, corporate director – Year 2000) reports directly to an executive vice president who in turn reports directly to the Chairman. The Year 2000 project leader updates his supervisor on a regular basis, advises Ameritech's management committee of progress on a monthly basis and meets with the Ameritech Board of Directors every six months. The Year 2000 project leader has consistently received strong support from Ameritech's executive team and he has access to funds required to complete the project.

**Ameritech's Year 2000 Initiative**

As I just stated, Ameritech's goal is to make the Year 2000 event "transparent" to our customers. We've been working since 1996 to ensure that our products and services avoid material problems associated with the Year 2000.

Our current program evaluation is that, as of March 31, 1999, nearly all Ameritech network components and IT systems deemed essential to the delivery of local switched voice and data telecommunications services (e.g., residence and business telephone lines, PBX trunks, Centrex and ISDN services), dedicated voice and data transport services (e.g., analog and digital private line services including X000 series circuits, DS1, DS3 and SONET) and switched and dedicated special access service (e.g., FGB, FGD, VG1-VG12, DS1, DS3 and SONET) are Year 2000 ready. Similarly, nearly all of the mission-critical components and IT systems for Ameritech's cellular, paging and long



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

distance services have been made Year 2000 ready. Preparations for the mission-critical components and IT systems for SecurityLink from Ameritech's security monitoring services, Ameritech Advanced Data Services' frame relay data service and Ameritech's cable television service are progressing well, and those mission-critical network components and IT systems are expected to be made Year 2000 ready well in advance of the turn of the century.

Let me now share some detail about Ameritech's Year 2000 Initiative.

Since 1996, Ameritech has been pursuing one of our most aggressive undertakings ever to assure a smooth transition to the twenty-first century for both Ameritech and its customers. We have established a corporate-wide initiative to address and resolve Year 2000 issues and more than 400 professionals from 31 different disciplines are working on a team that is headed by the Year 2000 project leader and involves every business unit in the corporation.

From Ameritech's standpoint, the initiative includes:

- Reviewing more than 2,500 products and services for Year 2000 issues;
- An IS portfolio of approximately 1,000 applications;
- Upgrading 1,400 host and remote switches that handle telephone calls;
- Analyzing and preparing tens of thousands of desktop and office components such as telephones, computers and fax machines;
- Preparing access and security systems, heating and cooling plants, alarms and elevators in 12,000 buildings and equipment vaults.

**Ameritech's Definition of "Year 2000 Ready"**

Ameritech regards systems as "Year 2000 Ready" if they will operate without any substantial decrease in performance as a result of processing date data into the next century.

In determining readiness, we utilize different standards depending upon the type of system involved. For example, our information services organization uses language adapted from the standard recommended by the US General Services Administration and our network organization follows the standards as described in Bellcore document *GR-2945-CORE*

**Ameritech's Definition of Mission-Critical**



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

Ameritech uses the term "mission-critical" to identify those systems which are vital to the provision of voice and data switching, processing and transport services to our customers. Examples of "mission-critical" systems include those network and essential supporting systems that enable us to provide our customers with local switched and data .

**Ameritech Year 2000 Initiative Program Phases**

Ameritech's business units, as well as the separate disciplines that fall under the corporate umbrella, are implementing comprehensive Year 2000 plans focusing on their customers and functional areas. Each of these plans include the following phases: inventory, assessment, remediation, testing (if required), deployment and monitoring.

**Information Services (IS) Readiness Plan**

The information services Year 2000 remediation process followed five distinct steps:
1) extract the application to be converted and establish baseline tests;
2) convert the application;
3) test the final product;
4) certify the application;
5) reinsert the application into production.

The two principal methodologies being employed in Ameritech's conversion process are the 40/60 Fixed Window solution and the Four-Digit Year Format as described in ISO Standard 8601.

As of March 31, 1999, Ameritech's corporate information services (IS) organization had completed its Year 2000 remediation activity on Ameritech's mission-critical information systems and applications and they are now Year 2000 ready. The majority of such systems have already been deployed back into production. Ameritech utilized the services of Telcordia (f. k. a. Bellcore), an ITAA certified Year 2000 company, to manage its remediation process.

**Network Readiness Plan**[1]

Ameritech's Year 2000 Initiative includes centralized readiness reporting on all networks within Ameritech, including our local exchange and internal office networks, our cellular network managed by Ameritech Cellular Services, our advanced data services managed

[1] Ameritech's network plan includes our local exchange and internal office networks, our cellular network managed by Ameritech Cellular Services, our advanced data services network managed by Ameritech Advanced Data Services, our video network managed by Ameritech New Media, Inc. and our long distance network managed by Ameritech Communications, Inc.



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

by Ameritech Advanced Data Services, our video network managed by Ameritech New Media, Inc. and our long distance network managed by Ameritech Communications, Inc.

Ameritech employs four key processes to ensure the readiness of its networks:

- Vendor Management and Inventory Assessment
- Working with suppliers to determine product readiness, product upgrade requirements and product upgrade availability
- Detailed Network Planning and Scheduling
- Scheduling and managing deployment of network upgrades
- Testing and Certification
  - ⇒ Determine appropriate certification level for each network component
  - ⇒ Obtain and analyze our suppliers' test plans and results
  - ⇒ Develop and execute test plans, as needed, based on Bellcore GR-2945 Year 2000 requirements, using Ameritech's Service Integration Laboratory (SIL) and supplier laboratories
  - ⇒ Interoperability tests of intra-network components conducted in the latter part of 1998 as part of the Year 2000 Telco Forum[2]
  - ⇒ Inter-network interoperability tests conducted in that latter part of 1998 in conjunction with ATIS[3]
- Implementation and Deployment

As of March 31, 1999, all identified mission-critical network components of Ameritech's local switched voice and data telecommunications services (e.g., residence and business telephone lines, PBX trunks, Centrex and ISDN services), dedicated voice and data transport services (e.g., analog and digital private line services including X000 series circuits, DS1, DS3 and SONET) and switched and dedicated special access service (e.g., FGB, FGD, VG1-VG12, DS1, DS3 and SONET) are Year 2000 ready. Similarly, as of March 31, 1999, all identified mission-critical network components for Ameritech's cellular, paging and long distance services 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.

[2] The Year 2000 Telco Forum is an organization of telecommunications companies dedicated to addressing the effects of the Year 2000 problem on the telecommunications industry. One of the main objectives of the Forum is to conduct interoperability testing of intra-network components and operations support systems.

[3] ATIS is the Alliance for Telecommunications Industry Solutions. This is an industry forum consisting of members from the LEC, wireless, IEC and C-LEC industry segments that addresses and seeks to resolve issues concerning national telecommunications standards.



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.

It should be noted that because Ameritech purchases all of its network components from suppliers, timely delivery of acceptable Year 2000 upgrades from those suppliers is key to Ameritech's ability to meet its projected timeframes to make all of its network components Year 2000 ready.

To assure the reliability of its network before, during and after the century date change, Ameritech is performing selective independent verification testing of some of the network component upgrades that it receives from suppliers. This testing is conducted in Ameritech's service integration laboratory in Hoffman Estates, Ill., which routinely tests software and hardware network component upgrades to ensure that they meet Ameritech's high standards for reliability and technical excellence. The laboratory, which replicates the current Ameritech network - complete with switches, data links and other equipment - is equipped to simulate peak traffic loads and analyze actual network performance in a trial run of such events as the turn of the century and leap year dates.

**Supplier Readiness Plan**

With the exception of some internal information services applications, Ameritech does not directly manufacture any of the various hardware and software components that comprise our telecommunications network infrastructure. To assure Year 2000 readiness for those components, we are entirely dependent upon our suppliers to provide us with the necessary upgrades in a timely manner.

We have a strong supplier compliance program in place and are confident that we will be successful in acquiring Year 2000 ready components from our suppliers in a cost-effective and timely fashion.

**Customer Responsibilities**

Ameritech's Year 2000 readiness plans generally do not cover customer premises equipment ("CPE") -- such as telephone systems, PBXs and voice mail equipment) or customer-owned peripheral hardware -- even though this hardware may be linked to equipment that Ameritech owns. This is typically equipment owned by our customers and for which they are responsible. Customers will need to contact the supplier or manufacturer of such equipment to determine it's Year 2000 readiness and to take all necessary efforts to assure the readiness of their own telecommunications infrastructure.

However, in support of our customers' efforts, Ameritech is working with its suppliers to determine the Year 2000 status of CPE, in order that this information may be provided to



This document and the information contained herein is intended, and for
all purposes shall be deemed, a *Year 2000 statement* and a *Year 2000*

our customers. We are prepared to pass this information on to customers as we receive it.

During the Year 2000 transition, Ameritech is striving to maintain all applicable service commitments, such as performance standards contained in state telephone service tariffs or in contracts and agreements with individual customers. In addition, Ameritech has been working actively with major customers, suppliers and trading partners to identify and resolve Year 2000 issues.

**Business Contingency and Continuity Planning**

Because customers rely on Ameritech's networks, rigorous business recovery planning has been a part of our standard operation for many years. Recovery plans are updated and tested frequently in disaster exercises with other telecommunications carriers, major suppliers and customers, and government agencies. As a part of the overall Year 2000 initiative at Ameritech, we expect to review, assess and update these existing business recovery plans as required.

In support of its network operations recovery plan, Ameritech intends to capitalize on established emergency operations control centers ("EOC") in each of our core operating 5 states. We are also developing appropriate staffing plans so that in the event of an occurrence, each center would be staffed with personnel around-the-clock and we have equipped those centers with the appropriate tools (e.g., radio for communications in the event the telephone network unexpectedly fails at an EOC, power backup in the event of a commercial power failure).

Ameritech also has a business recovery plan in place for its information services ("IS") infrastructure. Like the network plan, our IS plan includes a centralized center to monitor and coordinate activities in the event of an unexpected and unforeseen failure of one of our IS systems.

Ameritech has also launched a team to develop Year 2000 business continuity plans. In contrast to our business recovery plans which focus on the activities that may be required to return our operational infrastructure to working order in the event of an unforeseen failure, our business continuity plans will focus on the continuation of essential customer services and internal business functions if Ameritech is subjected to sustained disruptions of our systems, infrastructure or key services provided by our vendors.

The development of our business continuity plans is taking place in three phases:

- Phase I - Identification and Assessment



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.

- Phase II – Build and Integrate Plans
- Phase III – Test/Approve and Execute

We are continuing to evaluate the relative likelihood and anticipated impact of various Year 2000 disruption scenarios and to tailor our plans accordingly. Our current expectation is that we will complete all three phases and have a final Year 2000 business continuity plan for Ameritech in place by the end of the third quarter of 1999.

**Commercial Power Disruption Plans**

Although recent industry and other assessments of the utility sector are encouraging, Ameritech is also preparing for the possibility that commercial electric power could be disrupted during the century date transition. However, planning for this possibility this possibility is not unique to the Year 2000 in that many Ameritech operations are already prepared for a potential disruption in commercial electric power.

For example, our central office switches have diesel generators and batteries that serve as back-up power sources - - that's why Ameritech telephone service often remains uninterrupted even when storms disrupt the normal delivery of commercial electrical power. Those type of arrangements are already in place and may be bolstered where appropriate in anticipation of potential Year 2000-related disruptions in the commercial electric power supply.

**Year 2000 Telco Forum Interoperability Testing**[4]

Ameritech is a member of the Telco Year 2000 Forum ("Forum"), a nationwide group of major telecommunications companies. A major initiative of the Forum is the Network Interoperability Testing Project. This intra-network initiative is a voluntary project, entirely funded by the member companies, to test the network and various services for Year 2000 readiness. Its purpose is to verify the operation of the equipment and systems used widely by North American telephone companies.

In December of 1998, the Forum completed its Network Interoperability Testing Project. This testing effort was supervised by Telcordia (f.k.a. Bellcore) and was aimed at helping to detect Year 2000 issues within the public telecommunications network. The Forum's

[4] For additional information on the Telco Year 2000 Forum's activities see "Statement of William O. White, Member Telco Year 2000 Forum, Testimony Before the Subcommittee on Oversight of the House Committee on Ways and Means Hearing on the Year 2000 Problem and Telecommunications Systems, June 16, 1998"



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

testing effort covered a broad cross-section of services, from voice to high-speed data circuits, to complex 9-1-1 emergency services.

The goals of the testing project were:

- Test the functionality of date/time sensitive operations and, thereby,
- Minimize risk of network failures
- Minimize risk of service failures

In order to accomplish this testing without jeopardizing the integrity of their in-service networks, the Forum linked together several of the member companies' network testing laboratories, including Ameritech's.

Ameritech's test laboratory is located at its facilities in Hoffman Estates and provides a controlled environment that replicates the current Ameritech network: complete with switches, data links and other equipment. The laboratory is equipped to simulate peak traffic loads and analyze actual network performance in a trial run of such events as the turn of the century and leap year dates. The laboratory is generally used to conduct thorough testing of new network-based products before they are rolled out in Ameritech's service area and to conduct ongoing reliability testing of existing network services. Over the past six months, the laboratory has also been extensively involved in rigorously testing the Year 2000 upgrades required to make Ameritech's network Year 2000 ready.

The Forum's Network Interoperability Test Project began on July 6, 1998, and concluded, as scheduled, in December of 1998. During this initiative, over 2,000 test cases were conducted with a combined failure rate of less than 1% for Year 2000 related issues.[5] All deficiencies were referred back to the equipment providers, were addressed by those providers and have been re-tested to assure that the defect was corrected.

Additional information regarding the Forum and information regarding the Network Interoperability Testing Project, including test information documents, is currently available at the Forum internet web site (ｴﾗｰ! ﾌﾞｯｸﾏｰｸが定義されていません。).

An Ameritech representative also co-chairs the Network Testing Committee ("NTC") of Alliance for Telecommunications Industry Solutions ("ATIS") which recently completed additional national and possibly international interoperability testing of the telecommunications network.

[5] These results are very encouraging. On average, this rate of test case failure is significantly lower than historical rates for comparable types of testing.



This document and the information contained herein is intended, and for all purposes shall be deemed, a *Year 2000 statement* and a *Year 2000*

**Lessons Learned**

The Year 2000 project at Ameritech has constituted a major learning experience for us. Lessons that we have learned include:

- start your Year 2000 project early
- ensure that you have strong executive support
- ensure that you have funding available
- develop a comprehensive internal and external communications plan

**Conclusion**

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.

Thank you for the opportunity to share these thoughts with you today.



This document and the information contained herein is intended, and for all purposes shall be deemed, a *Year 2000 statement* and a *Year 2000*

Mr. BURTON. Thank you, Mr. Mitchell.

Who is next?

Mr. BEERING. Mr. Sloan from AT&T.

Mr. BURTON. Mr. Sloan.

Mr. SLOAN. Good morning. I would like to thank you, Mr. Chairman, and members of the committee, Congressmen, for allowing AT&T the opportunity to brief you on its preparation for the Y2K event.

I would like to say that several years ago AT&T recognized the importance of this Y2K event, and began by putting in place a rather extensive Y2K program. AT&T started with what I will call the executive authority or executive mandate. Our chairman, Mr. Michael Armstrong, brought together all of the different business units of AT&T, as well as the different operational-type, engineering-type people to put together a rather extensive plan.

The first step of that plan started 2 years ago in identifying all of the different relevant systems' piece parts which are necessary for AT&T's network to perform; and, therefore, for AT&T to deliver all of the services that it delivers today to its customers.

The slide above gives you a brief review of those different systems, and as you can see, it starts off with different software programs which AT&T has written to run its network, to bill for services rendered, and to provision those services.

Next drop down to the internal computer infrastructure which AT&T uses to run its day-to-day business; that would be our own local area networks and PCs that we use. Then there is the traditional gold-plated AT&T long distance network, which would include both the voice network, you are most familiar with, as well as all of the advanced ATM, frame relay and data networks. And then finally, there are very simple things like burglar alarms, air conditioning, heating, ventilation, things that are absolutely necessary for our buildings to operate.

I would like to give you an idea of the immensity and complexity of the AT&T program. And as a, what I will call "a phone company," our tasks are somewhat similar to what Ameritech would have to do. We have literally gone through our entire network. We have inventoried all of the different pieces of plug-in equipment, vendor equipment, fiber optic equipment, digital equipment. Everything was—had to be inventoried and assessed for its impact on services if, in fact, there was a Y2K problem.

Upon inventory completion, there had to be an assessment of each and every piece of equipment in the AT&T network for its vulnerability and then a separate test plan, and contingency plan put in place.

At this point in time, I would like to state that the network has been completely tested, and I qualify that by saying the AT&T network. In addition to working on our own internal issues, our chairman is the chair of the Network Reliability and Interoperability Council, and it is through this council that we work very closely with other companies, such as GTE, Ameritech, traditional phone companies. We work very closely with vendors who provide telco equipment—Lucent Technologies, Ascend—pretty much anyone who is in the telephone business providing equipment to AT&T and other phone companies.

And it is very important to us that not only the AT&T network be certified, but that by working very closely with our vendors—and we trust our vendors—but by working very closely with our vendors we agree that their equipment is Y2K complaint and, therefore, will work with our own network.

In addition, International Forums was mentioned by one of my colleagues, International Forums. Let me just state that both on a national level, as well as internationally, we are meeting, and sharing information. And at this point in time we are testing our networks and the services that ride on those networks across an AT&T environment, through for example, an Ameritech environment, into customer provided equipment, such that we can feel fairly confident that after the Y2K event, services will be delivered all the way, end-to-end, to customers without any interruption.

Most of the things that we have started have been completed already, and there are a few things yet to be done. Items we are still doing include final contingency planning and this end-to-end testing. We have done the network end-to-end testing, and now we are working on the international end-to-end testing making sure that calls, data, other information, can reach from, say, a New York to a Paris, a Tokyo to a California. We expect the completion of AT&T's Y2K work, including all of the contingency planning, to be complete by the late spring of 1999.

I would just like to summarize that we have made quite significant progress to date, and that all of the AT&T upper management, including its CEO, are very actively engaged. Funding was released for this program several years ago. AT&T has spent hundreds of millions of dollars, and we expect all of our testing and work to be complete very shortly this year.

I would like to thank the committee for this opportunity.

Mr. BURTON. Thank you, Mr. Sloan.

Mr. BEERING. Mr. Edwards.

Mr. EDWARDS. Chairman Burton, Congressman Horn, Congressman McIntosh, good morning. My name is John Edwards, project manager of the year 2000 program for Citizens Gas and Coke Utility. Citizens Gas has for over 100 years provided safe, dependable natural gas service to the residents of Marion County. Citizens values the relationship with our customers, the trust placed in us by them, and the high level of service expected by them, very seriously.

As you might expect, we have established operating plans which deal with severe weather, natural disaster and general equipment malfunctions. We have established plans to recover those systems necessary to conduct business in such emergencies. These plans allow us to maintain service and make it virtually transparent to the customer when difficulties occur. Our approach to the year 2000 issue is an extension of this mature process.

While somewhat simplistic, there are two basic questions around which we are developing our contingency plans. "What does it take to maintain gas service to the customer?" And, "What does it take to run the business?"

In general, the gas distribution system operates primarily on pressure demand and is not date-time dependent. Equipment used to control the pressure operates pneumatically. Certain critical ap-

plications have a level of redundancy and everything is capable of operating in a manual mode. Ultimately, the decision process is controlled by a human.

Mr. Chairman, the following two slides have been extracted from an AGA presentation made to the FERC earlier this year. This specific diagram represents the extent of the natural gas distribution network on a national basis. The following is a slide which depicts the year 2000 readiness based on AGA's latest survey information. I believe you might be familiar with this information, so I will not cover it today.

Translating into something a little bit closer to home, our ability to maintain and in some cases enhance the reliability of our business include: our major business systems, with the exception of our customer information system, now operate using client-server-based technology. The significance is we are no longer tied to the old legacy mainframe system with extensive lines of custom code which are susceptible to the year 2000 problem.

Recently, all desktop PCs were replaced, along with a standardization on the Microsoft suite of office products, including the NT operating system. We are in the process of upgrading both our customer information system and our internal telecommunication system. Combined, these two systems represent the most critical business systems to our operation.

Our CIS system is currently a legacy mainframe application, which is being transferred to a vended solution, which is client-server based. However, the old system, which is the legacy mainframe system, is being tested as a contingency, on the off chance that the new system is not up and running. So we have ourselves covered on both sides.

Operational readiness relates directly to our ability to maintain gas service to the customer. This system is concerned with both the technical side of mitigating the operational risks, reducing the possibility of a failure, as well as consequence management aspect, the actions we take if it does fail. The activities highlighted allow us to monitor our gas distribution system and safely deliver gas to our customer. Developing specific contingency actions, managing our gas supply portfolio, and having the personnel available to respond are all necessary parts of the overall process.

The sum of our presentation is whether gas will flow on January 1st. Citizens, and the gas industry as a whole, is very confident in its ability to maintain service to the customer. In summary, we view this issue as a real concern at all levels of the organization. We are actively working on remediation. We do not expect problems. However, at the same time, we are developing the necessary contingency plans just in case.

Mr. Chairman, that concludes my remarks. And I thank the committee for the opportunity to speak.

Mr. BURTON. Thank you.

Mr. BEERING. Mr. Gustin.

Mr. GUSTIN. Chairman Burton, members of the committee, thank you for allowing us to provide testimony at this field hearing today. My name is Joe Gustin, and I am vice president of information services; and I am also the officer in charge of the Y2K readiness efforts at Indianapolis Power and Light Co.

Our year 2000 efforts are directed by an ad hoc steering committee comprised exclusively of corporate officers; that committee meets regularly and provides a general oversight to the Y2K efforts of the corporation. Reporting to that steering committee is a compliance testing committee and a contingency planning group. In all, we have 43 employees with direct responsibility to those three committees, and another 100 to 150 employees in the field and in our generating plants actually performing the testing.

Mr. BURTON. I would ask that you would just take the microphone and bring it up so the back row can hear. Just move it.

Is that better? Great.

Mr. GUSTIN. We have 43 employees that have a direct responsibility to these three committees and another 100 to 150 employees in the field doing the actual testing, remediation, and planning.

Our compliance testing committee is responsible for searching all areas of our business and all of our business functions that have a possibility of being affected by the year 2000. Things such as computers, computer programs, vendors that provide critical services and equipment with date-sensitive embedded computer chips all have the potential of impairing our ability to provide electric service to our customers. That inventory is essentially complete, with those items being ranked as either critical or noncritical to our business. Parenthetically, I would say that we class this inventory as "essentially" complete because I think it is important that throughout this process we always continue to look for problems in our business.

Our assessment of those points are complete as well, and we are well into remediating those systems that we knew either up front were not Y2K compliant or that have failed our testing protocol. We anticipate having all of those critical systems ready and Y2K compliant. We have also contacted over 100 critical vendors, and we have received statements from many of those vendors stating they will be compliant and provide services into the new millennium. And we continue to work with remaining vendors to assess their individual states of readiness.

Contingency planning is our second line of defense in the event compliance testing overlooked a point in the inventory process, or if a point was remediated improperly, or in the event that there is a disturbance from outside our service territory that comes in to us through the grid. We have identified roughly 50 core business functions and we have Y2K contingency plans for all of those systems.

We expect the testing and validation of those plans to be complete by the end of the second quarter. Concurrently, we are conducting testing on the plans that are finished and we expect to have all of our training finished by the end of the third quarter. We then the fourth quarter this year to do the final staging, preparation and rehearsal.

I would like to talk about three issues that are critical to IPL and our ability to provide electricity to our customers. Electric utilities are connected to a common transmission grid that traverses the entire country. And because of this interconnection, there is a possibility that faults in one system can travel through the grid and enter another system through the points of interconnection. It is because of this possibility that the North American Electric Reli-

ability Council, NERC, and the Department of Energy are closely monitoring the progress of all electric utilities in conducting coordinated contingency planning drills.

The next slide shows the geographical division of NERC. Indiana is part of the East Central Area of Reliability council, ECAR. We submit monthly reports to ECAR stating our readiness and what we have accomplished. ECAR compiles those reports and responses from all of the member utilities and sends a monthly report to NERC. And then NERC, as you know, sends quarterly reports of this progress to the Department of Energy.

At Indianapolis Power and Light Co., we have a very sophisticated energy management system that maintains system frequency by balancing the flows of electricity into and out of our system with our customer load and the amount of electricity being generated by our units. We have tested, remediated, and retested this energy management system, and we are pleased to report that this very critical system has been successfully operated for an extended period of time in the year 2000. We participated in the NERC April 9th drill to test the contingency plans for loss of normal communications. This test simulated complete loss of traditional communications between generating stations, substations and central operating centers. That test for us was an unqualified success. We were able to control and dispatch our entire electric system using Y2K-compliant backup communications.

On September 8th and 9th, there will be another drill. And that drill will be essentially a full dress rehearsal for the utility industry. We will also participate in that.

As far as generation is concerned, all of our major generating units over 50 megawatts have been operated in the year 2000 as part of our testing protocol. All but one of those units are currently operating in the year 2000 date mode, and we intend to leave them in that mode until after the real year 2000 arrives; then their internal clocks will be reset to actual time. We have contingency plans in place for those units, and they are being tested now and we will be able to launch those if necessary.

And finally, I would like to turn to business functions. Last year we began converting all of our legacy mainframe systems to Y2K-ready Oracle financials. We finished that conversion at the end of 1998. And on January 4th of this year we went live with all of our financials on that Oracle system.

Our service restoration program still resides on the mainframe computer. This is the program we use in the event of an outage to track incoming calls, analyze outage patterns, and help dispatch our crews to efficiently restore service. That program has been converted to a Y2K compliant version.

Our shareholder services program will also remain on the mainframe, and it too has been converted to Y2K-compliant conversion.

Finally, our customer billing system is the last major program that will remain on the mainframe. We are in the process of remediating that legacy system right now and expect to finish that effort within the next 30 to 40 days.

So, in summary, Indianapolis Power and Light, has a Y2K plan in place, and that plan is very active. It has high visibility, and high priority within our corporation. We have successfully com-

pleted the April 9th drill and will participate in the September 8th and 9th drill. We are actively engaged with other city utilities and the Metropolitan Emergency Management Group, coordinating our respective year 2000 contingency plans. And our goal is to have all our critical systems ready to go by June 30.

Thank you.

Mr. BURTON. Thank you, Mr. Gustin.

Mr. BEERING. Mr. Miller from the Indianapolis Water Co.

Mr. MILLER. Mr. Chairman, thank you for this opportunity to tell you how Indianapolis Water is prepared for the year 2000.

We are the largest private investor-owned water utility serving a metropolitan area. We have been serving Indianapolis since 1881. Today, we have an average demand of 132 million gallons a day serving over 240,000 customers. Our primary source of supply is here locally, consisting of three reservoirs, each with a capacity of 7 billion gallons and one ground water major source on the south side of Indianapolis, which, when filled out, will have the capability of 80 million gallons a day capacity.

We have been working closely with the other utilities to identify critical facilities for the past year. And internally we have been checking out our pump valve and purification control, hardware and software for year 2000 compliant. And we are in the process of updating our latest little item, which is a $700 auto dialer.

Our internal IT people, they are working on the software for billing and customer service, and that will be completed by—June 1st is their target deadline. We have 6 million gallons of elevated storage of water, and another 60 million gallons of underground finish water that can be pumped into the system.

At our major facilities, we have diesel generators to drive the treatment process and engine-driven pumps to pump the water out into the system, should we lose power or there be a major ice storm or any other natural emergency. We have 3 days' of fuel at these facilities and we will have arrangements for additional fuel tankers to be on the property should an event occur and last of any length.

In summary, Indianapolis Water has an average day demand of 132 million gallons a day. We anticipate on a typical New Year's Eve, usage of 100 million gallons, and with our generators and pumps, we can treat and pump 160 million gallons a day into the system, ensuring that these flows will assure to the community adequate fire protection and normal water usage.

Thank you.

Mr. BURTON. Thank you.

[The presentation of Messrs. Beering, Miller, Edwards, Gustin, Mitchell, and Sloan follows:]

Ameritech®

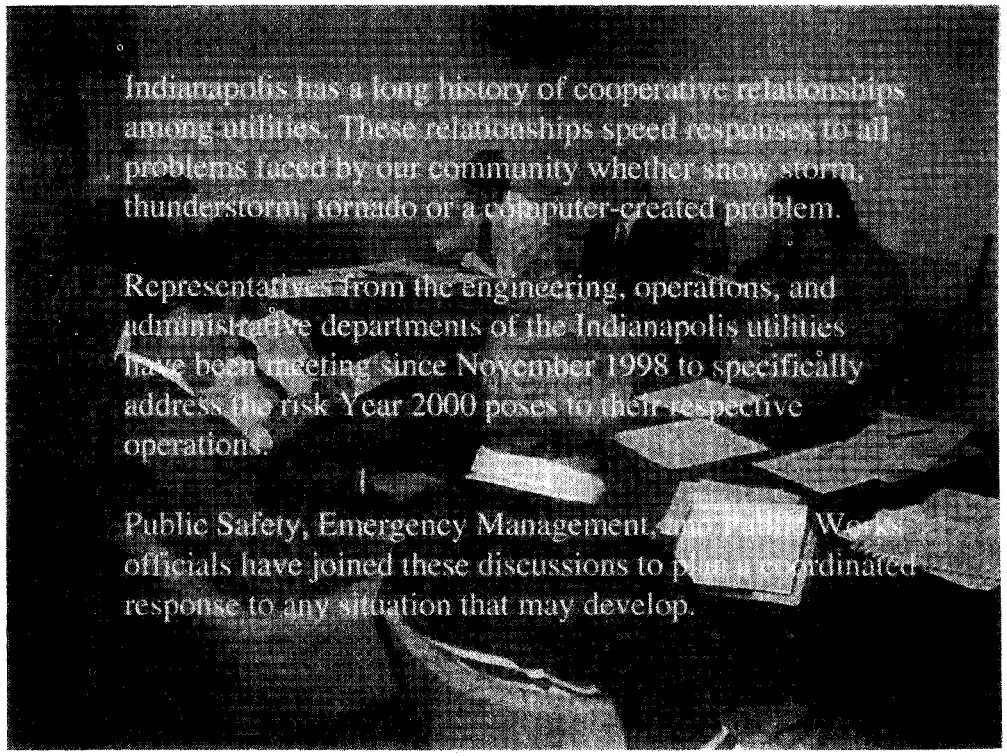
AT&T

citizens gas

# Indianapolis Utilities Year 2000 Readiness Group

IPL

INDIANAPOLIS WATER COMPANY


Indianapolis has a long history of cooperative relationships among utilities. These relationships speed responses to all problems faced by our community whether snow storm, thunderstorm, tornado or a computer-created problem.
Representatives from the engineering, operations, and administrative departments of the Indianapolis utilities have been meeting since November 1998 to specifically address the risk Year 2000 poses to their respective operations.
Public Safety, Emergency Management, and Public Works officials have joined these discussions to plan a coordinated response to any situation that may develop.

# Compliance Testing

- Each utility has evaluated and ranked potential problem systems
- Once identified, the systems are being tested and assessed for compliance
- Remediation is well underway on affected systems
- Systems are being re-tested once remediated
- Testing methodology includes critical dates and operating in post-2000 time frame



This material constitutes Year 2000 Readiness Disclosure

# Contingency Planning

- Each utility has identified and shared key facilities locations
- Contingency planning efforts are being coordinated with city and county officials.
- Emergency communications are being planned with other utilities, utility employees, and with customers for outage reports.
- Mission critical functions, facilities, and supplies are being identified and procured.
- Plans include staffing, production, distribution, and billing operations

# Communications

•Each utility is cooperating with the Indiana Utility Regulatory Commission (IURC) as to Year 2000 testing, remediation and contingency planning.

•Employees are being briefed and key employees are being identified for response to outages that may occur.

•Media information is being provided in a timely way by all participating utilities. Customer communications are being handled by the respective utilities.

•Indianapolis utilities are participating in national coalitions assisting smaller utilities in surrounding communities.

Ameritech is committed to ensuring that the Year 2000 event is transparent to Ameritech and its customers

- Ameritech has a strong Year 2000 Initiative in place with full executive support.
- Mission-critical systems remediation effort is 98% complete.
- Any remaining remediation activity, testing and deployment will be completed well in advance of the century date change.
- Testing strategy is well-defined and on-going for mission-critical components.
- Contingency planning efforts both inside and outside the company are underway.

Ameritech®

# Ameritech Year 2000 Initiative

- Ameritech is encouraging cities, businesses, and others to review their own communications' equipment to verify they are Y2K ready.
- Ameritech has year 2000 partnerships with the following:
  - Year 2000 Telco Forum - a consortium of 8 telephone companies
  - Alliance for Telecommunications industry solutions - network interoperability testing
  - FCC sponsored Network Reliability and Interoperability Council
  - International Telecommunications Union
  - The Indianapolis Utilities
- .For more information see www.ameritech.com/y2k

Ameritech®

YEAR 2000

AT&T

*Year 2000 Program Update*

AT&T

# Program Focus

YEAR 2000

| | |
|---|---|
| AT&T-Developed Applications | **Software written by AT&T to support business functions such as ordering, provisioning, billing, payroll, etc. Also includes external data interfaces (e.g., data from LECs, PTTs, telemarketing groups) critical to the running of the application.** |
| **Computing Platforms/ IT Infrastructure** | Hardware, software and communications platforms/ components that support the applications, including common modules; third-party software, such as compilers, database managers; mainframe and server processors; operating systems; communications software. Also includes desktop platforms and local area networks, as well as premises voice/data systems |
| **AT&T Networks** | All network elements, such as 5ESS, conversants, network servers, and operation support systems which directly support the daily operation of the AT&T Worldwide Intelligent Network. Also includes BOU-specific networks, e.g., Frame Relay data network, 5E-OSPS network for 0+ and calling cards. |
| **Non-IT Infrastructure** | AT&T's internal infrastructure, including building automation systems (e.g., security systems, heating, ventilation and air-conditioning systems, elevators, time clocks, etc.) and other non-IT categories like corporate aircraft and multimedia products / services. |

AT&T

# Network Certification Plan

YEAR 2000

- Extensive inventorying of all components/interfaces
- Thorough vendor/AT&T assessments
- Compliance testing of all components/interfaces
- Integration testing of network components and adjacent elements
- Risk assessment of network plans
- Contingency planning for critical components

Network element and operations support system (NE/OS) certification completed by December 1998

AT&T

## Network Reliability and Interoperability Council

YEAR 2000

**Strategy**

- Promote information sharing and joint planning
- Identify testing and contingency plan gaps and formulate solutions

**Communication**

- Public council meetings
- Meeting minutes available at www.nric.org

**Members**

- Local carriers, inter-exchange carriers, equipment suppliers, wireless carriers, cable companies, satellite companies, standards and research groups, trade associations, consumers
- Chaired by Mike Armstrong, AT&T Chairman and CEO

AT&T

YEAR 2000

# Program Completion

***1999 targeted for final assurance of Y2K-compliance ...***

- Independent verification of critical applications
- Deployment of all applications in Y2K-certified production environments
- Deployment of all Y2K-certified network elements
- All AT&T sites (non-IT infrastructure) certified Y2K-compliant
- End-to-end testing completed for applications, environments, systems, …
- Network interoperability testing
- Y2K-specific contingency plans certified and tested

AT&T

# Summary

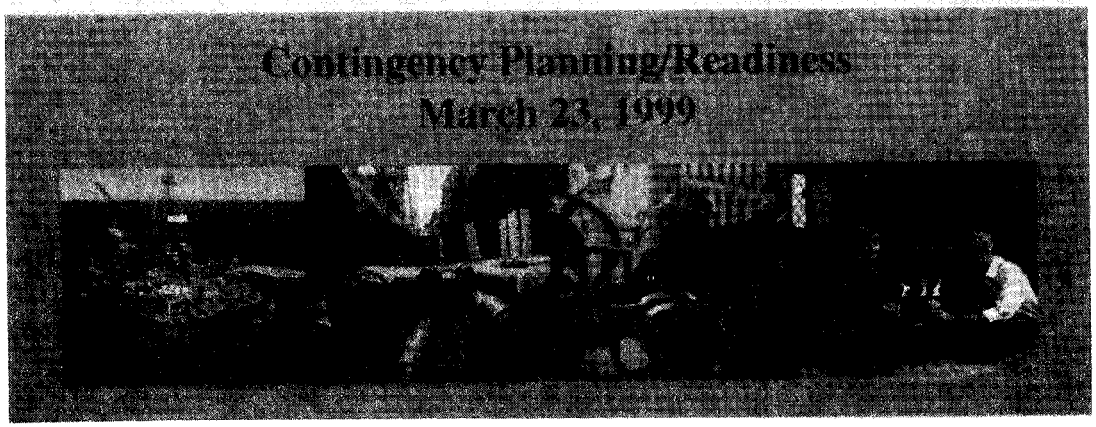
YEAR 2000

- Significant progress to date -- on target to meet objectives
- Centralized program management / decentralized implementation
- Board of Directors / CEO engaged
- Triaging -- customer-driven priorities
- Funding/objectives assurance
- Interoperability testing / contingency plans being defined for early 1999

***The AT&T Y2K program will be successful!***

citizens gas

# Contingency Planning/Readiness
March 23, 1999



# Contingency Planning Framework

Citizens Gas has developed the following:

Business Recovery Plan

Severe Weather Plan

Equipment Malfunction Plan

Natural Disaster/Emergency Plan

Year 2000 Plan

- Unique Aspects
- Collaborative Emphasis

citizens gas

# Mission Critical Processes

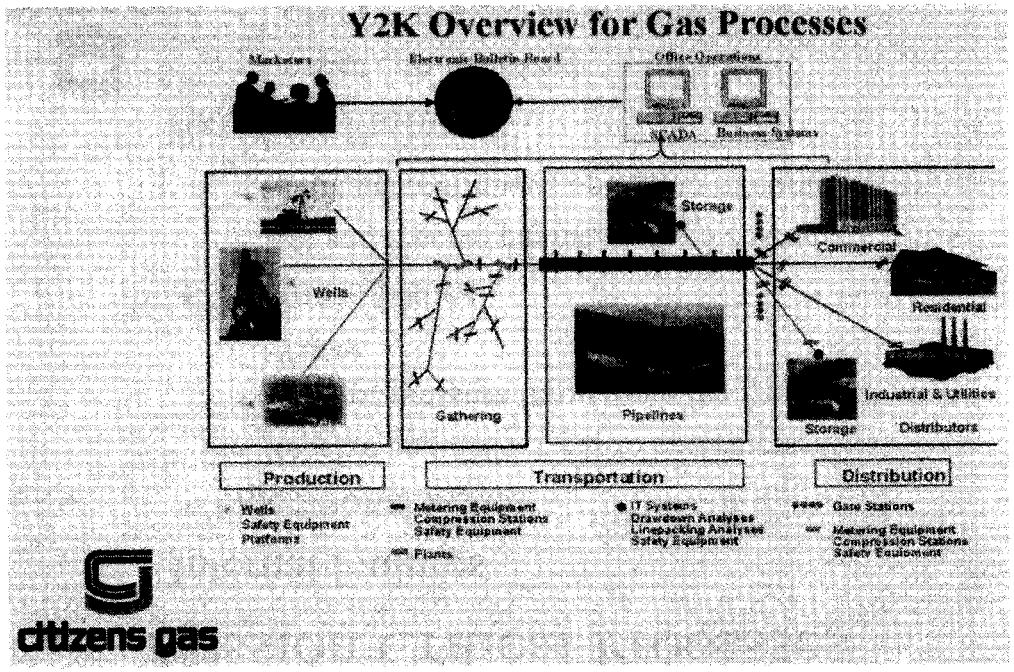
## Internal Failures

- Operational Issues
  - Receive and deliver gas to customers
  - Monitor pressure throughout the gas distribution system
- Business Issues
  - Bill and receive payments from customers
  - Maintain continuous operation of computer systems

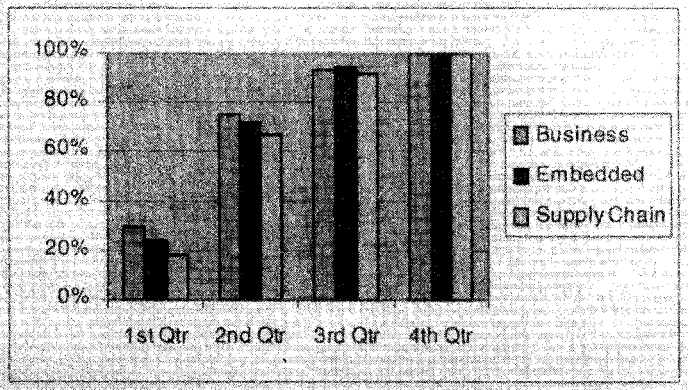
## External Failures

- Loss of customer load
- Loss of critical business partner

citizens gas


Y2K Overview for Gas Processes
Wells
Gathering
Storage
Pipelines
Commercial
Residential
Industrial & Utilities
Storage
Distributors
Production
Transportation
Distribution
Wells
Safety Equipment
Platforms
Metering Equipment
Compression Stations
Safety Equipment
Plants
IT Systems
Drawdown Analyses
Linepacking Analyses
Safety Equipment
Gate Stations
Metering Equipment
Compression Stations
Safety Equipment
citizens gas

# Gas Industry Y2K Readiness




American Gas Association Presentation to FERC

Oil/Gas Industry Survey - February 1999

citizens gas

# Business System Readiness

Highlights

- Overall move toward client/server technology
- Standardization on Microsoft Windows NT operating system and Microsoft Office Products
- Customer Information System Upgrade
- Upgrade of internal telecommunications system
- Contingency plans based on worst case assumptions

citizens gas

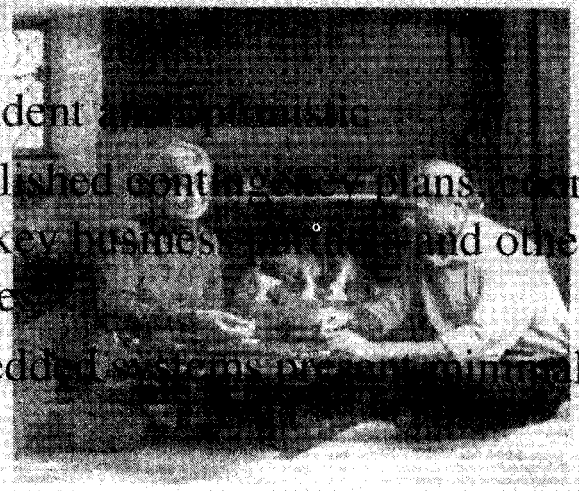
# Operational Readiness

Highlights of compliance activity:

- Gas supply strategies based on various scenarios
- Supervisory Control/Data Acquisition (SCADA)
- 800MHZ Trunked Radio System
- Use of [illegible] itate testing of [illegible] systems
- Su[illegible] analysis
- Documentation of specific contingency actions
- Personnel availability

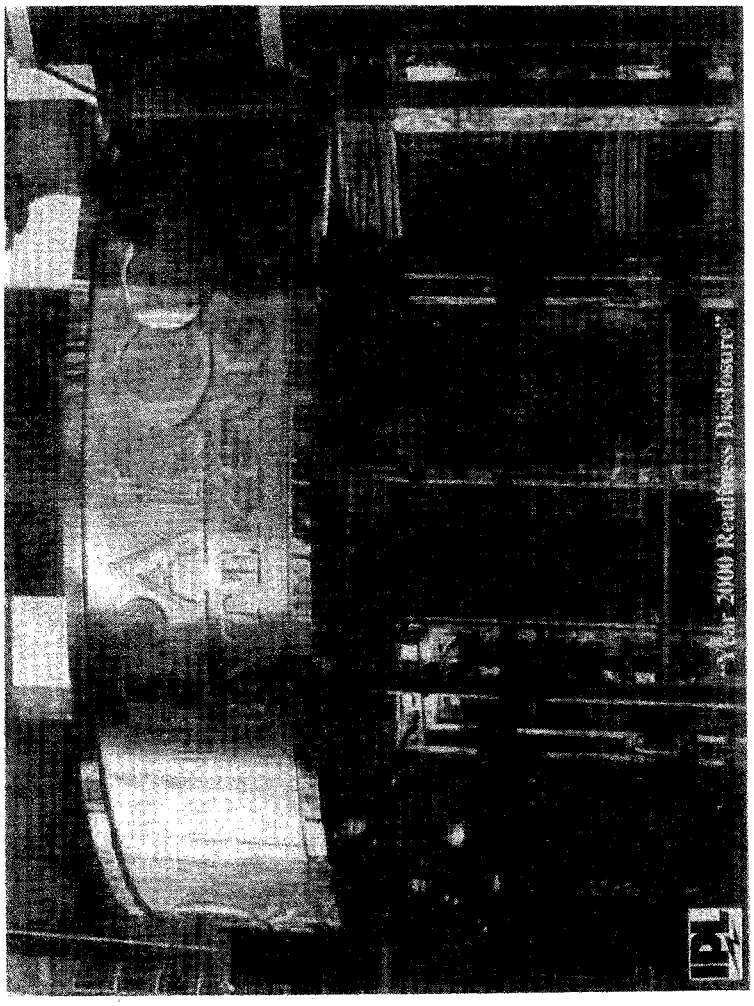
citizens gas

# Will gas flow on January 1, 2000?



- Confident and optimistic
- Established contingency plans, coordination with key business partners and other utilities
- Embedded systems prevent minimal risk

citizens gas


Year 2000 Readiness Disclosure

- Inventory of Number of Systems Completed
- Ranking, Testing/Assessment Complete
- Remediation in Progress
- Goal - All Critical Systems Compliant by 6/30/99
- Critical Vendors have been Identified / Contacted

IPL

"Year 2000 Readiness Disclosure"

- Core Business Functions Identified
- All Contingency Plans for Critical Systems Complete
- Testing to be Finished by End of 2nd Q
- Training to be Finished by End of 3rd Q
- Final Staging and Preparation During 4th Q

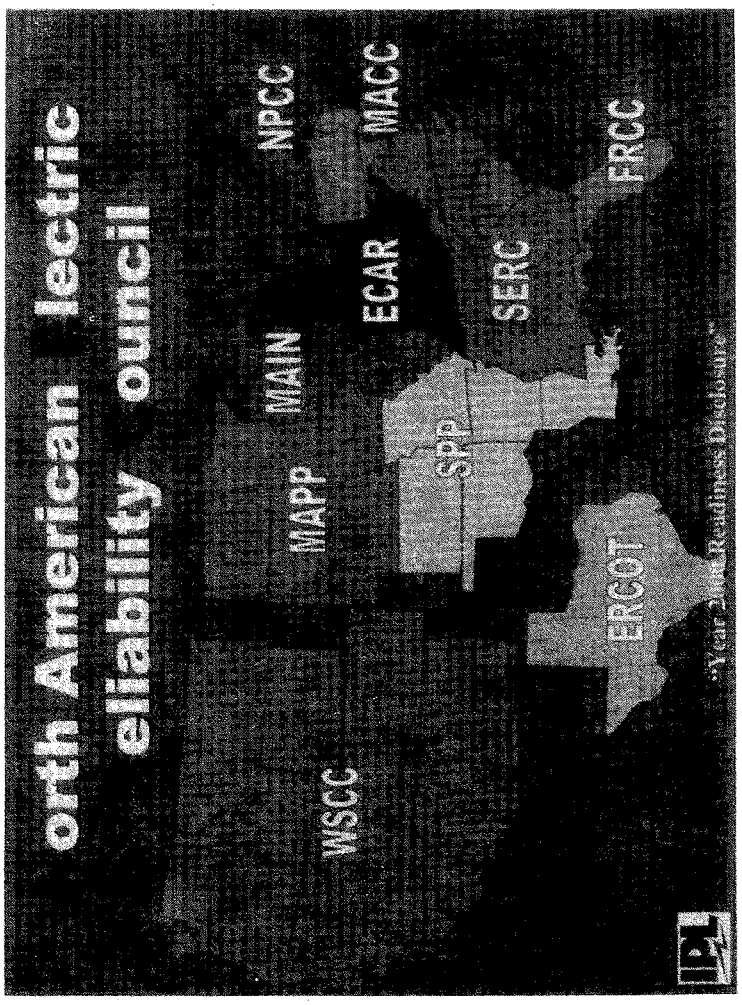
IPL

"Year 2000 Readiness Disclosure"

- U.S. Electric Grids Interconnected via Common Transmission Network
- National Preparation Coordinated by North American Electric Reliability Council (NERC) at request of DOE
- Regional Reliability Councils coordinate contingency plans

IPL

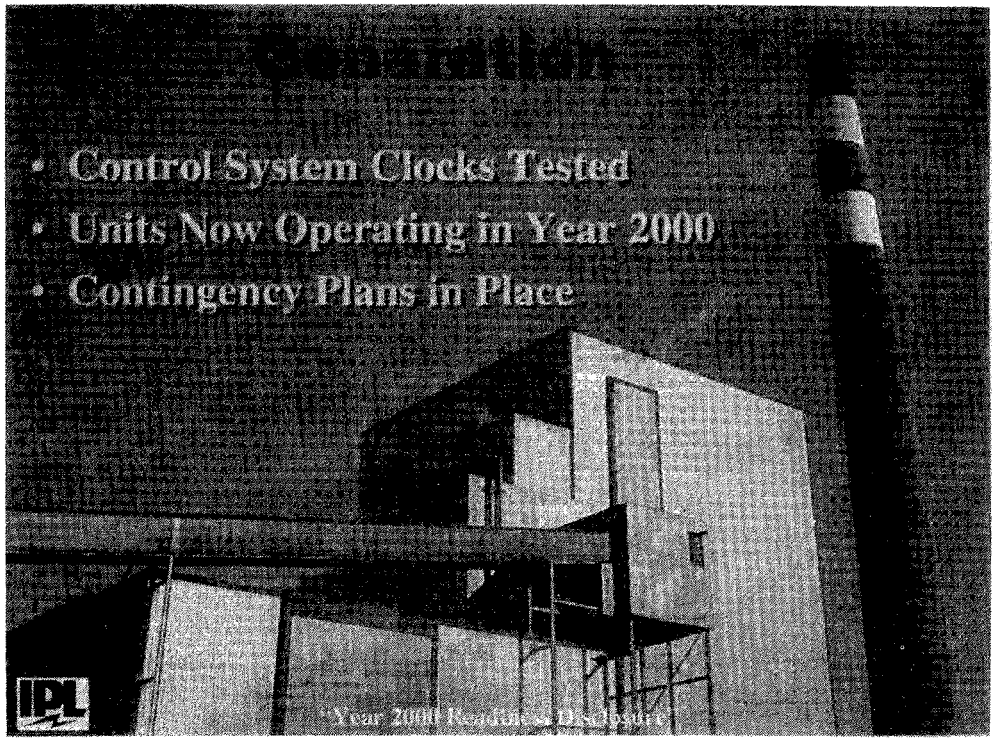
"Year 2000 Readiness Disclosure"

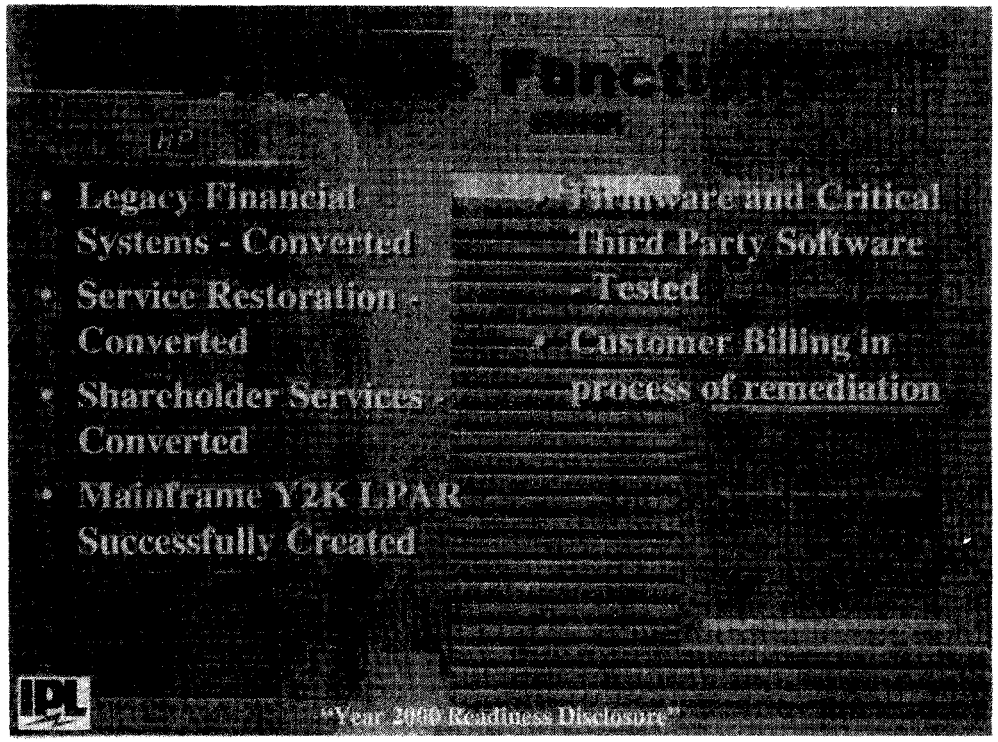

orth American lectric
eliability ouncil
WSCC
MAPP
MAIN
NPCC
SPP
ECAR
MACC
SERC
ERCOT
FRCC
"Year 2000 Readiness Disclosure"

- EMS System Successfully Operated in Y2000
- Delivery Systems ~ 95% Ready
- Contingency Plans have been Written
- Plans have been Submitted to ECAR
- ECAR Testing 4/9 and 9/8-9
- Black Start Capability Exists

IPL

"Year 2000 Readiness Disclosure"

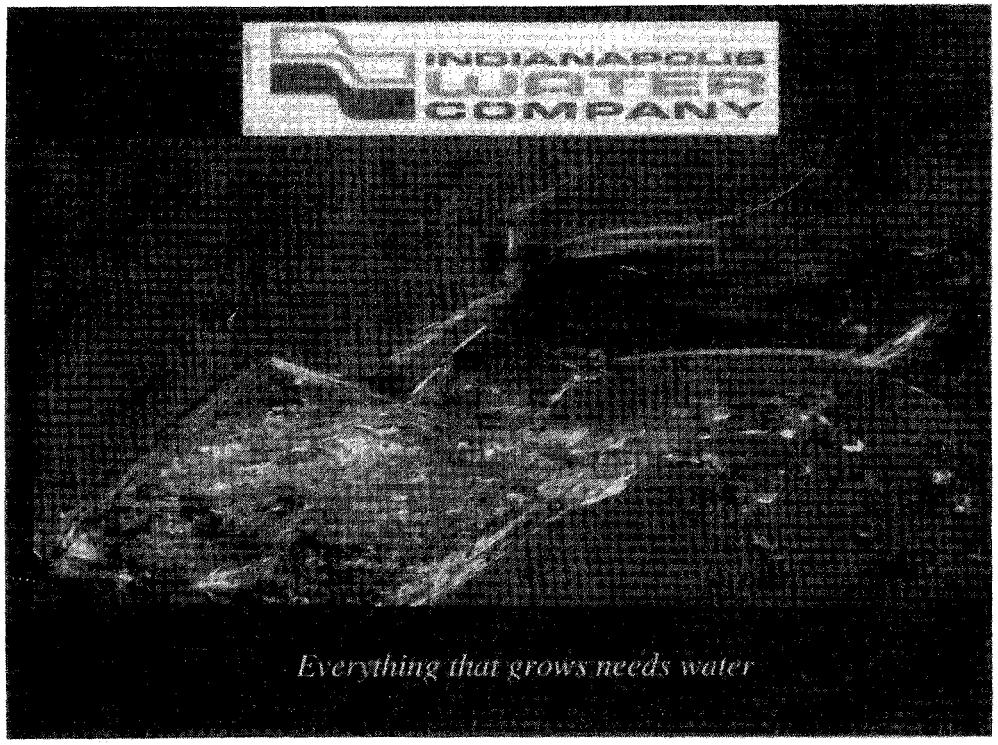

Generation
• Control System Clocks Tested
• Units Now Operating in Year 2000
• Contingency Plans in Place
IPL
Year 2000 Readiness Disclosure

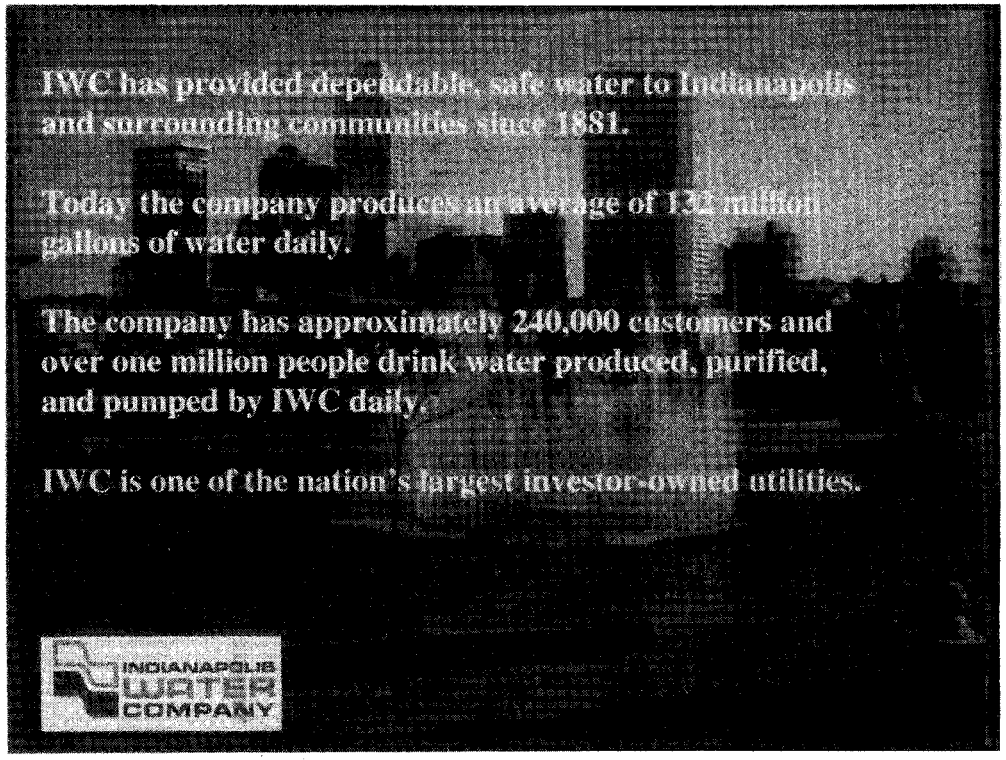

Legacy Financial Systems - Converted
Service Restoration - Converted
Shareholder Services - Converted
Mainframe Y2K LPAR Successfully Created
Firmware and Critical Third Party Software - Tested
Customer Billing in process of remediation
IPL
"Year 2000 Readiness Disclosure"

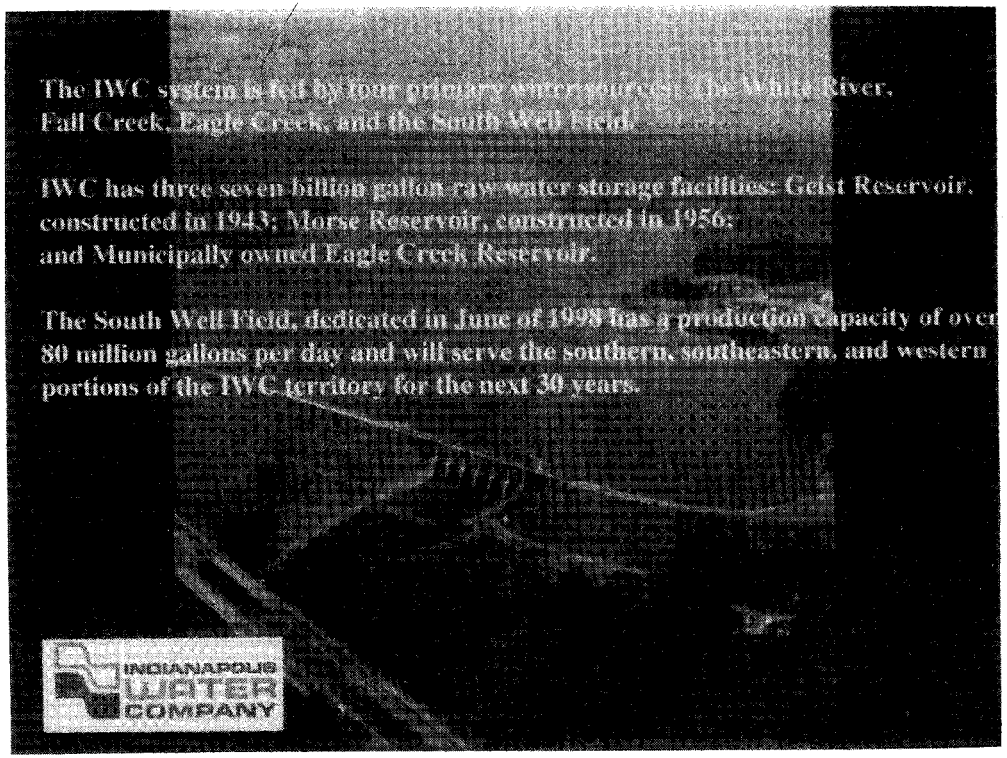
- Y 2K Plan In place and Active
- High Visibility / High Priority
- Industry Wide (ECAR) Tests 4/9 and 9/8-9
- Integrated Preparation with other City Utilities and Emergency Management Infrastructure
- Goal - All Critical Systems Ready by June 30th

IPL

"Year 2000 Readiness Disclosure"


INDIANAPOLIS
WATER
COMPANY
Everything that grows needs water


IWC has provided dependable, safe water to Indianapolis and surrounding communities since 1881.
Today the company produces an average of 132 million gallons of water daily.
The company has approximately 240,000 customers and over one million people drink water produced, purified, and pumped by IWC daily.
IWC is one of the nation's largest investor-owned utilities.
INDIANAPOLIS WATER COMPANY

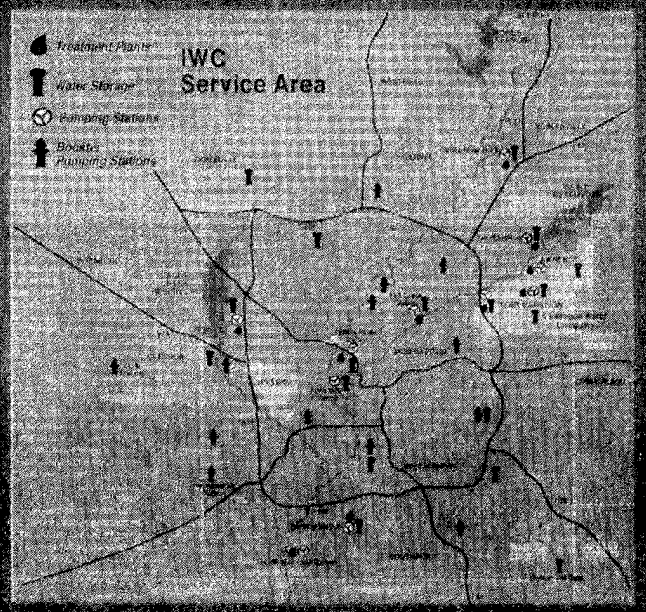

The IWC system is fed by four primary water sources: the White River,
Fall Creek, Eagle Creek, and the South Well Field.
IWC has three seven billion gallon raw water storage facilities: Geist Reservoir,
constructed in 1943; Morse Reservoir, constructed in 1956;
and Municipally owned Eagle Creek Reservoir.
The South Well Field, dedicated in June of 1998 has a production capacity of over
80 million gallons per day and will serve the southern, southeastern, and western
portions of the IWC territory for the next 30 years.
INDIANAPOLIS
WATER
COMPANY



98

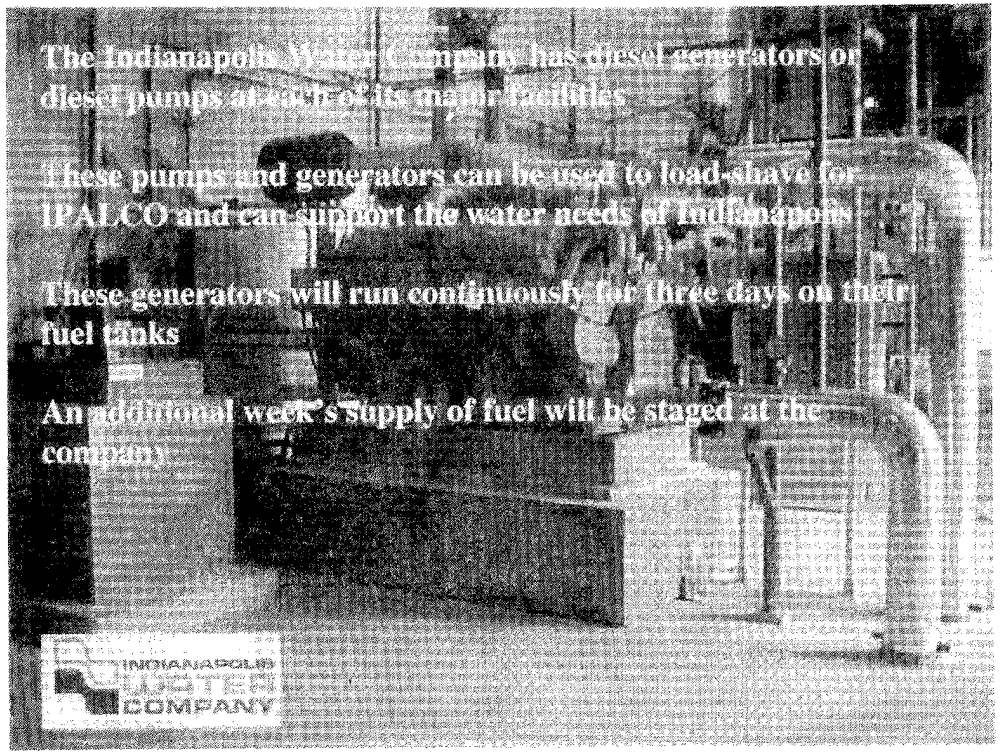
The Indianapolis Water Company has been working closely with the other utilities to identify critical facilities for the past year.

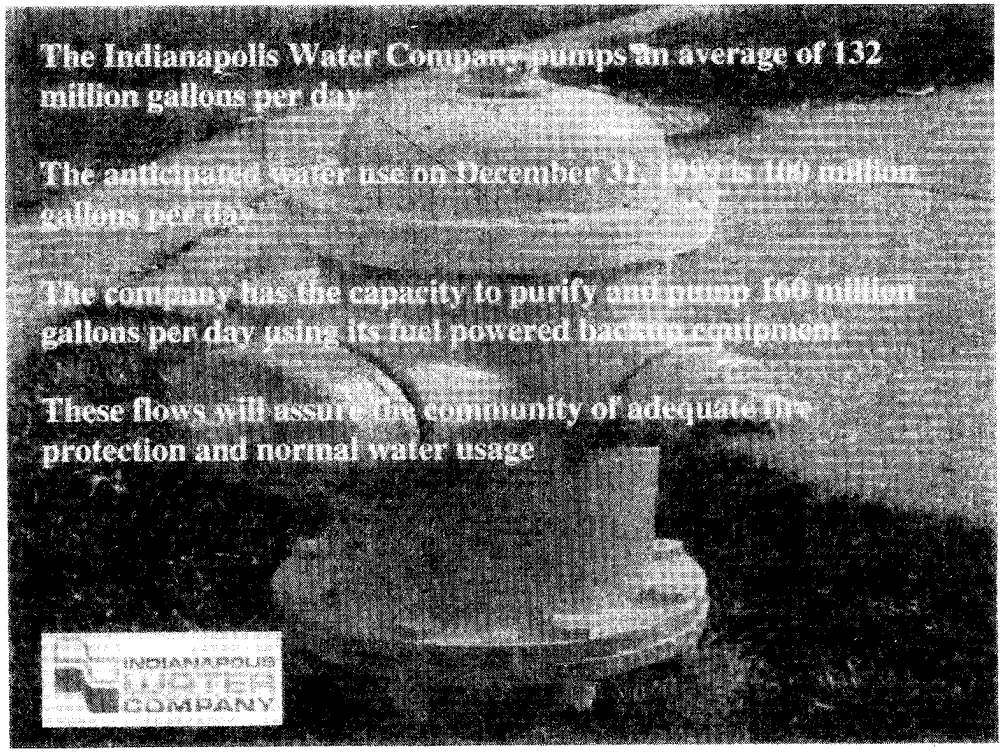
The pump, valve, and purification control hardware and software have been evaluated for both year 2000 compliance and embedded chip compliance

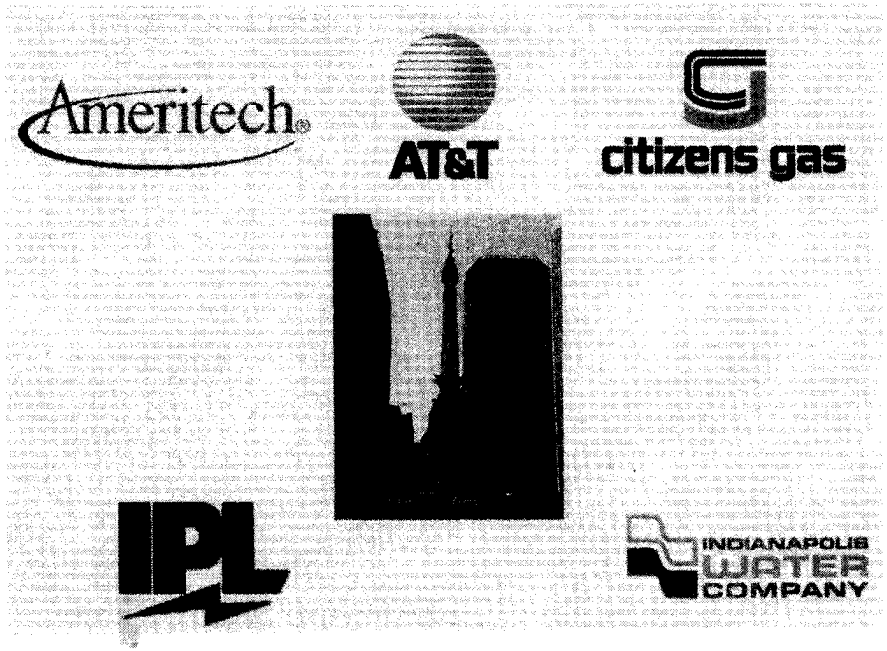



INDIANAPOLIS WATER COMPANY

INDIANAPOLIS
LUBRICANTS
COMPANY


The Indianapolis Water Company has diesel generators or diesel pumps at each of its major facilities
These pumps and generators can be used to load-shave for IPALCO and can support the water needs of Indianapolis
These generators will run continuously for three days on their fuel tanks
An additional week's supply of fuel will be staged at the company
INDIANAPOLIS WATER COMPANY


The Indianapolis Water Company pumps an average of 132 million gallons per day
The anticipated water use on December 31, 1999 is 180 million gallons per day
The company has the capacity to purify and pump 160 million gallons per day using its fuel powered backup equipment
These flows will assure the community of adequate fire protection and normal water usage
INDIANAPOLIS
WATER
COMPANY


Ameritech
AT&T
citizens gas
IPL
INDIANAPOLIS
WATER
COMPANY

Mr. BEERING. Mr. Chairman, that concludes the formal presentation on the part of the utilities panel. We would be happy to field any questions that you or your colleagues may have.

Mr. BURTON. Thank you.

You can turn the lights up a bit now. Mr. Horn, do you want to start with the questions?

Mr. HORN. Actually, I would be glad to yield to Mr. McIntosh. If he doesn't cover something, why I will be glad to jump in.

Mr. MCINTOSH. Thank you. I had just a couple of questions that came up as a result of the presentation, which I thought were very impressive.

You mentioned, Mr. Mitchell, that you had been working with your customers on making sure that the equipment that they own and operate, that they are aware of potential problems. What are you finding in that inventory?

I imagine there is a range from some equipment that is Y2K compliant and some that isn't anywhere near it. How would you evaluate the risks to the system and the different customer equipment that you are aware of?

Mr. MITCHELL. As you said, Congressman, it is all of the above. Those items and pieces of equipment, or pieces of telecommunications equipment that might connect to our network, we are listing those on our Web site. We are informing customers as we interface with them. The volume of that, the size of the problem, is not overwhelming. I wouldn't be able to put a percentage on it at this time.

Mr. MCINTOSH. Is most of it business customers that have, say, Centrex or other types of exchanges?

Mr. MITCHELL. Primary PBXs, private lines, that kind of thing. They need to be aware primarily.

Mr. MCINTOSH. How about for residential users? Is there a list of different fax machines or telephones that they might have that you guys keep track of, some of the companies said, these work, and others you don't have information on?

Mr. MITCHELL. Yes. Others we don't have information on; that is correct.

The other piece of information you should be aware of is the equipment itself may indeed work after the year 2000, but certain functions that are time and date sensitive stamp may not. Such as, When did the fax come in? It may have come in on January 1, 1900, based on the date on the top of the fax, but it indeed came in.

Mr. MCINTOSH. Right. So people will have to figure out their own systems and take a look at them and see what they might need to do, correct minor problems like that.

Mr. MITCHELL. That is what we are recommending, yes.

Mr. MCINTOSH. Do you plan to do any mailings or distribution to your customers with that information?

Mr. MITCHELL. We have some mailings that we will be doing, particularly on the equipment we own, for instance, with 911 systems. We have several different manufacturers of the equipment. We don't do manufacturing ourselves, so when we complete all the 911 systems that are manufactured by Lucent, when we know

those are Y2K ready, we send out a mass mailing to the 911 systems.

We have got about 850 public safety agencies we support in the five-State area Ameritech operates in. So we will be sending those out in May.

Mr. MCINTOSH. The only other question I want to ask at this point was to Mr. Edwards.

I noted you indicated that you had changed your computer and were keeping the legacy computer in place. Do you see other benefits, essentially for that changeover, that perhaps were spurred on by the necessity of being Y2K compliant?

Mr. EDWARDS. Of maintaining the legacy system?

Mr. MCINTOSH. No, of transferring to the new one.

Mr. EDWARDS. It is a realization of greater business technology more than anything. That is really what drove the process to move, to being that transformation of going from the legacy system into the client service system. Certainly, the year 2000 has helped accelerate some of that activity, but that wasn't the initial driving impact in this instance.

Mr. MCINTOSH. The reason I asked is, I have heard anecdotally that there may actually be a benefit to the economy in the sense that many businesses have chosen to accelerate some of the efficiency gain—or technology transfers that could lead to efficiency gains, and yours seems to be a potential example of that.

Mr. EDWARDS. That is correct. We really looked to advance the business and move forward. With deregulation of the natural gas industry, the legacy systems don't support that, so we had to make that move initially. That is really a business issue.

Mr. MCINTOSH. OK. Those are the only questions I have, Mr. Chairman.

Mr. BURTON. Thank you, Mr. McIntosh.

Mr. Horn.

Mr. HORN. Thank you, Mr. Chairman.

Just along Mr. McIntosh's point, let me ask one semirelated to that last question, and that is the degree to which you found this exercise in trying to figure out the impact of the year 2000 on your particular systems, has that enabled you to really go through and think through the various mission critical systems that each of the firms have? And have you decided that it has nothing to do with the year 2000, that, Hey, we really don't need that system or we need a better system, et cetera? How often has that happened with you?

In other words, I am trying to look for the constructive aspects of not just repairing something on the year 2000 bit, but what has it done to improve—and this is Mr. McIntosh's question, too, I think—What has been done to improve your own business once you gave it some thought? You know the old line of "garbage in, garbage out." And sometimes these systems just grow up, and nobody takes a look at them and says, Do we really need to do this, or is there a better way to do it? Because all computers do is reflect what your own decisionmaking ought to be in any particular firm.

Do you want to start down the line, Mr. Beering? Have there been any situations where you have gotten rid of systems that have nothing to do with the year 2000?

Mr. MILLER. I will just speak for the water company, Mr. Beering and myself. Yes, as we start this process, our biggest, major investment to date is replacing our phone system, which is 1976 vintage. And it is driven—it will still function in the year 2000. We won't have the date stamp. But as of 1999, replacement parts are no longer being made. That forced us to look at something that was becoming obsolete instead of becoming obsolete and catching us after the fact.

Being acquired by NIPSCO Industries 2 years ago, just for efficiencies and consolidations, we have gone through a process of changing over all of our financial packages and accounting packages, and as I had mentioned, customer information services, just were more efficiencies, and going to the platform migrations.

Mr. HORN. Any thoughts on that?

Mr. EDWARDS. Just to add to my comment to Mr. McIntosh. We had found several obsolete packages that were being used that were being supported for no reason, and those, obviously, have been eliminated. But again, I would really like to drive home the point it is a business opportunity for us; by upgrading and moving our technology forward, we are certainly capable of being able to do more.

Mr. BURTON. Can you put the microphone in front of you? They can't hear you in the back.

Mr. HORN. Go ahead.

Mr. EDWARDS. As I said, it is really a business issue, as we advance the technology, to allow us to do a better job of doing the business of being in business. It really is an enhancement to our system and supports our overall efforts toward the natural gas industry and serving the residents of Marion County.

Mr. HORN. Mr. Gustin.

Mr. GUSTIN. Speaking for IPL, one of our biggest expenditures in the last 2 years has been the conversion of our financials from mainframe legacy systems to Oracle. I can say that decision wasn't made entirely as a result of Y2K, although we are getting some year 2000 benefits from that. But that move to enterprise resource planning has given us the opportunity to access information much easier than we could have with the legacy systems; it has given us the ability to analyze and convert that data, that information into knowledge.

As far as examining some of our business functions, we have a very comprehensive set of disaster recovery plans, as you might well expect for an electric utility. Part of the Y2K effort, though, has caused us to go back and review every one of those disaster recovery plans. We have made some modifications to those, and because of the year 2000, we have added things to those existing plans. So year 2000 has made us improve those types of disaster recovery issues.

Mr. BURTON. Mr. Mitchell.

Mr. MITCHELL. One of the learnings I think for Ameritech, and maybe for business in general, has been, we have probably got the most extensive comprehensive inventory of what is in our systems that we have ever had. That means some of the things, some of the embedded systems that have been built on top of each other over the years, no longer are really necessary. And as Mr. Edwards said,

we have eliminated those. And where we can, we—we do that very restfully.

We also look at upgrading things now in 1999 that we were going to do in the year 2000 or beyond. We have accelerated those to include that this century. Those are going to be representing tremendous cost savings for the company.

Mr. BURTON. Mr. Sloan.

Mr. SLOAN. Excuse me. Thank you.

There are two main advantages, or opportunities rather, that the Y2K problem presented us with. First, like the other firms present before you, we did have an opportunity to fully assess all of the different equipment and systems that we had, and we speeded up the retirement of some of those systems.

Because of the digital revolution, a lot of what is in the AT&T network is fairly new, installed in the last 10 or 15 years. So we do not have some of the problems maybe that some other folks have. But at the same time, we did have some carryover systems that we looked at, and it was a matter of, Do we make it Y2K compliant or do we just simply retire it? And so we opted for early retirement of those systems.

The second item, which is a little subtle, is that this Y2K problem gave us, as an industry, an opportunity to get together. And as you all know, if one part of the industry standardizes on one set of standards, and another wants a different set of standards; if we are not working together, having this engineer meet with that engineer; and having those type of relationships exist between policymakers a little bit higher up, then sometimes you have the Tower of Babel, where things just don't work together as well as they should, or perhaps at all. So I saw it as an excellent opportunity for us to meet on a regular basis and to sit down with a lot of our brethren in the telecommunications industry.

Mr. HORN. Mr. Chairman, I see my time is up. I hope we have a second round here, but I think you probably have some questions. Do you want to do it now?

Mr. BURTON. Why, thank you. I will ask a couple questions, and I will yield back to you, Mr. Chairman. I liked your biblical metaphor.

Let me start off by saying—by asking a question about the electrical system at Indianapolis Power and Light. When you sent out billings—and you and I talked about this last night, so this is more for public consumption because I think you answered my question—there was some concern among a lot of the people who received the billing and the information that there might be an outage or outages as a result of the Y2K problem. And last night at dinner, I think you elaborated on that to me and indicated that this would not be out of the norm.

So could you, for the benefit of anyone else who is paying attention, go into that in some detail?

Mr. GUSTIN. Yes, I would be glad to. I think there may have been some negative reaction by some of our customers regardng that first statement that was issued. What we intended to get across to our customer base, though, is that they should take a look at how they use electricity in their own lives, because there are many things other than year 2000 that could affect service and delivery—

tornadoes, ice storms, cars hitting light poles on the corner; those types of things can also stop the flow of electricity to customers. And we thought it was important that we just refresh that in our customers' minds, and take a look at how, in fact, they use electricity and how important it was to them.

We don't guarantee electric service. We don't guarantee uninterrupted flow of electric service, but I hope that as our customers see these presentations and learn and understand the types of efforts that we have put into Y2K remediation that we all benefit from the situation.

Mr. BURTON. I guess the point I wanted you to make, and I hope it is clear is that you don't anticipate anything that would cause outages any more than you would if there was an ice storm or a tornado or a car hitting an electric utility pole and knocking out the service.

So you don't think there are any unusual things that are going to happen because of the grid system or anything like that?

Mr. GUSTIN. Well, I don't know that I can foretell what things might happen with the grid. But as each day goes by, we see that more and more utilities are, as we are, I feel, having all of their units already operating in year 2000; having their main computer systems operating in the year 2000. The likelihood of problems goes down every single day.

Mr. BURTON. Well, let me ask it one more way, so we can be as clear as possible.

Is the likelihood of an outage because of the grid system, or something related to the Y2K program, is it any greater than we would have from an ice storm, for instance?

Mr. GUSTIN. Mr. Chairman, I don't know that I can really answer that question. I don't know.

Mr. BURTON. OK.

Ameritech, in your comments, you said that the suppliers were going to be responsible for informing individuals and companies about problems that might have—they might have with equipment outside of your control. Are you working with and contacting those suppliers to make sure that they are informing the customers that there might be a problem with their equipment?

Mr. MITCHELL. Absolutely. We have got a very comprehensive supplier management program in place.

Mr. BURTON. So are you working hand in glove with them to make sure that the customers are all informed that there might be a problem beyond your control that the supplier would have to deal with?

Mr. MITCHELL. Absolutely. We are telling the customers on one hand, but we are certainly advising the suppliers they have to take action, too.

Mr. BURTON. Are any of you affected by something that might happen in another part of the world? I know there are many of us in Congress that have heard that there might be an interruption of oil supplies because of the Middle East—because they are not computer Y2K compliant. Would that affect any of your industries or any of your services to the constituents we represent? You don't think it will have any impact?

Mr. GUSTIN. From the electric utility standpoint, we do have units that burn fuel oil for electric generation. Those units only amount to a small percentage of our total installed capacity. The remainder is coal-fired, so I don't see that that would have a long-term adverse effect.

Mr. BURTON. But are you storing reserves just in case of that eventuality?

Mr. GUSTIN. Prior to December 31st we will have an increase in the supply of coal that we would normally have, and we also will have much more fuel oil on hand than we normally have.

Mr. BURTON. So you will have contingency plans made in case there is an interruption of those energy sources?

Mr. GUSTIN. That is correct.

Mr. BURTON. I do want to ask you a question. You mentioned then—this is not of a local nature—but you mentioned that FAA and some of the health care industries at the Federal level were not compliant. A lot of us fly a lot and may be on a plane on January 1st. I would just like to know why the FAA is not compliant, and what can we do to get them compliant. Because I don't want to be up there when the communication goes out.

Mr. WILLEMSSEN. A couple of points on FAA. One, they have got a tremendously late start in addressing with Y2K. When we testified before Chairman Horn in February 1998 many of the basic management mechanisms that should have been in place were not in place. So they were way behind from the start.

They have made tremendous progress in the last 12 to 15 months under the new administrator, so they have done some great things. Unfortunately, their environment is so computer-intensive and so far flung across the Nation, that there still remains quite a bit that needs to be done, FAA has about 20 major en route centers and about 180 various terminal radar approach control facilities, so there is a lot to do yet. But they are going in the right direction. They have got a good plan in place with a little room to spare, but not much.

Mr. BURTON. Well, let me just followup by saying, are we going to have people at risk in January when these planes go into the air? Will they be compliant by that date, in your opinion?

Mr. WILLEMSSEN. I think, under the current scenario, it is likely that there may be some system failures. Fortunately, FAA has put a lot of effort into a business continuity and contingency plan, so that to the extent that there are some system failures, they will have backups in place. I am fairly confident of that.

I would not be confident in saying that there will be absolutely no problems.

Mr. BURTON. Are you going to be willing to fly on January 1st?

Mr. WILLEMSSEN. I would make that decision based upon data available later in the year, frankly.

Mr. BURTON. I would like you to keep me and the committees informed as much as possible about that.

Mr. HORN. Well, if I might, Mr. Chairman, we have had extensive hearings with the new administrator. She was blindsided by some of her staff, and I told her in my first hearing that, You ought to fire the whole bunch of them. She is an outstanding adminis-

trator, and she is doing a good job. They didn't even tell her what was going on for about 6 months.

So I think, as Mr. Willemssen says on behalf of the analysis of the General Accounting Office, that they are on the right track. I have said I would fly January 1st; that has not pleased my wife. But the administrator would do it. She is going to go Washington-New York. I am going Washington-Los Angeles, assuming we don't vote for 1 or 2 days. So I don't want to miss votes.

But the fact is, they are—they have got it on the right track, and I think we could be optimistic. The fact is that the administrator has complete power from the Congress to give an order to any plane on the ground when it comes to safety. So if they feel there was an overload on the system of radar and whatnot, that she can deal with that, and her people can deal with that delegated authority from her.

So nobody is going to be in an unsafe situation; let's put it that way. We have people running around loose—I even had one on my committee several years ago that said, Oh, planes are going to drop from the sky. Well, hopefully, they will be piloted and landing in a landing field.

It isn't planes dropping from the sky, but there are a lot of people who like to sell books, as I said earlier, or get radio programs, or ratings, or whatever, or TV programs; and I just think that that is nonsense. They are not going to take off. And we will know in time, as Mr. Willemssen says. He is right to wait a little longer in the year until we see what happens.

Mr. WILLEMSSEN. If I may add, Mr. Chairman, I have had several years of experience working with FAA systems. And within the systems environment, safety has always been the paramount issue, so that to the extent that FAA does have some systems-related problems come January 1, 2000, I would expect that not only would they put contingencies in plans, but they will not risk the safety of the flying public.

Mr. MCINTOSH. Would the gentleman yield for another followup in that area?

Mr. BURTON. Sure.

Mr. MCINTOSH. Mr. Willemssen, I read in the paper recently that they were testing a new computer system at FAA, and that they were not happy with the speed at which they were able to follow the planes. Is that on a separate track for the year 2000, or part of the same one that you were describing?

Mr. WILLEMSSEN. That is on a separate track. And because FAA cannot rely on that replacement system as their Y2K solution, they will have to remediate the existing systems as, again, a backup.

Now, to the extent that some of these new systems come in at the time, great. But we would concur with FAA, not to rely on the replacement system, especially with the problems it is having. It needs to go into the existing system, remediate that to make sure that it works through the change of the century.

Mr. BURTON. Mr. Horn.

Mr. HORN. Just to followup on a couple of questions. A number of you used the phrase, "contingency plan," and Mr. Burton in his questioning got out of one of you what one of those examples was.

When we surveyed the Federal agencies, they keep reporting to us "in progress." In other words, they don't have a contingency plan. Or some of them have the U.S. Postal Service as their contingency plan.

So then we called a hearing with the U.S. Postal Service, and they don't have a contingency plan. And everybody is depending on them to get momma's check out or Aunt Minnie's check or whatever, and instead of electric deposit, which is the sensible way to do things and avoid robbery, burglary, and all the rest that goes on with Federal checks.

But I would just like to go down the line, and if you could tell me, what is the contingency plan that you have. Let's just start in the order, with the water company.

Mr. Beering, what is the contingency plan?

Mr. BEERING. Congressman Horn, one of the real success stories from Indianapolis is that we have long been on the forefront of emergency planning. In my last position with the Indianapolis Department of Public Safety, I was largely responsible for a complete rewrite of the Indianapolis and Marion County Emergency Operations Plan. That plan, when it was retooled, embraced the local utilities and recognized the importance of having them participate in broader community emergency planning to the quick restoration of normalcy for both the customers and also for the citizens who rely on various city and other services. That planning effort has continued among the utilities that you have heard from this morning. We have——

Mr. HORN. Well, let me just ask this: Is there a grid for water as there is a grid for some aspects of power?

Mr. BEERING. There is not.

Mr. HORN. OK.

Mr. BEERING. We are able to purify and deliver water using engine-driven pumps far in excess of what the anticipated demand would be. And we are also able to help IPALCO in the event that there is a problem, because we can load shave for them. We represent one of their larger customers and are able to spin up our generating and fuel-driven machinery to take some of the burden for them.

Mr. HORN. Well, would you say it would be wise for somebody to at least have a couple of 5-gallon cans of water around?

Mr. BEERING. I think that our consensus recommendation has always been to encourage people to follow both Red Cross and FEMA guidance; and that is, that all citizens should always have 72 hours' worth of supplies available to them. And that would include battery-operated flashlights, battery-operated radio equipment, and enough supplies so that they can sustain themselves.

Mr. HORN. Well, as has been noted here, the sewage people, the waste disposal people, aren't really represented on this panel.

Does anybody know what they are going to do if you don't have any water and things can't be flushed?

Mr. BEERING. Actually we do. We have had extensive discussions with our colleagues from that particular operation, the White River Environmental Partnership. They have identified 15 out of their, I think, it is 350 lift stations, they have shared with IPALCO, those

that are deemed to be the most critical in terms of keeping sewage out of people's basements.

In addition, fortunately, much of the sewage system is a gravity-feed system that does not particularly require electricity. There are certain parts of the process that do require electricity, and they are developing some contingency plans to be able to operate all parts of the collection and treatment system, so that we are not going to have a problem with sewage.

Mr. HORN. Anything to add, Mr. Miller?

Mr. MILLER. Just that we do have a draft written of our contingency plan and have identified key people that can't take vacation.

Mr. HORN. Mr. Edwards, when it comes to the gas company, I am reminded that Russia supplies most of Eastern Europe and some of Central Europe with most of the natural gas. Now, this is all going to occur in the case of Europe, and would also in Indiana—you get some, not exactly sunshine every day in January, so that would be a problem.

And we are told that the refineries have a microprocessor-microchip problem. We are told that the pipelines in Europe have a microchip problem; we are told that the refineries in Europe have a microchip problem.

Do we have a similar problem in Indiana in terms of where your gas sources come from, how they get there so you can utilize them with your customers?

Mr. EDWARDS. The analogous grid of the natural gas industry, I will refer back to the overview slide of the gas process, which was in the presentation. We get—the primary supply of our gas comes from two major suppliers, and it comes basically out of the Louisiana Gulf area, as well as from the Oklahoma-Texas panhandle area.

The ultimate contingency for us would be a complete failure of that national grid for natural gas distribution. In that case, it reverts back to the way we managed our supply portfolio. Citizens is not unique in the natural gas industry, but we have company-controlled supplies, which on a ultimate failure scenario, would last us, without interruption of service, for at least a week. Certainly, those supplies can be extended.

And the other part of that contingency is to look at our interruptible customers and being able to extend that supply.

Mr. HORN. Is that sort of the national standard, to have at least a week of supplies in the natural gas field?

Mr. EDWARDS. I cannot comment on that, sir, as far as the national standard. It just so happens that the underground and above-ground storage that we have gives us enough supply, based on an average day's use in January, of about 7 days' worth of capacity.

Mr. HORN. How about the contingency plan, Mr. Gustin? Any further comments on that?

Mr. GUSTIN. We don't have a single contingency plan; we have numerous contingency plans for all of our various business functions.

I know there is a concern about the electric grid and what might happen to that. And I don't know that anyone has a real definitive answer. I can tell you that this grid is a very vast and very robust

piece of infrastructure. It has over 600,000 miles of transmission distribution lines, it has over 800,000 megawatts of capacity that is installed at various points about the grid; and it would take a very significant disruption to bring that grid down.

From our perspective, the worst case in any electric utility industry would be the loss of the grid. We have——

Mr. HORN. Well, of the various grids you showed us here, now, is there interchangeability among all of those grids so they could move from the West or the East and give you power if you didn't have them?

Mr. GUSTIN. There is good interconnectability east to west and north to south. There is limited interchange ability however between Texas and the other areas.

From our perspective, we have what is called "black start" capability at each one of our generating stations. And in the event that the grid goes down, and there is no electricity flowing, we have the ability to start all of our generating units up from a black start and connect our customer base independent of the grid.

Mr. HORN. And that would take how long?

Mr. GUSTIN. It is hard to tell.

Mr. HORN. A week, 2 days?

Mr. GUSTIN. Probably less than a week.

Mr. HORN. Less than a week. So presumably then we could work our way out of that.

Mr. GUSTIN. We would have the ability to work our way out.

Mr. BURTON. Would the gentleman yield?

Mr. HORN. Sure.

Mr. BURTON. If you had that kind of grid catastrophe and interruption, and you say it is up to a week to get those gas-fired generator, oil-fired generators to get started, you are talking about an outage of up to a week, you said?

Mr. GUSTIN. It is possible. I don't think anybody has a good handle on that.

Mr. BURTON. OK. Let's just say, advising the citizens of Indianapolis for any contingency, what would you advise them to do in the event that there was that kind of a problem with the grid system and the startup time was up to a week? Would you ask them to have generators or what?

Mr. GUSTIN. Well, that is a concern for us. I know that there are a lot of homeowners out there that are buying electric generators. We are concerned about that from a safety standpoint. If those generators are installed improperly, there is a risk of electric shock, explosion, to the homeowner. There is also a risk that our linemen will be exposed to stray currents because of those electric generators.

So I would certainly like to take this opportunity to let all of our customers who have those types of generators know that we have a problem with that. And, please, if you are going to hook those up, get a qualified electrician to do that for you.

Mr. BURTON. Of course. But I guess the question isn't really answered.

Your contingency plan is the black generator option, I guess that is what you call it?

Mr. GUSTIN. "Black start" capability.

Mr. BURTON. Black start capability would not be something of an immediate nature? You couldn't start it up—if there is an outage in Indianapolis, you couldn't start it up within a couple of hours?

Mr. GUSTIN. Probably not.

Mr. BURTON. How long would it take, did you say?

Mr. GUSTIN. That is hard to say, because when a unit is up to operating temperature and hot, and it trips off the line, those types of restarts can be done fairly quickly within a couple of hours. But if the unit is cold, it takes a much longer time to do that.

I think in that particular scenario, more of the problem would come with synchronizing all of the generating units and placing the system back into service, section by section. And I don't know honestly how long that might take. It would be—it would certainly be site specific.

Mr. MCINTOSH. Mr. Chairman, if you would yield for a second.

Mr. BURTON. Steve has the time.

Mr. MCINTOSH. Steve?

Mr. HORN. Yes.

Mr. MCINTOSH. Followup on a question on that: If the grid went down, just so I understand it correctly, and you had to go through this black start, what protection do you have that the electricity you generate doesn't flow outside of the—your area into the grid that has a problem?

Mr. GUSTIN. We are connected to the grid at 11 different points.

Mr. MCINTOSH. Do you disconnect those——

Mr. GUSTIN. Yes, if the grid is completly de-energized.

Mr. MCINTOSH [continuing]. And serve your own customers?

I see.

Mr. HORN. Do you have primarily hydro production of electricity, or are there nuclear reactors involved?

Mr. GUSTIN. No, we have no hydrogeneration, we have no nuclear generation. Our generation portfolio is approximately 95–96 percent coal-fired and the balance oil or natural gas.

Mr. HORN. Let's finish on the contingency plan.

Ameritech, what is our contingency plan?

Mr. MITCHELL. Well, we operate in the contingency mode quite a bit, as mentioned. The weather we have, summer, winter, things that go wrong, as people are digging, backhoes knock out cable and telephone lines, so we are already prepared to go into contingency mode at any time. So if we lose electricity in the summer, perhaps from a thunderstorm, we have backup batteries as well as backup diesel generators at our 1,400 central offices.

The other thing that we are focusing on, besides the various multiple contingencies, is also business continuity plans. So if for some reason you could not handle the day-to-day business of installing, repairing and maintaining telephone systems, how would we go about that if we had to bill people manually? If we had to get the repair records manually, we are going through that process now, so we will be prepared in that event.

Mr. HORN. Mr. Sloan, anything to add for AT&T?

Mr. SLOAN. Not very much. I think the Ameritech spokesman said it. Our industry is a model for redundancy and contingency planning.

And I would say this. Vacations have been canceled of all management employees a week before Y2K and a week afterwards, such that our customers would be able to get in touch. And regardless of whether there is power and water, we will deliver calls. Customers will be able to call us, as well as anybody else that they choose.

Mr. HORN. See, I remember Washington, DC, when President Kennedy was assassinated, everybody picked up the phone and called home. The switches just couldn't handle it. That is what often happens when people want to share or relate or make sure their relatives are OK. That overload really brings the whole system down.

Are you prepared for that?

Mr. SLOAN. Well, the networks are entirely different than they were in that timeframe. And I will give you a more recent issue we had in the State of Illinois, and it is referred to as the Hinsdale Crisis for those in the telecommunications business. It was a major catastrophe for the telephone business.

We had a problem in that all of a sudden everyone picked up the phone at the same time to try to call their loved ones, relatives, to see if they were OK.

What happens in a modern telephone network is that when that happens, our engineers that monitor the network, implement what are called "network controls" so we can slow down the flow and none of our systems are overloaded.

Customers may experience some delays. However, we will still deliver calls. Volume of calls will not bring the network down.

Mr. HORN. That is my last question, but I would like to have a subunit here of maybe some questions we would be able to send to various gentlemen.

Mr. BURTON. Yes. Would you be willing to respond in writing to us so we could have those in the record?

Mr. HORN. If we missed a few things.

Mr. BEERING. Absolutely.

Mr. BURTON. I want to thank you. It has been a very informative panel, and you are to be congratulated on doing a good job. But I don't know yet whether I will be flying on January 1st, and I am not sure I will buy a generator.

Mr. HORN. I should tell you, Mr. Chairman. I have told the Administrator of FAA she should not be arguing with controllers on January 1st.

Mr. BURTON. Thank you very much. I appreciate that.

Our next panel is going to be elected officials. We have the Honorable Dennis R. Redick, mayor of Noblesville; we have the Honorable Charles G. Henderson, the mayor of Greenwood; and we have the Honorable Carlton Curry, councilman from the city of Indianapolis, representing Indianapolis.

OK, if we can have everybody hold their voice down a little bit, we will go ahead and start. My colleagues will be back in a moment. Because of the time constraint, however, I think we ought to proceed, and then we will get to the question and answers.

This panel consists of the mayor of Noblesville, the mayor of Greenwood and Mr. Curry, who is a councilman and leader on the council in the city of Indianapolis, and what we wanted to do is

find out how they are preparing for the Y2K problem. I want to make sure everybody who wants to hear can hear.

So we will start with the mayor of Noblesville, Mr. Redick.

**STATEMENTS OF DENNIS R. REDICK, MAYOR, NOBLESVILLE, IN; CHARLES G. HENDERSON, MAYOR, GREENWOOD, IN; AND CARLTON CURRY, COUNCILMAN, INDIANAPOLIS, IN**

Mr. REDICK. Thank you, Chairman Burton.

Mr. BURTON. And could you make sure you pull those microphones as close as possible because some of the people in the back can't hear you.

Mr. REDICK. The following is a brief overview of the city of Noblesville's efforts to become Y2K-compliant. The city's Y2K project has several major goals. One is to maintain or increase our standards for public safety and communications. Second one is to keep the city systems as trouble-free as possible. And the third one is to be completed by the end of summer 1999.

Our project is divided into two parts, and these were started in late 1997. The first part is the systems are committed public safety, specifically the Dispatch Center. The second part is the general systems that are related to all other city projects. The reasons for the division is limited funds and having to prioritize the necessary changes from the most to the least critical.

In our system, the dispatch center and LAN are interconnected to allow for advanced resource management by our personnel. One of the perceived threats to public safety is the loss of power. We have, therefore, placed our dispatch computer and emergency operating centers on generator power filtered through an uninterruptible power supply. With our current fuel capacity, we can operate for 41 days without resupply. All of our portable radios are digital, and they have been reprogrammed to meet the necessary standards, and our in-car computers in the police cars are in the process of being tested for BIOS date and compatibility, and the appropriate operating system release.

After the upgrade of the dispatching system, we then upgraded the associated application software, And not all of these upgrades are complete. Several of other vendors and/or related agencies are not yet finished. We fear a flood of last-minute upgrades and requirements from other Federal and local agencies that we are connected to, thus making an emergency situation for us to respond to them.

We have experienced some difficulties with the upgrades. For instance, the computer-aided dispatch system is now time-sensitive, and the entire network has to be in a time lock step to prevent emergency alarms from sounding. This is creating the need to install a world clock into our system.

We have also been affected by incompatible programming where related systems that once worked now do not, and the program interfaces have to be rewritten to get back what we lost.

All of our network nodes have been tested and upgraded, and the systems that were not feasible to upgrade have been scheduled and funded for replacement. For our applications software, we must rely on the vendor's published statements, consultant's review, and their final testing.

After we feel that we are finished with all of the necessary upgrades, we will perform a systemwide test. This will occur in midsummer of 1999. We will change the date to just before midnight on December 31st and let the clock run through the end of year and on into the year 2000. We will then have each department test their applications and automated documents, and from this we will develop a list of any further modifications and prioritize them by their urgency.

Our current progress is excellent for those items that we have control over. Our hardware is basically finished, with the exception of some subsystems; software is coming along nicely, and we are actually ahead in some areas. Where we are behind is where we have to wait on outside agencies to make a decision or set a standard that is common to all, like public agencies. Some vendors and manufacturers have been slow to respond. Some have not had patches or fixes available until recently, which has caused unexpected delays or issues. Overall, the city of Noblesville is ready to handle any problems that may arise. Thank you, Mr. Chairman.

Mr. BURTON. We will have some questions for you.

[The prepared statement of Mr. Redick follows:]

## Public Safety Systems

- Power
  - Generator
  - UPS
- Radios
  - Reprogramming
- In Car Computers
  - BIOS
  - Software

## Public Safety Systems, cont.

- Software
  - Computer Aided Dispatch
    - CISCO
    - Upgrade OS to NT
- Computer Upgrades
  - BIOS
  - Memory

## Public Safety Systems, cont.

- Software Upgrades
  - Paging
  - Word Processing
  - Radio Controls
  - CDPD
  - E-mail
  - IDAX

## Public Safety Systems, cont.

- Emergency Operations Center
  - Weather Radar Computers
    - Satellite Link
  - Ham and CB Radio Systems
  - Tornado Sirens

7

## City Wide Systems

- Attacked Problem on Several Fronts
  - Network Nodes
  - Consultants are performing a review of:
    - Routers and Switches
    - Software
      - Network
      - Application
    - File Servers

8

## City Wide Systems, cont.

- Network Servers
  - Effects of upgrades
    - Network Timing
    - Incompatible programming

9

## Public Safety Systems, cont.

- Emergency Operations Center
  - Weather Radar Computers
    - Satellite Link
  - Ham and CB Radio Systems
  - Tornado Sirens

7

## City Wide Systems

- Attacked Problem on Several Fronts
  - Network Nodes
  - Consultants are performing a review of:
    - Routers and Switches
    - Software
      - Network
      - Application
    - File Servers

8

## City Wide Systems, cont.

- Network Servers
  - Effects of upgrades
    - Network Timing
    - Incompatible programming

9

## City Wide Systems, cont.

- Network Nodes
  - All bios tested last year
  - Network clients upgraded
  - Firmware upgraded
  - Replacements funded for failed systems

10

## City Wide Systems, cont.

- Software Review
  - Rely on vendors statements
  - Testing

11

## All Systems Test

- Will occur in mid to late summer
- Requires co operation of all departments

12

## Current Status

- High-level overview of progress against schedule
  - On-track in what areas
    - Hardware testing
  - Behind in what areas
    - Beyond our control
      - 911 systems
      - IDAX
    - Ahead in what areas
      - Software Review

## Current Status

- Unexpected delays or issues
  - Vendors tend to be slow to respond
  - Political system non responsive and reacting too late.

Mr. BURTON. Mr. Mayor. Mayor Henderson.

Mr. HENDERSON. Mr. Chairman, thank you for the opportunity to appear here, and I appear here wearing two hats; one as the mayor of the city of Greenwood, but mostly today as the President of the Indiana Association of Cities and Towns to inform what cities and towns across the State are doing and we as an association are doing.

As President of Indiana Association of Cities and Towns, I can report that we have been working with the National League of Cities and its technology arm, Public Technology, Inc. They have been offering up advice and tool kits for member cities and towns. IACT held its own technology conference December 9, 1998, in Indianapolis. I am confident as a result of this support, the cities and towns have been supplied with a wealth of information. A national update is available online at www.algov.org. That is National League of Cities' Access Local Government site. At my request, as president of the IACT, the IACT monthly magazine, Action Line, which I have here, the March issue is devoted to information-sharing from various Indiana cities and towns. Most towns feature action plans for the Y2K problem. I will touch on some of these in my remarks.

In Greenwood, in 1997, I asked the city council to fund appropriate moneys for a Technology Department, something we did not have at that time. That took place effective January 1998. The city hired a consultant to assist the Department of Technology with inventory of all city equipment which might possibly be effected by this problem. City officials will determine the proper means to correct any inefficiencies that might be found. Contingency plans were being developed for unexpected problems with city services and from outside agencies and utilities, such as electricity, water, natural gas and telephones.

Fishers, IN, a small community to our north of about 25- or 30,000 people, began planning early 1997. Manager information services and task force appointed; inventory of all town equipment that took—that could be affected. All items on the inventory list were looked at for upgrade or replacement cost. Vendors were contacted and all upgrades completed. Working with town vendors to determine their ability to provide uninterrupted supplies and services. City of Bloomington, IN. City of Bloomington's Information and Technology Department has been checking all information and technology systems in order of importance, with financial systems checked first; inventoried systems and all departments; created public awareness of the efforts by the city which lead to information-sharing.

Lafayette, IN. Inventoried software, hardware, office equipment, including fax machines, postage meters and diagnostic equipment for vehicles; analyzed which did not meet year 2000 compliance; repaired or replaced those items; ensured that critical business partners would also be Y2K-compliant.

Carmel, IN. Conducted inventory of all systems which it used and those expected to be used in the future. Project manager and steering committee acquired a list of at-risk items and ascertained the cost of upgrading to compliant systems. Committee identified the systems and components whose failure might bring hardship and inconvenience to citizens. This list was prioritized. Upon com-

pletion, research, gathering information, the city began the process of replacing and updating those items that were noncompliant; as of December 1998, began testing the Y2K-compliant system.

The cities and towns previously mentioned have all attacked the Y2K problem in basically the same manner. Each formed special committees, hired consultants, inventoried all systems that might be affected by Y2K, prioritized these and began replacement of deficient systems. Each has looked outside the city's offices and to the community, offering assistance and information-sharing to obtain compliance. Utility companies have had a top priority on the list. Cities and towns are attempting to keep services provided to its citizens unaffected by Y2K and inspire confidence in the community they serve.

Mr. Chairman, that completes my formal remarks.

Mr. BURTON. Thank you, Mayor Henderson.

[The prepared statement of Mr. Henderson follows:]

# MAYOR CHARLES E. HENDERSON
## City of Greenwood, Indiana
## President of Indiana Association of Cities and Towns

## Testimony - Y2K

As President of the Indiana Association of Cities and Towns (IACT), I can report that we have been working with the National League of Cities and its technology arm, Public Technology, Inc. that have been offering up advice and tool kits for member cities and towns. IACT held its own technology conference December 9, 1998 in Indianapolis. I am confident that as a result of this support, the cities and towns have been supplied with a wealth of information. A national update is available on-line at www.algov.org - NLC's Access Local Government site.

The IACT monthly publication, *Actionlines*, March issue is devoted to information sharing from various Indiana cities and towns. Most of the towns featured had similar action plans for the Y2K problem.

Greenwood, Indiana:

** Financial records in the City Clerk-Treasurer's office upgraded to specifications by mid 1998
** City hired a consultant to assist Department of Technology with inventory of all city equipment which might possibly be affected by this problem.
** City Officials will determine the proper means to correct any deficiencies that might be found.
** Contingency plans are being developed for unexpected problems with city services and from outside agencies and utilities such as electricity, water, natural gas and telephones

Fishers, Indiana:

** Began planning in early 1997
** Manager of Information Services and task force appointed.
** Inventory of all town equipment that could be affected
** All items on inventory list were looked at for upgrade or replacement cost.
** Vendors were contacted and all upgrades completed.
** Working with town vendors to determine their ability to provide uninterrupted supplies and services.

Bloomington, Indiana:

** City of Bloomington's Information and Technology Department has been checking all information and technology systems in order of importance, with financial systems checked first.
** Inventoried systems in all departments
** Created public awareness of efforts by the City which lead to information sharing.

Lafayette, Indiana:

** Inventoried software, hardware, office equipment including fax machines, postage meters, and diagnostic equipment for vehicles
** Analyzed which did not meet Year 2000 compliance
** Repaired or replaced those items.
** Insured that critical business partners would also be Y2K compliant

Carmel, Indiana:

** Conducted inventory of all systems in use and those expected to be used in the future.
** Project Manager and Steering Committee acquired a list of at-risk items and ascertained the cost of upgrading to compliant systems.

** The committee identified the systems and components whose failure might bring hardship and inconvenience to citizens. This list was prioritized.
** Upon completion, research, gathering information, the city began the process of replacing and updating those items that were non-compliant
** As of December 1998, began testing the Y2K compliant systems.

The Cities and Towns previously mentioned have all attacked the Y2K problem in basicially the same manner. Each formed special committees, hired consultants, inventoried all systems that might be affected by Y2K, prioritized needs, and began replacement of deficient systems. Each has looked outside of the City's offices and into the community offering assistance and information sharing to obtain compliance. Utility companys have had a top priority on the list. Cities and Towns are attempting to keep services provided to it's citizens unaffected by Y2K and inspire confidence from the communities they serve.

Mr. BURTON. Councilman Curry.

Mr. CURRY. Thank you, Mr. Chairman, Representative Horn, ladies and gentlemen. We have had a number of items occur since the last hearing here in Indianapolis, and I would like to extend my personal thanks to some of the things actually you started here that we have overlooked. For example, I would like to extend some appreciation to some of the things going through the Congress that would relate to tort support, so that committees and cities and counties and communities and government agencies who are doing a good will, good faith effort aren't subject too much to certain of our colleagues in the trial lawyer world.

Second, we were able to generate better communication and coordination with the Department of Correction in Indiana, with our county clerk, the justice system, and whatnot, such that certain remediation actions that are being done by all of these groups are now keyed to the same reference dates, where particular programs weren't being redone.

And last, from the area of Chairman Burton, you and Sheriff Cottey, I would like to personally thank you for the assistance you did on some capital funds for an automatic fingerprint identification system and a mug shot program, because I can tell you, we went from leading the pack in Indiana to well behind the pack, couldn't communicate with the State police or the FBI, but with the new system that is coming on line, which we just appropriated money for, we will solve the Y2K issue on that as well as let us be a fair partner.

With respect to works that are going on, I think there are still some areas that we can work with noncontractor discriminates. What I mean by that is, where we are buying services from contractors, it seems to me critically important that where we can, as the government is a procurer of the services, that we should be procuring to a common standard to the degree that is possible. And I would caution from experience when I used to do work in a certain part of the industry, that that standard that we would like help in is the what, not the how. For example, the coding for a fingerprint identification varies among about six or seven suppliers, and so the various programs actually don't talk to each other in terms of developing how that is sensed. And I just used that as a single for instance.

The status of Indianapolis is that, for a change, on some of the testimony you have heard, we are actually on schedule and under budget. We appropriated $12.9 million new dollars, which supplemented the dollars that were already in our budgets for the various city and county agencies, and the appropriation was in the face of $19-, rising to a $21 million estimate. But through our triage approach and specific assignments with a series of consultants which were selected in key areas, we brought that down to where it appears we will bring it under the $12.9. My personal goal was $10 million.

But in any event, we also had a hearing with the utilities in our committees for two reasons. One, we were concerned as to whether or not we would have electrical power, gas, long- and short-distance communication. We were particularly concerned with public safety. It turns out that we have the 800-megahertz system in that com-

bined communications with the sheriff, police and other law enforcement, fire and providers of medical support. And we are set up with 30 days of fuel supply with no added effort. This is our standard. I suspect we will probably have more than that.

Then from the city/county council standpoint, we are concerned about the attitudes of our citizens, the information that they have been getting. We have been using the local government channel, channel 16, to provide some advice for that. We have also keyed on the 72-hour type of reserve that a citizen or group of citizens should have. We have already done some work along this regard, and we plan in the August/September/October timeframe to do more intensive work in terms of communicating with the people of Marion County and the city of Indianapolis, where they stand with us, what they might expect, and how we might then approach.

And with that, Mr. Chairman, I will end, except for one item: I need your vote on May 4th.

Mr. BURTON. You have it. And I am hoping that in a year or so you will reciprocate.

Mr. HORN. And you are welcome to register in Long Beach, CA.

[The prepared statement of Mr. Curry follows:]

**THE COUNCIL**
**CITY OF INDIANAPOLIS**
**MARION COUNTY**

CARLTON CURRY
Councillor at Large

CITY OF INDIANAPOLIS & MARION COUNTY
YEAR 2000 PROJECT MANAGEMENT OFFICE

April 19, 1999

Subcommittee on Government Management, Information, and Technology
Congress of the United States
House of Representatives

***Update on Local Government Efforts toward Year 2000 Readiness***

Good Morning and welcome back to Indianapolis. On behalf of our community I wish to express my appreciation for the efforts you and your fellow Congressmen have made in addressing the litigation issues raised during your last visit. Since the disclosure immunity bill was passed in December of 1998, The City of Indianapolis - Marion County's Year 2000 Project Management Office has witnessed a tremendous increase in the substantial information received from vendors, utilities and neighboring communities related to their Year 2000 readiness. This has enabled our staff to prepare targeted contingency plans based on this information exchange. I am also encouraged by the tort immunity legislation that has passed through a number of state legislatures protecting state and local governments from frivolous Year 2000 related lawsuits. Your interest in not only assessing the Year 2000 readiness of units of government throughout the country as well as to act on their greatest concerns is much appreciated here in the heartland of America.

As mentioned during your last visit, the City of Indianapolis - Marion County established the Year 2000 initiative as a high-priority enterprise-wide project in the fourth quarter of 1997 to address the significant risks that the City County would face with respect to the Year 2000. This Year 2000 project encompasses over 100 County Agencies and City Departments. The primary objective is to identify and certify mission-critical systems and chip-embedded technology that may be date sensitive, and therefore be affected by the century date change. There are a number of municipal corporations, township organizations and non-profit organizations affiliated with the City/County that are outside of the scope of this Year 2000 project, however these agencies are actively under review by the City/County Year 2000 Council Committee regarding the progress of their remediation efforts. The general strategy employed by the Y2K project management team mirrors the approach utilized by many public and private organizations across multiple industries. A four phase process has been developed including: (1) Inventory, (2) Assessment & Planning, (3) Renovation, (4) Testing & Certification. At present the project is well into the *renovation* and concurrent *testing* Phases. All mission-critical systems marked with a certify disposition are being scheduled for certification testing in a Year 2000 simulated environment managed by the Year 2000 project team.

Overall, the City of Indianapolis - Marion County are moving steadily towards Year 2000 readiness. The following sections highlight the significant areas addressed in this project. As of March 31, 1999, $7.2 million of the nearly $13 million appropriated for Y2K readiness have been expended or encumbered. With approximately $5.4 million still available in the Y2K fund, the City of Indianapolis - Marion County is well-positioned to address any unforeseen issues that may arise this summer in a timely fashion.

4927 Windridge Drive • Indianapolis, IN 46226 • Phone: (317) 377-0238

**Applications Summary**

As the Year 2000 project enters its 18th month, 50% of the City/County's mission critical applications are in a testing phase. A few of the major systems undergoing significant system upgrades or system remediation include; the Clerk's Child Support System, the JUSTIS systems, IDACS/NCIC, and other Indianapolis Police Department/Marion County Sheriff Department (IPD/MCSD) applications. While 46% of mission-critical applications are still under remediation, they remain on schedule for certification by September 30, 1999.

Thirty-two percent of non-mission critical applications are still under assessment. Remediation of these applications will ensue as mission critical application projects are completed. With the triage approach the City/County has adopted, there will be non-mission critical applications that will not be Year 2000 ready at the turn of the century. While a delay or disruption in public services is not expected, staff may be inconvenienced. The principal information technology contractor, SCT, is aware of this and will place a high priority on addressing such problems at the start of the year.

In total, 8% of the City/County applications are certified compliant, 41% are undergoing testing, 28% are currently being remediated or upgraded, and 23% remain under assessment. Functional teams are being identified for all those applications undergoing system certification tests and contingency planning. In February and March the JUSTIS, KPMG, and Payroll/Personnel functional teams underwent extensive test plan development initiatives in preparation for certification testing.

Public Safety and Criminal Justice Applications

The JUSTIS system, under remediation by contractors Gottlieb & Wertz (GW), is on schedule according to the Marion County Justice Agency (MCJA). Having completed their initial programming efforts, GW awaits feedback from the testing team which consists of SCT and key members of the user community. The base year issues mentioned last fall have been fully remediated so that no issues related to integration with state or federal agencies are anticipated. The Fire Records Management System (RMS) is targeted for Y2K certification at the end of June with the CAD and Law Enforcement RMS scheduled for implementation in late September. Internal Projects for MCSD and IPD, such as Ximage and AFIS, are on schedule.

It is important to note that the interface for data transfer with both State of Indiana law enforcement agencies and national agencies, especially the FBI and NCIC. As an aside to the Y2K issues, standard national algorithms would be a great help in identification procedures.

Public Works Applications

IMS will undergo certification in early summer following the completion of their current system upgrade. The Tidemark Permits application has completed its system upgrade and is preparing for certification testing.

Finance and Property Applications

The Property system is nearly certified Y2K compliant with a few modules still undergoing rigorous Y2K testing. The KPMG suite is currently undergoing Y2K certification testing. Testing will conclude by mid-April. The Auditor and Treasurer's office have numerous applications that are being converted to Access-based, Y2K-compliant applications.

Other Public Services

In addition to the upgrade of the Clerk's Child Support system, the integrated voice response application associated with this system will be upgraded to a Y2K compliant package quarter.. This project and all other mission critical applications are on track for the September 30th deadline. The Department of Capital Asset Management (DCAM's) Capital Improvement Plan (CIP) database and Parks Registration (CLASS) system are preparing for certification testing. These systems are used to plan and monitor construction projects.

## Information Technology Infrastructure Update

The mainframe LPAR is busy with Y2K certification testing activity. In April, an NT server will be ready for Y2K testing of client-server applications. SCT is completing testing of all the connectivity devices in the enterprise. Server consolidation and certification is also well underway. Utilizing 1999 budget dollars, City Departments and many County Agencies are replacing older PC equipment and upgrading PC software. To augment County agencies limited technology budget dollars, the County Auditor included $400,000 in the Y2K fund targeted for PC replacement. The Y2K PMO is working with County agencies with the oldest PC inventories to complete replacement projects by September 30, 1999.

## Chip-embedded Assets Update

At this time there are few Y2K issues which will adversely affect mission-critical chip-embedded assets. The existing analysis shows that 22% of our assets are non-compliant with 87% of these assets being home detention units utilized by the County's Community Corrections Agency. These assets are being upgraded to Year 2000 compliant units. The remaining assets are primarily office automation products such as fax machines. While these assets are deemed non-compliant based on the City/County's compliance definition, they are not viewed as critical because the problem results in a cosmetic versus functional problem. The remaining assets, which were determined to be non-compliant, do not pose a significant problem because the functionality that is not compliant is not currently utilized by the City/County. In September 1998, Raytheon assisted the Year 2000 project management office in an in-depth review of the City/County's chip-embedded assets. Security and Fire Alarm systems, HVAC control systems, Traffic light controls, telephone systems, environmental monitoring systems, and other public safety assets were included in this review. As a result of this analysis, the number of assets that need to be addressed further has been narrowed significantly. At present, there are a few types of HVAC control and traffic control systems that are especially susceptible to Year 2000 problems. We are concentrating efforts such as test coordination, replacement strategy and contingency planning in these two areas primarily.

## Contingency Planning Update

According to a recent Gartner Group Study, 90% of Y2K-related failures will be resolved within the first 72 hours of occurrence. For that reason, the Y2K Project Management Office and the Marion County Emergency Management Agency have prepared an internal approach to contingency planning which focuses on the impact of the first 72 hours of a potential Y2K-related failure. Our approach mirrors what other communities are implementing to meet this need. The internal approach focuses on contingency planning for individual systems, chip-embedded assets, and suppliers. More importantly, public safety and service organizations will participate in regular meetings to build organizational management plans that would be implemented in the event of a Y2K (or other emergency-related) disaster. Numerous scenarios will be examined and addressed in these plans.

**Supply Chain Update**

In mid-February, the County identified 433 vendors as mission-critical requiring a Year 2000 survey response. Therefore, in addition to the 1825 sent to City vendors, the PMO has identified 2258 business relationships that should have a Y2K disclosure form on file in our office. Of these vendors, a smaller subset are deemed mission-critical by purchasing and departmental representatives. These business relationships will require a more in depth review of their Y2K readiness.

There is an important final note. Recent public hearings involving local utilities have been conducted. Electric, gas, water and telephone service providers have shared overviews of their Y2K compliance plans. This public coordination enabled local government to advise the local populace concerning progress toward resolving potential issues. Plans are underway to help define suggested procedures that the public may take to offset a Y2K related service failure. Indianapolis plans to use its government access channel and the local commercial media to further educate the public as verification testing is accomplished. It is believed that this public service will be a great aid to overcome troubles that may occur.

Carlton Curry

Carlton Curry, Chairman

Year 2000 Ad Hoc Committee

Mr. BURTON. Mayor Redick, you said that you had generators for emergency purposes to make sure that the communications go on with fire and police, and you went to a digital—new digital phone system so you could stay in touch. I just wanted to ask all three of you, in the event that we did have a grid problem, or an electricity problem, or a shutdown in any of the utilities we are talking about, do you have a backup plan in Indianapolis and in Greenwood, as well as Noblesville, to make sure that communications take place and that you have an energy source to be able to make sure that you can send them that information?

We will start with you.

Mr. REDICK. Yes. Our UPS, the uninterruptible power source, we have in place and have always had in place.

Mr. BURTON. That is not only fire, fire, police and ambulance service?

Mr. REDICK. Correct. And we can operate that for a total of 41 days without refueling.

Mr. BURTON. How about in Greenwood?

Mr. HENDERSON. Yeah, we are making sure we have an ample supply of gasoline, because that is what runs the generators. We have major generators in place to run our communication system. We have 11 lift stations that lift our sanitary sewer to our gravity lines. We have generators and standby for those lift station, which don't run continuously, as you know, and petroleum for that. We have also put into place a no-days-off policy for public safety people to have those folks on standby with their vehicles.

Mr. BURTON. What about the length of time that your gasoline and fuel supplies to run those things—how long a period do you have those for?

Mr. HENDERSON. Well, normally our gasoline supply is usually a month, but on this we think that if everything goes down, it will—we are thinking it will last 2 weeks.

Mr. BURTON. I see. So you do have a supply to keep things running?

Mr. HENDERSON. For 2 weeks. We are hoping that nothing will be more drastic than that. We have to start using it for all the generators and things. It will reduce us to about a 2-week supply.

Mr. CURRY. We have concern over the supply of fuel for vehicles, but as far as the communications, our 800-megahertz system is not only a redundant; that is to say, we have a second facility, which we can under reduced protocol handle all of our public safety requirements for communication in Marion County. It is an uninterruptible supply that immediately goes to battery, while the generators come up and the generators carry on. And we, as our standard course of business, have always 30 days of fuel underground at the site. So, from the communications standpoint, I, frankly, have few worries.

Mr. BURTON. So, if some kind of a breakdown or emergency occurs, how long could you keep everybody in communication with one another and keep things moving?

Mr. CURRY. Communication, we're good for at least a month, and that is with doing nothing else but what we are already doing. With respect to guaranteeing fuel in every police car, ambulance,

and fire apparatus, that is something that we are still wrestling with a number.

Mr. BURTON. So, you don't have a date. You don't have a timeframe.

Mr. CURRY. Today I do not.

Mr. BURTON. But you are working on that.

Mr. CURRY. That is correct.

Mr. BURTON. Do you know what the goal is? Is the goal to have a week's supply?

Mr. CURRY. My goal, my personal goal, would be that a week isn't enough. My personal goal would be 2 weeks.

Mr. BURTON. Two weeks?

Mr. CURRY. And that flies in the face of some other things. And we have some meetings that are scheduled, Mr. Chairman, with respect to our local emergency management people to help work these things out. As a matter of fact, there is a meeting this morning at 11 o'clock that is working on this thing. But as we approach this incrementally, we are making a strong effort to tell the citizens that a 72-hour supply is what an individual should have in their domicile. From a government standpoint, certain critical services, it seems to me, are going to require more than 72 hours, because the fact of the matter is if there should be a widespread Y2K occurrence, if 50 communities are affected around the country, the State and local folk can handle that, but if 500 communities are affected in each State, there aren't enough resources to handle that. So we are going to have to look to home to make sure that we do our best and help our neighbors if we can.

Mr. BURTON. Mr. Horn.

Mr. HORN. All three of you have very well-prepared statements, and I thoroughly enjoyed reading them on the plane, as well as here. I would just like to ask Mayor Henderson, since you are president of the Indiana Association of Cities and Towns, have you looked at the Lubbock, TX, experiment, and Montgomery County, MD, experiment where they worked on a basic emergency function? They said, we are going to pretend that January 1 has come, and they stayed up all night and just watched what actually happened. Because those are two diverse cities that I think we could learn a lot from, and I wondered if that information was shared by the National League of Cities with the various State affiliates.

Mr. HENDERSON. Yes, sir, it was—like I said, in our March issue, we dealt with what was going on in the State. In our latest issue that just came out last week, we referenced the Lubbock, TX, issue and told our membership that that is something that they needed to look at and gave them information on the computer Web site where they could get that.

So, yes, we as a staff at IACT have looked and that and have moved that information on.

Mr. HORN. Good.

I think, Mr. Chairman, before the panel breaks up, I would like to have Mr. Willemssen come back, because he might well have some national perspective on some of this that I don't have.

Mr. WILLEMSSEN. Well, based on what I have heard, it is clear that the entities as represented here are aggressively pursing the Y2K issue. I think you have hit on the right issues. I think that

the fact that they emphasized a contingency planning element should be noted, and should be for the citizens that they represent. They should feel pretty good about that, that even in the event that there are system failures, that there are backup plans in place.

Other than that, I think what the chairman said again needs to be reemphasized; that many of these communities faced the Y2K issues. I think to the extent that we can hear further replication of the kind of efforts that the local officials here have talked about, the better off we will all be.

Mr. BURTON. Can I ask just one question? You said that 72 hours of supplies ought to be on hand. Is there any way that you are disseminating that kind of information out to the people in the center part of the State or Indiana as a whole? And are they making a list of the kind of supplies that people ought to have on hand as protection?

Mr. CURRY. Yes and yes. What we are doing, Mr. Chairman, is we are identifying a recommended list of things that should be done and should be purchased, obtained or somehow held together. And then that particular list will be a part of this August/September/October heavier push, which I talked about earlier in my remarks.

Now, we aren't just going to wait for that, however, because we have had a number of programs, again, using the local government channel, channel 16, and also local media releases, but I think that our biggest push will be in the fall as we have completed some of the testing we have, because we can also add with that then the status of success at that point.

Most of our systems that are undergoing remediation and testing and verification that are critical systems will have been tested well before the end of September. And so, if we start with the August, September, and October timeframe, we can add confidence of actual test results instead of telling people how great it is going to be. We can say, here is what we have done. Here is what we recommend you might consider. And we will do this in a broader basis, but we will be somewhat reliant on the media to help carry these things. From the government TV channel, I am sure we can influence that locally.

Mr. HORN. That is all I have, Mr. Chairman.

Mr. BURTON. Well, I don't have any more questions. I think you are to be congratulated on moving in the right direction rapidly, and if we can be of any help to you in Washington, if you need anything, of course, give us a call. We will be glad to help you any way we can. Thank you very much.

Mr. CURRY. 256 more days.

Mr. BURTON. The next panel we have is the Honorable Jack Cottey, the sheriff of Marion County; the Deputy Fire Chief John Spahr, the Lawrence Township Fire Department; our good friend and media great, Mr. Greg Garrison; and Miss Kate Ekins, manager of public affairs of St. Vincent Hospital and Health Services. OK, welcome.

One of the most important areas that we are going to be looking at, of course, is the emergency problems that we might encounter, and law enforcement, and fire and emergency services, ambulance

services are important, as well as the hospitals, to see how they are all going to be handling this.

So let's start off with Sheriff Cottey, our good friend.

**STATEMENTS OF JACK L. COTTEY, SHERIFF, MARION COUNTY, IN; JOHN SPAHR, DEPUTY FIRE CHIEF, LAWRENCE TOWNSHIP FIRE DEPARTMENT; J. GREGORY GARRISON, CBS LEGAL ANALYST; AND KATE EKINS, MANAGER OF PUBLIC AFFAIRS, ST. VINCENT HOSPITAL AND HEALTH SERVICES**

Mr. COTTEY. Thank you, Mr. Chairman. It is a pleasure to be here, and I am going to echo with Councilman Curry's statement, that $1.5 million meant a lot to this community. Thank you for the assistance.

I would like to make a few brief remarks. First of all, I am glad that Councilman Curry did precede me. As you can tell, he was given this awesome responsibility about 2 years ago to be more or less in charge of the city and county government to make sure that Y2K—that we were in compliance, and I think he did an excellent job. I commend him for that.

Mr. Chairman, members of the committee, from a local law enforcement standpoint, Y2K translates into a short, basic list of the seemingly simple but critical questions for policymakers and those who are sworn to serve and protect. No. 1, when someone dials 911, will the call go through? No. 2, will the dispatchers be able to answer that 911 call? No. 3, will they, the dispatchers, be able to gather keystrokes and relay vital information on to the emergency patrol officers, sheriff deputies, EMTs and firefighters? No. 4, will those in the field receive that information by a radio and car computer which are MDTs and pager in order to respond? No. 5, will it be able to forward or query information from the scene? Will they be able to call for backup, signal that they are in need of help or, worse yet, that an officer is down? No. 6, when an arrest is made, will inmate processing with digital mug shots and automated fingerprint systems work? No. 7, will inmate medical reports, jail records and court records be available and accurate throughout all jurisdictions? No. 8, will it be able to interface with other local, State and national criminal justice agencies and data bases? What about record checks, outstanding warrants, protective orders, extradition information and so forth?

If I say these may seem like simple questions, especially when compared to scholarly, intricate detail you have heard at this and other hearings, but I respect your appreciation for the critical nature, and I applaud your interests in seeing they are answered before the bell tolls and before the calendar changes, because at midnight on December 31st there will be these eight basic questions which will likely be answered not only first, but instantaneously, not only here, but in every hometown across America. Then moments later I predict attention will shift from Times Square to air travel, to banking, to utility delivering, to virtually everything else dependent upon computers.

When I say this, I by no means take away from the significance of the FAA, the Department of Treasury, NASA, the Veterans Administration or Housing and Urban Development, all of which play vital roles in the lives of millions. But I do mean to say that com-

puter failures on the local, State, and national level involving public safety will be felt swiftly and severely, and that, God forbid, the absence of law and order on our streets would be felt first.

Now, the challenge is for me and every police executive across America to ensure that we can honestly answer yes to each of those eight basic questions, to see to it that those public safety computer failures do not occur, and that there is no absence of law and order on our streets. The good news is, from what I gather, from the National Sheriffs Association, International Association of Chiefs of Police, most of us law enforcement executives are trudging toward some early to midsummer test dates on our 911 systems to include telephone, radio, and computer-aided dispatching. And here locally we are presently on schedule for compliance at the Marion County lock-up and jail for inmate process, jail records, medical records, automated fingerprints, and digitized mug shots.

At the same time external concerns force us to be at the mercy of other public and private agencies: NCIC, the National Crime Information Center, a national data base of felonies and extradition information; No. 2, IDACS, Indiana Data and Communications System, a data base for local warrants and stolen property; also Bureau of Motor Vehicle driver's license and vehicle plate information; No. 3, JUSTIS, our local booking and courts records; and finally, utilities, a normal household's list like water, electricity, natural gas and so forth, which you have already addressed this morning.

These external conditions are being closely monitored by a committee of my top administrators. This same group headed by Colonel Jerry Cooper, Colonel Scott Minier, and Deputy Chief Larry Logsdon is also tasked to coordinate with our year 2000 Project Management Office for the city of Indianapolis, which, with the help of outside vendors and Y2K consulting engineers, has for many months been identifying and reviewing year 2000 concerns in preparation for this summer's verification and testing.

"No man is an island" will perhaps never ring truer in our lifetimes than at the stroke of midnight on New Year's Eve this year. As independent as we like to believe we are, as independent as our public and private agencies and all levels of government like to think we may be, the truth is we are all in this together. And that is why this sheriff and just 1 of the Nation's more than 17,000 local law enforcement agencies thank you for your time and your concern about how Y2K will impact local law enforcement and public safety. Thank you, Mr. Chairman.

Mr. BURTON. Thank you, Mr. Sheriff.

[The prepared statement of Mr. Cottey follows:]

**Remarks of Marion County Sheriff Jack L. Cottey**
**Before the Government Reform Committee**
**Monday, April 19, 1999**
**Indiana University - Purdue University at Indianapolis**

Mr. Chairman, Members of the Committee, gathered guests:

From a local law enforcement standpoint, Y2K translates into a short, basic list of seemingly simple, but critical questions for policy makers and those we are sworn to serve and protect:

1. When someone dials 9-1-1, will the call go through?
2. Will dispatchers be able to answer that 9-1-1 call?
3. Will they (dispatchers) be able to gather, keystroke and relay vital information on the emergency to patrol officers, sheriff's deputies, EMTs and fire fighters?
4. Will those in the field receive that information by radio, in-car computer (MDTs) and pager in order to respond?
5. Will they be able to forward or query information from the scene? Will they be able to call for back-up? Signal they are in need of help? Or worse yet, that an officer is down?
6. When an arrest is made, will inmate processing with digital mug shots and automated fingerprint systems work?
7. Will inmate medical records, jail records and court records be available and accurate throughout adjudication?
8. Will we be able to interface with other local, state and national criminal justice agencies and databases? What of records checks, outstanding warrants, protective orders, extradition information, etc.?

As I say, these may seem like simple questions ... especially, when compared to the scholarly, intricate detail you've heard at this and other hearings ... but I respect your appreciation for their critical nature and I applaud your interest in seeing they are answered before the bell tolls, before the calendar changes.

Because at midnight on Dec. 31st, it will be these 8 basic questions which will likely be answered not only first, but instantaneously ... not only here, but in every hometown across America.

Then, moments later, I predict attention will shift from Times Square to air travel, to banking, to utility delivery and to virtually everything else dependent upon computers.

When I say this, I by no means take away from the significance of the FAA, the Department of the Treasury, NASA, the Veterans Administration or Housing and Urban Development – all of which play vital roles in the lives of millions. But I do mean to say that computer failures on the local, state and national level involving public safety will be felt swiftly and severely ... and that, God forbid, the absence of law and order on our streets would be felt first.

Now, the challenge is for me … and every police executive across America … to insure that we can honestly answer "yes" to each of those eight basic questions ... to see to it that those public safety computer failures do not occur … and that there is no absence of law and order on our streets.

The good new is -- from what I gather from the National Sheriffs' Association and International Association of Chiefs of Police -- most of us law enforcement executives are tirelessly trudging toward some early- to mid-summer test dates on our 9-1-1 systems to include telephone, radio and computer-aided dispatching.

Here locally, we are presently on-schedule for compliance at the Marion County Lock-Up and Jail for inmate processing, jail records, medical records, automated fingerprints and digitized mug shots.

External concerns force us to be at the mercy of other public and private agencies:

- NCIC (National Crime Information Center – a national database for felonies and extradition information);
- IDACS (Indiana Data and Communication System – a database for.local warrants and stolen property, also Bureau of Motor Vehicles' drivers license and vehicle plate information);
- JUSTIS (local booking and court records); and
- Utilities (a normal household's list) like water, electricity, natural gas, etc.

These external concerns are being closely monitored by a committee of my top administrators. This same group – headed by Col. Jerry T. Cooper, Col. S. Scott Minier and Deputy Chief Larry J. Logsdon – is also tasked to coordinate with our Year 2000 Project Management Office for the City of Indianapolis, which with the help of outside vendors and Y2K consulting engineers has for months been identifying and reviewing Year 2000 concerns in preparation for this summer's verification and testing.

"No man is an island" will perhaps never ring truer in our lifetimes than at the stroke of midnight on New Year's Eve this year. As independent as we like to believe we are, as independent as our public and private agencies and levels of government like to think we may be, the truth is we are all in this together.

And that is why this sheriff, from just one of our nation's more than 17,000 local law enforcement agencies, thanks you for your time and your concern about how Y2K will impact local law enforcement and public safety, Mr. Chairman.

Mr. BURTON. Mr. Spahr.

Mr. SPAHR. Mr. Chairman, Congressman Horn, it goes without saying that probably the most critical concerns of any person is their own personal health and safety and the safety and health of their loved ones, and to that end, the fire service is dedicated to the extent of even giving our own lives to that protection of the public.

It goes without saying also, therefore, that we would be violating our sworn oath to protect the public if we ignore the Y2K compliance issue. Indeed, computers also play a very large part in the operations of my fire department, the Lawrence Township Fire Department, 1 of about 12 or 13 in Marion County, but also one that is very typical.

The department uses computers for record storage, reports, correspondence, budget considerations, computations, and summaries, emergency statistics reports, records management and a number of other uses. It was, therefore, alarming to be informed of the problem that we would face on January 1, 2000, when many if not all, of our computers would become inoperable.

The department has since—my department has, since 1991, used Apple McIntosh computers, comprised of 12 desktops in our offices; more desktops in remote fire stations and several printers. The office and station computers are networked to permit in-house communication, as well as the transmission of run report information from the stations to headquarters, and these computers range in age anywhere from 1991 to 1998.

Now, that system has been adequate and has served us well over the years, although it is beginning to require more and more maintenance and repair as time goes on. New technology, new program availability, coupled with the Y2K problem has, therefore, required us to consider replacing the system with PCs, and this may be the silver lining in the Y2K cloud, as Congressman McIntosh mentioned earlier. This has provided us with the impetus to explore and investigate new technology and, therefore, increase our capacity to serve.

We have selected a company to replace that system. We did take three bids, and currently the current bid is approximately $77,000. Obviously, this is not an inexpensive thing, but is certainly a necessary one.

Since submitting my initial report, I have received more information on compliance within Marion County within the fire departments, and I would ask that that addendum be included in my original report. The survey of the 12 or 13 departments in Marion County indicate that they are all pursuing to some degree steps toward the compliance. This can—this ranges in anything from modifications to their current systems to a total revamping of their systems.

Now, my department itself will complete the installation of our new system sometime next month. We will be totally networked as we were before. Following that, we will then begin to survey the vendors that we have used in the past and the vendors that we have used at this time to gain written confirmation of their products and compliance. Obviously, if they come back saying it is not compliant, then needless to say, we will take appropriate action at

that time. That project should be completed by August 1st, leaving us approximately 4 months to handle any further problems that come up.

Now, as I have stated, the fire departments in Marion County are aggressively pursuing this problem, ranging anywhere from no budgeted funds, that being funding simply coming out of operating up to 305,000, which is the highest funding that I have heard, but I think I can speak for them in confidence that with the efforts being put forth by these departments, we feel that if the citizen calls 911 on January 1, 2000, a dispatcher is going to answer the phone, and they are going to send the appropriate law enforcement, fire or emergency medical equipment. And that is a service that our citizens have come to expect, and they deserve it, and it is also the service that we swore to provide.

In closing, though, I would like to express my appreciation to the committee for this opportunity to come before you, and I would like to commend each of you for the time and effort you have put on this issue. I think it is rewarding for the public to see that, indeed, the Congress is concerned about the well-being, and willing to go to these steps to show it. Thank you.

Mr. BURTON. Thank you.

[The prepared statement of Mr. Spahr follows:]

Lawrence Township
FIRE DEPARTMENT

Administrative Office
6260 E. 86th Street
Indianapolis, IN 46250
(317) 845-4933

**Y2K Compatibility at the**
**Lawrence Township Fire Department**
**Indianapolis Indiana**

Like every other emergency service, the fire service has become dependent on computers. The dispatching of fire and medical emergency responses is, with a few exceptions, done by the Indianapolis Fire Department Dispatch Service using equipment owned and maintained by the Metropolitan Emergency Communications Agency (MECA). MECA officials have been involved in a substantial testing program of the equipment to determine Y2K compliance and have been assured by the manufacturer, Motorola, that all dispatching capabilities are, indeed, compliant and that there is no cause for concern. The final two areas of testing are scheduled for completion in July, 1999.

Computers also play a very large role in the operations and administration of the Lawrence Township Fire Department. The department uses computers for records storage, reports, correspondence, budgetary computations and summaries, emergency statistic reports, records management and a number of other uses. It was, therefore, alarming to be informed of the problem that we would face on January 1, 2000, when most of, if not all, of our computers would become inoperable.

The Lawrence Township Fire Department is a combination career/volunteer fire department responsible for fire and emergency medical protection in northeast Indianapolis, Indiana. Its district covers approximately thirty-five square miles with a nighttime population of about 50,000 and a daytime population of approximately 95,000. It operates out of four fire stations with a staffing of 106 firefighters and five civilians. The fire department administration is housed in an adjoining building to one of the fire stations.

The department has, since 1991, used a Apple Macintosh system comprised of twelve desktops in the headquarters offices, four desktops in the remote fire stations, and several printers. The office and station computers are networked to permit in-house communication as well as the transmission of run report information from the stations to headquarters. The computers range in age from those purchased in 1991 to those obtained in 1998.

The Macintosh system has been adequate and has served us well over the years, although it is beginning to require more maintenance and repair as time goes on. New technology and program availability, coupled with the Y2K problem has, therefore, required us to consider replacing the system with IBM compatibles.

A local company, Data Systems Inc., has introduced software (Fire Tech) designed for the fire service and customized to fit our needs. Thus, it is felt that to successfully handle the Y2K problem and to enable us to utilize the new technology available, it is most prudent and cost effective for us to replace the entire system with one which is IBM compatible. This system will be completed in May, 1999. A list of the components of the new system is included in this report.

Obviously, this will not be an inexpensive change for the department. We have obtained three bids for the project. The one which has been selected will include the hardware, software, training, installation, configuration and one year support of hardware and software for a cost of $76,651. When completed, the system will enable us to accomplish the same transferring of information from remote stations and the same processing of information as we did before but at a much higher speed and in a more dependable fashion. Most importantly, however, the new system will not be affected by the Y2K problem and will permit us to continue operation after December 31, 2000.

**Lawrence Township Fire Department**
**Indianapolis, Indiana**
**Computer System Components**

| | | |
|---|---|---|
| 1 | NEC Pentium II 450 MMX MHz. 256 MB SDRAM, (2) 6.4 GB UDMA Hard Drive, 512K Cache Memory, 4 MB ATI AGP Graphics, 32X CD-ROM & 3COM 10/100 Network Grid. This system will serve as the Network Host for Headquarters. | $ 3440.00 |
| 1 | NEC Pentium II 350 MHz. 128 MB SDRAM, 6.4 GB UDMA Hard Drive, 512K Cache Memory, 4 MB ATI AGP Graphics, 32X CD-ROM & 3COM 10/100 Network Grid. This system will serve as the Remote Access Server for all the Remote Workstations to dial into. | 2450.00 |
| 1 | Tripp Lite Battery backup BC PRO 600 | 225.00 |
| 1 | Windows NT Ver. 4.0 (25) User License | 1850.00 |
| 1 | T5000 Tape Backup & 5 Tapes | 575.00 |
| 1 | NT Server and Exchange Backup Software | 1050.00 |
| 1 | Microsoft NT Terminal Server (5 User). This software is utilized on the Remote Server. | 1225.00 |
| 1 | Citrix Mediframe Remote Software (15) User. This is utilized on the Remote Server. | 4500.00 |
| 1 | 8 Port Equinox Board with Octopus Cable. Utilized for the Remote Station Connection. | 1190.00 |
| 8 | U.S. Robotics 56K Extrernal Modems & Cables. These will be utilized at the Host & 4 Remote Locations. | 1248.00 |
| 1 | Microsoft Exchange Server Mail (125 User) License | 7500.00 |
| 18 | NEC Pentium 350 Mid Tower Computer - includes: 64 MB RAM, 6.4 GB Hard Drive, 32X CD-ROM, 15" monitor & Network card in 16 of the units. These will be utilized at Headquarters and the 4 Remote Stations. | 39600.00 |

| | | |
|---|---|---|
| 1 | Complete FireTech 32 bit Windows program. This is a discounted price based on Data Syatems Inc. installing the hardware. Otherwise it would be priced on the regular price sheet at approximately $16-18,000 depending on modules selected. | 3000.00 |
| | Installation and Configuration as outlined | 10500.00 |
| **Total cost for installation:** | | **$76561.00** |

Since submitting my initial report, I have received more information on the Y2K compliance programs being instituted by the various fire departments in Marion County. I ask that this addendum be attached to my original report.

The fire departments in Marion Count, Indiana are all pursuing compliance with Y2K in varying degrees. Several of the departments have created committees whose purpose is to investigate that department's compliance and recommend corrective action if necessary. Several others have made the necessary modifications to their systems to meet the requirements. Some of the departments have confirmed that their systems are, indeed, compliant. Others, like Lawrence Township, have replaced their systems entirely.

The Lawrence Township Fire Department will complete the installation of the new computer system within four to six weeks. Once that has been done, we will then survey the vendors that we use or have used in the past to gain their assurance that their products are compliant. If a vendor states that their equipment is not compliant, we will, of course, take corrective action. This survey will include everything from Citizens' Gas to the company that installed the apparatus bay door openers to vendors that supply our emergency apparatus. Our first step will be to inventory all equipment that is dependent or includes computers or computer chips. Following that, letters will be sent to the vendors querying whether their product is compliant and, if not, what action needs to be taken. This project should be completed by August 1, 1999.

There is a concern among departments regarding liability and the Y2K problem. As I have stated, all departments in Marion County are making good faith efforts to correct this problem. However, since there is no real precedent to follow, we are treading on new ground and our efforts are simply the best we can do. I would ask that Congress consider removing the liability from municipal, city, town, township and volunteer fire department if their efforts to meet this problem are ineffective.

As I have stated, I feel confident that, with the efforts being put forth by the Marion County Fire Departments, if a citizen calls 911 on January 1, 2000, a dispatcher will answer and send the appropriate emergency equipment. This is the service that our citizens have come to expect and that they fully deserve and each department is striving to maintain that level of service.

In closing, I would like to express my appreciation to the Committee for this opportunity to come before you and report on the readiness of the Marion County Fire Service. I would also like to commend each of you for the efforts that you have put in to insure the safety and well-being of the citizens of our nation.

John T, Spahr
Deputy Chief
Lawrence Township Fire Department
Marion County, Indiana

Mr. BURTON. Mr. Garrison. Greg, my good friend.

Mr. GARRISON. Good morning. I will go to these comments directly, but would say, by way of introduction, when your counsel takes apart the testimony heard in the first hour this morning, which I am confident they will do, they will discover two admissions which were only brought to light by—for a guy that is not a lawyer, that is a pretty good cross-examination by a Congressman.

The first thing that you will learn if you examine the record is that the Indianapolis Water Co. misapprehends the architecture of the provision of sanitary sewage treatment and the way that is moved from the site of the residence to the site of the treatment, categorically. And this statement that was made was completely false—and I don't suggest that it was false intentionally, but I believe that he was mistaken—is that we are gravity-fed, when, in fact, we are not. From the point of the residence to the point of treatment, almost every subdivision in the northeastern quadrant of Marion County to the southern quadrant Hamilton County is forced main, driven by electricity. Eight hours without electrical power, and I would submit to you that that—that the capability of the Indianapolis Water Co. to sanitize and treat water will go something on the order of a quarter million homes whose sewage no longer can be pumped uphill, will simply be dumped into Fall Creek and into the White River.

That is how it works. We know because we had property condemned for that purpose. We had property that is low, and it is at Mud Creek, and we know that if the treatment pump at 106th and Cumberland Road quits and backs up, it dumps in, and that all goes into the water supply and then has to be treated. So, No. 1.

No. 2, upon pretty skillful cross-examination this morning, you learned if we lose our power, it takes a week to get it back. The representative from IPALCO didn't want to say that, and he tried not to three times. So, a week is a long time in January.

Mr. Chairman, let me begin by saying that I am honored to return to this seat, having testified before Congressman Horn at the last field hearing held in Indianapolis. Certainly the problems posed by this fascinating computer anomaly have not resolved themselves over the months which have elapsed since the last hearing. We face some difficult choices in the time that remains before the advent of the millennium.

In addition to the date-sensitive difficulties proposed by the problem itself, we now find that we have the all too familiar conundrum caused by the impact of politics and disingenuous conduct in the public forum by those responsible for the public interest as well. It is that problem more than any specific area of preparation that I would like to address this morning.

Probably the most glaring example of the pretext used to disguise the facts has come from the White House itself, where the entirety of this problem has been largely ignored until last summer. Since the administration has begun to address the area, we have seen repeated examples of conflicting reports, overstated accomplishments, and disinformation concerning not only the problems, but the purported efforts to correct them. For example, the success of the Social Security Administration has been extolled from the rooftops, the clear implication being that its recipients need have

no fear of a timely delivery of their checks after January 1st. Of course, such nonsense ignores, even conceals the fact, that the Social Security Administration does not print the checks nor deliver them. The Treasury Department produces them, and its preparations are much less impressive.

Another example comes directly from this committee where Chairman Horn reported, following his review of preparation by the Federal Aviation Administration under new leadership, that he foresaw more than adequate progress at that crucial department in the executive branch. Some weeks later, after having the opportunity to verify many of the claims of the FAA independently, I believe he has discovered that they were much less prepared than they said.

Public utility companies have followed the administration's lead very well, resorting to generalities of what amounts to deception at every turn; plain and direct answers have been supplanted in the public discourse by complicated recitations about all the committees empanelled, the commissions approached, the studies undertaken, and the progress made.

What has been missing from the rhetoric has been the exposition of fact. Reports from various utilities or their organizations have been long on studies and short on results, long on predictions of success and short on fact. They have, even in the surveys and reports that they have generated, failed to report with specificity the degree with which they fixed the problem.

Careful examination of such reports discloses that even the number of utilities which have been examined has been small. Further, these commissions and committees have relied on the individual utilities for reporting instead of insisting on independent audit and examination of the relevant systems. In most cases, testing has not yet been accomplished, with much of that not scheduled until this summer. Predictions of readiness use target dates dangerously close to the end of year, and nobody has proposed a plan for what they will do if the system fails the test.

Recently, we have had the opportunity to look at the transportation industry with regard to those problems. One expert told us that the biggest problem with trying to assess preparations in this area is the vast number of small carriers that make up the whole. Most of America's goods are delivered by truck, and most of the trucking is done by small or medium-sized businesses. Thousands of these businesses, continued proof of the viability of the capitalist economy and ideal, move billions of dollars worth of goods every year. However, because there are thousands of these businesses, determining how old their computers are, what date-sensitive programs they contain, and what has been done to prepare for Y2K is most problematic. Similarly, communication firms, of which there are many, all play an important part in the vast and complex interdependent system, which presently transmits not only voice communications, but also data in quantities too huge to estimate.

Mr. Chairman, my point is simple. Enormous, even heroic efforts have been commenced all over the American landscape, both public and private, to address and correct this computer mess. Much has been accomplished in a short time, evidence once again of the power of a free people to address challenges and find solutions.

However, it is late enough in the game that exclusive focus on the fix is no longer responsible—no longer a proper discharge of trust and stewardship owed to the people by government, as well as private enterprise.

It has become fashionable over the last 25 years to filter information and to shade the facts. "Don't ask, don't tell" has spread like some kind of virus throughout government and industry alike, a legacy much more likely to survive the merciful end of this administration than even the manifest disgrace so painfully obvious in other areas.

No one can divine the motivations of this administration or the many industries in the private sector for refusing to encourage preparation for the possibility of such interruptions. We are a great and resourceful people, Mr. Chairman. We have demonstrated with steadfast consistency over the entire history of this Republic we can and will address adversity whenever we must. We must be told. Our people are not bereft of their greatness only because of their present prosperity, not rendered incompetent to care for themselves only because they are led by persons who seek to encourage a society of a governmental dependence. We must be told in clear terms just what the problems are and how long they may last. There is nothing alarmist about encouraging communities to do some planning to help families to recognize that brief interruptions in their life-styles may occur. We have now arrived at a new scheme: "Ask if you want, we will not tell."

I encourage the Congress to address the issues of preparation. The fact that people may be complacent is a temporary state. They continue to live in the present because they are led to believe that it will continue without interruption. When they are told otherwise, they will react, pull together, make reasonable preparations and succeed as they always have. The time has come to tell the people that they may experience some temporary electrical failure called "rolling brownouts," as the experts call them. They may face temporary stoppage in the flow of goods and services, or even some break in communication, if only for a few days. It is not unreasonable for the diabetic to stock up on insulin or the heart patient to buy some extra nitroglycerin. Such preparation is not alarmist, it is simply smart living. And so far, this administration has again indulged itself and the people in another fiction, one dealing with some problems that may be unavoidable, and certainly suggest the need for advance preparation.

In response to the mantra of Mr. Clinton's information managers, I would suggest that we say to them, "It's not the economy; it's the truth, stupid." The truth is a commodity that has been in short supply there these past years. Certainly, there is no better place than in the Congress of the United States for the truth to be spoken. Address the subject of responsible preparation. Tell the people. Do not try to take care of them, just tell them the unvarnished truth, and they will take care of themselves. Thank you.

Mr. BURTON. Well, I will definitely have some questions for Mr. Garrison. You are very interesting and controversial, as always.

[The prepared statement of Mr. Garrison follows:]

**BEFORE THE CONGRESS OF THE UNITED STATES**

TESTIMONY OF J. GREGORY GARRISON REGARDING
THE YEAR 2000 AND REMAINING COMPUTER ISSUES.

*"READY OR NOT"*

Mr. Chairman, let me begin by saying that I am honored to return to this seat, having testified before Congressman Horn at the last field hearing held in Indianapolis. Certainly the problems posed by this fascinating computer anomaly have not resolved themselves over the months which have elapsed since that last hearing. We face some difficult choices in the time that remains before the advent of the millenium. In addition to the date sensitive difficulties posed by the problem itself, we now find we have the all-too-familiar conundrum caused by the impact of politics and disingenuous conduct in the public forum by those responsible for the public interest, as well. It is that problem, more than any specific area of preparation, that I would like to address this morning.

Probably the most glaring example of pretext used to disguise the facts has come from the White House itself, where the entirety of this problem was largely ignored until last summer. Since the administration has begun to address the area, we have seen repeated examples of conflicting reports, over-stated accomplishments, and disinformation concerning not only the problems, but the purported efforts to correct them. For example, the success of the Social Security Administration has been extolled from the roof tops, the clear implication being that its recipients need have no fear for the timely delivery of their checks, after January 1. Of course, such nonsense ignores, even

conceals the fact, that the Social Security Administration does not print the checks. The Treasury Department produces them, and its preparations are much less impressive. Another example comes directly from this committee, where Chairman Horn reported, following his review of preparations by the Federal Aviation Administration under new leadership, that he foresaw more than adequate progress at that crucial department of the executive branch. Some weeks later, after having the opportunity to verify many of the claims of the FAA independently, I believe it was discovered that they were much less prepared than they said.

Public utility companies have followed the administration's lead very well, resorting to generalities and what amounts to deception at every turn; plain and direct answers have been supplanted in the public discourse by complicated recitations about all the committees empanelled, the commissions approached, the studies undertaken, and the progress made. What has been missing from the rhetoric has been the exposition of fact. Reports from various utilities or their organizations have been long on studies and short on results, long on predictions of success and short on fact. They have, even in the surveys and reports they have generated, failed to report with specificity the degree to which they have fixed the problem. Careful examination of such reports discloses that even the number of utilities which have been examined has been small. Further these commissions and committees have relied on the individual utilities for reporting, instead of insisting on independent audit and examination of the relevant systems. In most cases, testing has not yet been accomplished, with much of it not scheduled until this summer. Predictions of readiness use target dates dangerously close

to the end of the year, and nobody has proposed a plan for what they will do it the systems fail the tests.

Recently we have had the opportunity to look at the transportation industry with regard to these problems. One expert told us the biggest problem with trying to assess preparations in that area is the vast number of small carriers that make up the whole. Most of America's goods are delivered by truck, and most of the trucking is done by small or medium size businesses. Thousands of these businesses, continued proof of the viability of the capitalist economy and ideal, move billions of dollars worth of goods every year. However, because there are thousands of these businesses, determining how old their computers are, what date-sensitive programs they contain, and what has been done to prepare for Y2K, is most problematic. Similarly, communications firms, of which there are so many, all play a part in the vast and complex, interdependent system which presently transmits not only voice communications but also data in quantities too huge to estimate. The issue of systems integrity and the specter of the contamination of large segments of this array of connected arrangements receive little attention, in large measure because solutions appear difficult if not impossible.

Mr. Chairman, my point is simple. Enormous, even heroic efforts have commenced all over the American landscape, both public and private, to address and to correct this computer mess. Much has been accomplished in a short time, evidence once again of the power of a free people to address challenges and find solutions. However, it is late enough in the game that exclusive focus on the fix is no longer responsible—no longer proper discharge of the trust and stewardship owed to the people by government as well as private enterprise. It has become fashionable over the past twenty-five years to

filter information and shade the facts, often to the exclusion of the truth, for the stated purpose of not causing consternation in the population. "Don't ask, don't tell," has spread like some virus, throughout government and industry alike, a legacy much more likely to survive the merciful end of this administration than even the manifest disgrace so painfully obvious in other areas. It has held the floor throughout the last year's discourse on the Y2K issue. The time has come to level with the people, beginning to advise them with some clarity concerning the likelihood of at least temporary interruption in the delivery of goods and services, electrical power and the flow of money in the marketplace.

No one can divine the motivations of this administration—or of the many industries in the private sector—for refusing to encourage preparation for the possibility of such interruption. We are a great and resourceful people, Mr. Chairman, and we have demonstrated with steadfast consistency over the entire history of this republic that we can and will address adversity whenever we must. But we must be told. Our people are not bereft of their greatness only because they are presently prosperous, not rendered incompetent to care for themselves only because they are led by persons who seek to encourage a society of governmental dependence. But we must be told in clear terms just what the problems are and how long they may last. There is nothing alarmist about encouraging communities to do some planning or helping families to recognize that brief interruptions in their life styles may occur. There is everything dishonest in continuing to pretend things are fine, when they are not. We have now arrived at a new scheme, "Ask if you want, we won't tell."

I encourage the Congress to address the issues of preparation. The fact that the people may be complacent is a temporary state. They continue to live in the present because they are led to believe that it will continue without interruption. When they are told otherwise, they will react, pull together, make reasonable preparations, and succeed as they always have. The time has come to tell the people that they may experience some temporary electrical failures, or "rolling brownouts," as the experts at times predict; they may face temporary stoppage in the flow of goods and services, or even some break in communications, if only for a few days. It is not unreasonable for the diabetic to stock up on insulin, or the heart patient to buy some extra nitroglycerin. Such preparation is not alarmist; it is simply smart living. And so far, this administration has again indulged itself and the people in another fiction—one dealing with some problems that may be unavoidable, and certainly suggest the need for advance preparation.

In response to the mantra of Mr. Clinton's information managers, I would suggest that we say to them: "It's not the economy; it's the truth, stupid." Truth is a commodity that has been in short supply over the past years. Certainly there is no better place than in the Congress of the United States for the truth to be spoken. Address the subject of responsible preparation. Tell the people. Do not try to take care of them, just tell them the unvarnished truth, and they will take care of themselves.

Mr. BURTON. Ms. Ekins, a tough act to follow.

Ms. EKINS. Mr. Chairman and members of the committee, I appreciate the opportunity to speak before you this morning. My name is Kate Ekins, and I am the manager of public affairs at St. Vincent Hospitals and Health Systems. At St. Vincent, we have over 1,000 beds across Indiana, and we employ over 6,000 individuals.

The issue you have chosen to address is very important to the medical community. At St. Vincent, we feel we have made great progress in our preparations for January 1, 2000, and plan to be complete with all of our preparations by September of this year. Our preparations began in 1996. Focus throughout the last 3 years has been on patient care. As a health care provider, we are strong advocates for our patients.

As part of our Y2K readiness, we looked at several areas of our delivery system. These included medical devices, supplies, our internal computer systems, central services, such as power and water and staffing. Just to go through a few of those, what we looked at with medical devices was ensuring that all the devices were going to be functioning properly. We obviously purchase those—this equipment from other vendors, and so we need to test them to make sure that they are compatible with our systems internally.

Our supplies, we are looking at having adequate number of supplies, such as pharmaceuticals and bandages and oxygen. We anticipate that all hospitals throughout the country, and other providers, will be doing this, so we have already begun our effort in controlling our purchasing so that by January we have about a month's supply in case of some sort of unforeseen occurrence.

Our internal computer systems, we are presently about 75 percent computer-driven in terms of other doctors' orders, and everything that is done is done via computer network as opposed to paper-driven. And so we are working with them. We updated our contingency plans that exist for those already, so we are prepared with a paper-driven plan for this model should these systems fail.

Staffing we are looking at right now in terms of maintaining a high level of care throughout the transition, and we are planning to make sure that the appropriate staff will be available throughout the hospital.

And then the central services for us, power and water, any type of utilities, are similar to what you heard earlier today, and we will be relying on the different utility companies to perform what they have performed in the past. But we do have contingency plans in case of a disaster. We have generators, and we have backup supplies in other areas in terms of them. We are also developing contingency plans to house people from nursing homes or other facilities should our hospital be the one site with power and water. We have also developed a plan for us to evacuate our patients should that be necessary.

And the secondary concern we have with Y2K is one of cash-flow. Our equipment for processing bills and claims has been checked, and it is ready; however, we are unsure of where our payers stand in this preparation. So, we have a contingency plan developed should we encounter problems in the area of reimbursement.

The final effort we are making internally is educating our employees on how they can be prepared in their personal lives and their families for Y2K. We are confident that our employees will be more willing to come in to help at the hospital if they feel comfortable that their families are safe while they are away.

The bottom line for hospitals across the State and across the country is that we are always prepared for disasters; we are always anticipating something such as tornado or an ice storm, or even bomb explosions. And people who work for hospitals are always prepared for these type of emergencies. No one is entirely sure about what complications will arise with Y2K, so our commitment to be prepared to the transition is unwavering, and the people we serve deserve nothing less. Thank you for this opportunity.

Mr. BURTON. Thank you, Ms. Ekins.

[The prepared statement of Ms. Ekins follows:]

**Testimony By**
**Kate Ekins**
**Manager of Public Affairs at St. Vincent Hospitals and Health Services**

**Before the Committee on Government Reform**
**April 19, 1999**

Mr. Chairman and Members of the Committee

I appreciate the opportunity to speak before you this morning. I am Kate Ekins, Manager of Public Affairs at St. Vincent Hospitals and Health Services. St. Vincent as you may know, has over 1,000 beds across Indiana. We employ over 6,000 Associates.

The issue you have chosen to address is one that is very important to the medical community. At St. Vincent, we feel we are making great progress in our preparations for the year 2000.

Our preparations with Y2K began in 1996. The focus throughout the last three years has been actually on Patient Care. As a health care provider, we are advocates for our patients.

As part of our Y2K readiness, we looked at several areas of our delivery system. These included:

- Medical Devices
- Supplies – pharmaceuticals, bandages, oxygen
- We anticipate that all hospitals and providers will be doing this so we have already begun our efforts in controlling supplies to have an additional one-month supply at the end of the year.
- Our Computer Systems used to enter doctor orders
- These are periodically "down" so we are prepared with paper-driven contingency plans
- Essential Services – Power, Water
- We have contingency plans already written for disasters. These are being reviewed and broadened in the case of some type of outage, and have resources to provide power and water in that event.
- Staffing
- Our objective is to maintain a high level of care through the transition
- Appropriate staff will be available throughout the hospital
- Certain staff have already been identified as "necessary" for an emergency
- We are creating an alternative communications mode in order to comfort our patients, Associates and the community at large.

We have also developed contingency plans for all of these areas should we experience any problems. We have a contingency plan to house people from nursing homes or other facilities, should our hospital be the one site with power and water. We have also developed a plan for us to evacuate our patients, should that be necessary.

A secondary concern with Y2K is one of cash flow. Our equipment for processing bills and claims has been checked and it is prepared. We are unsure of where our payers stand in its preparation. We will have a contingency plan developed should we encounter problems in the area of reimbursement.

The final effort we are making is educating our Associates on how they can be prepared in their homes and personally for Y2K. We know that our employees will always be willing to help in a time of crisis. However, we want them to feel that their families are safe while they are assisting at the hospital.

No one is entirely sure about Y2K complications, so our commitment to be prepared for the transition to January 1, 2000, is unwavering. The people we serve deserve nothing less.

Mr. BURTON. Do you want to start the questions?

Mr. HORN. Whatever you wish, Mr. Chairman.

Emergency response agency. Let me pose one to you, Sheriff, in particular. Most of the 911 emergency dispatch centers, known as public safety answering points, I guess, in the jargon, are highly automated, and they are particularly in the case of the enhanced 911 systems. Have the local 911 systems been thoroughly tested, and what do the tests show?

Mr. COTTEY. As Councilman Curry stated earlier, Congressman, that will be done this summer, and we feel very confident that things are in place. Councilman Curry and my committee, as well as the chief of police and his people, meet about every 30 days. We have been doing this for over 2 years. We feel very comfortable, and we feel when the test takes place around July, early August, things will be where they need to be.

Mr. HORN. Are you planning to give extra training to people that answer the calls?

Mr. COTTEY. Yes, we are.

Mr. HORN. Because I am sure there will be quite a different situation.

Mr. COTTEY. We have about 154 employees at the communications center.

Mr. HORN. Do you really? And that just covers Marion County?

Mr. COTTEY. All of Marion.

Mr. HORN. All Marion.

What do those counties surrounding Marion do?

Mr. COTTEY. Well, they have a 911 system also, but it is just like anything—it is not as large as ours because of the area here. But that is an area that the State police at this time through the legislature which is meeting is trying to correct that to make that more of a statewide to help the smaller communities. That went on to the statehouse right now.

Mr. HORN. Yeah, I agree with that. I think the real problem in America is the small communities that simply don't have staff.

Mr. COTTEY. And, Congressman, if this goes through the legislature this time, the State police superintendent has advised me that they are ready to put that in place.

Mr. HORN. According to the Bureau of Justice Statistics, there are over 17,000 police and sheriff departments in the United States. And has the Marion County Sheriff's Department coordinated its year 2000 efforts with other local law enforcement agencies? You are saying it is really the State police's responsibility?

Mr. COTTEY. Right here in Indiana they are doing most of that.

Mr. HORN. And what types of problems, besides the fact that you haven't tested for them, do you expect to have? Or did you deal with the test?

Mr. COTTEY. Well, talking to Mr. Curry, him and I do stay right in bit of contact. He is a guy I greatly respect. I am not a computer expert, believe me, and I feel he is, and he just feels the things that have been going on with vendors, and the things that are in place, that he feels that when we test it, it will be a positive science when we test it.

Mr. HORN. When you say "going on with vendors;" what do you mean?

Mr. COTTEY. Well, Mr. Curry, the city/county, as he stated earlier, we spent about $12 million for all city and county government, including public safety. And he has been meeting with them and bringing outside vendors to bring up—bringing equipment in, to ensure when we are ready to test, that those things will work properly. And, you know, just like—I don't think none of us can sit here and say for sure that we ought not have any problem, but I was just making a few notes on some of the things we have been through in the last 4 years, such as a major snowstorm where nobody can move around for about 2 weeks; a tornado last June that hit the entire east side of Marion County, the south side of Marion County at the same time; disturbances that went on two or three different areas in this community; the bomb scares; hostage situation; and we have always been there, and I am confident that we will be there after the testing in July.

Mr. HORN. Now, FEMA, the Federal Emergency Management Agency, is taking quite an interest in this. Has there been any direct relationship between the regional office of FEMA and your office?

Mr. COTTEY. Well, here again, the local emergency management and people who I have assigned, along with Mr. Curry, meet with them periodically on this.

Mr. HORN. And that is the State/county part of FEMA?

Mr. COTTEY. Right, right.

Mr. HORN. So, you are pleased with the support granted by those agencies then?

Mr. COTTEY. I have not heard any negatives yet. I think Congressman Burton will tell you when I hear negatives, I am usually not bashful.

Mr. HORN. You are not shy?

Mr. COTTEY. No.

Mr. HORN. And, Mr. Spahr, in terms of the fire trucks and ladder equipment, have they been checked for 2000 compliance?

Mr. SPAHR. Ours have not. This is something we are going to have to be contending with. We are fortunate in that a majority of our fire apparatus is one company. So, consequently we are going to be approaching, first of all, the person who sold it to us, and second, it appears, the manufacturer who produced this equipment, along those lines.

I will be frank with you. We have little idea of how the tests are done—not a lot of information has been disseminated among the fire service.

Mr. HORN. Now, is that true nationally or just State or what?

Mr. SPAHR. I think it varies. I think probably one of the biggest issues is knowing where to go to get that information.

Mr. HORN. I will give you an example, and then I was going to ask Mrs. Ekins—we could combine these two.

After I held a hearing in Indianapolis last year, I went to Cleveland, and in Cleveland we had the Cleveland Clinic testify. That is one of the world's—Nation's major medical centers. They had created a Web site where, if you checked, say, emergency room equipment, you looked up the manufacturer's number, the manufacturer, where you track that down, so not everybody has to reinvent the wheel 17,000 times, in the case of sheriffs and police of-

ficials, and they would put it on there, and everybody could check it.

Now, I was going to ask Ms. Ekins if they were doing this here in Indiana, or did they feed into the WWW, World Wide Web, that has been set up to deal with emergency room equipment of which there are hundreds of different manufacturers, all the rest of it, including the sort of paramedic vans that often are under your fire department control, and checking them out on the equipment used between the time you pick up the patient and end at the hospital.

Ms. EKINS. We have done a little of both, as far as using that as a first source of information and then double-checking on our own.

Mr. HORN. Now, did you find you had pieces of equipment that they didn't have on that Web?

Ms. EKINS. Uh-huh.

Mr. HORN. Yeah, well, I just would hope that, frankly, the International Association of Fire Chiefs would be able to establish that Web.

Mr. SPAHR. This is something, to be honest with you, Congressman, they may have. We just have not investigated it as yet.

Mr. HORN. I was wondering, if you pay dues to this crowd, if they give you services.

Mr. SPAHR. And indeed, as I said, they may very well have that.

Mr. HORN. Because there are 32,000 fire departments, I am told by staff, and, in your judgment, you haven't had a chance to look at the equipment yet?

Mr. SPAHR. Exactly.

Mr. HORN. And what is your contingency plan, if something goes awry?

Mr. SPAHR. Well, basically, again, this is something we are not to the point yet of even finalizing. We have concentrated the first quarter of this year simply on this computer system. This has been enough of a challenge for this first quarter.

The next phase that will be is to begin contacting vendors to see if they feel that they are compliant. Following that, again, as you said, we need to investigate these things, and the apparatus and the equipment, the bay doors, the HVAC system, things of that nature, And in that respect, we are probably a little behind. However, we feel that, fortunately, the majority of our vendors are local. It is not like we have to fly people in from Washington State or something.

So this has not been—has not been adequately or completely addressed as yet, but I feel it will certainly be by the end of the second quarter or third quarter.

Mr. HORN. When I was in New Orleans last August on a hearing, we had the chief executives of Baton Rouge before us. Baton Rouge had checked their ladder and their pumper. One was 2000-compliant, one wasn't. And you had a case, if there is a fire on the fifth floor, why, you got a water supply, but you can't get it up there to get people into safety. So at that point the New Orleans chief executive said, gee, I hadn't even thought of checking the fire department. But, you know, we are now almost a year—or a half year.

Mr. SPAHR. There is an organization here in Marion County, Marion County Fire Chief's Association, and I think that this will be the proof that will bind all this together. Again, as I have said, we have got 12 or 13 different fire departments, and one purpose of this association is to meet and share information.

Mr. HORN. Share.

Mr. SPAHR. Share, and consolidate those things.

Mr. HORN. We passed a Good Samaritan bill in the Congress, and it is law, so in case of private industry, certainly they can have an antitrust judgment thrown out when they are sharing information. In our hearings last year, we found that some of the most competitive firms between each other were now working together, and that is as it should be.

I have one question for you, Ms. Ekins, as to what are the contingency plans that St. Vincent's Hospital and Health Services has in mind if it all doesn't quite work out. Are you getting generators?

Ms. EKINS. We have backup generators. That is what I was just saying in my remarks. We have backup generators. When there is an ice storm—they had a winter up in northwestern Indiana that shut down the northwest quadrant. Hospitals were basically one of the few places that had power. So we have—we have almost standard contingency plans for just about everything that could happen.

Mr. HORN. What is the length of time your generators can give you power in the hospital?

Ms. EKINS. That I don't know.

Mr. HORN. Two weeks, 1 week?

Ms. EKINS. I think so.

Mr. HORN. Two months?

Ms. EKINS. We are developing everything to a 1-month for the month of January so that we would be able to get through any sort of program.

Mr. HORN. So when I say to people it would be prudent—not being a panic scarist, but it would be just prudent if people had, say, several weeks of food, maybe a month. When I tell that to my Mormon friends, they smile and they say, we have been doing that for years. They are the only group I know in America that has planned ahead for that for a year. So, anyhow, that might the prudent at the hospitals to do.

What are the greatest risks to you so far that you have in terms of that sort that surprised you?

Ms. EKINS. Well, the greatest risk would be if we have to move our patients out of the hospital, just because of the size of our hospital. It is probably the second largest, you know. Just—there are not a whole lot of other facilities nearby to take people, and if we are in trouble, then it is likely to assume that the other hospitals in town would be in that same situation.

Mr. HORN. How many beds do you have at St. Vincent's?

Ms. EKINS. At our 86th Street facility, we have 465. Then we have a hospital—we have four other hospitals around the State that are smaller. In some we have 40-bed neonatal intensive care units, which those children would be probably the most critical of anyone to move.

Mr. HORN. These are the preemies.

That is all I have, Mr. Chairman.

Mr. BURTON. Thank you, Mr. Horn.

The fire departments and the sheriffs departments and the other law enforcement agencies, what kind of a coordinating mechanism have you arranged? For instance, I mean, if we had a major electrical breakdown; for instance, you might have a real jump in crime or some kind of emergencies. If the stoplights went out, and there was a multicar accident, or criminals were taking advantage of an electrical outage, what kind of coordination and communications abilities do you have between various fire departments and police departments and law enforcement agencies across county lines?

Mr. COTTEY. Mr. Chairman, we can all talk, believe it or not, together. It isn't like it used to be 10 years ago, just like the Indianapolis department and Marion County Sheriff Department were on different frequency in the radio systems. The way the setup has been for the last 10 years, we can all communicate by going to different channels with each other. Like I say, we have used backup several times through storms. We have had to startup our alternative source. It has always worked. We can just communicate with each other right now.

Mr. BURTON. Do you have—and I would like for Mr. Spahr to answer these questions, too—do you have any kind of a contingency plan worked out where you would coordinate or work with, say, the sheriff's department in Hamilton County or Johnson County to help them with an emergency situation?

Mr. SPAHR. In our particular district, we are in the northeastern portion of Marion County, so we work very closely with Hamilton County always. We have communications capability with them. So, we are—in that respect we are in very good shape. And, again, we have a very good familiarity with them.

Mr. BURTON. What I am trying to get at, has there been any contingency plan made? Let's say that there was a major catastrophe in Johnson County or Hamilton County or Hancock or Hendricks, or whatever happens to be around Indianapolis, and they didn't have the capability to deal with that. Have there been any coordinated efforts between our law enforcement agency in Indianapolis and our fire agencies to deal with that kind of problem?

Mr. SPAHR. There stands an agreement, and it has always stood. It is a mutual aid agreement. Essentially we will respond to any call for help, be it to another department, to another county, whatever. Obviously, we will not—we still have our own obligations at home. We will not strip our department, but we will certainly respond to any department, much the same as Marion County would respond to IPD's call for help, or even out of county if necessary. So, that is actually nothing new. We have been practicing that for years.

Mr. BURTON. But you will be prepared to do it.

Mr. SPAHR. Exactly yes.

Mr. COTTEY. Mr. Chairman, we continually do. Calls may come from Hancock County. We have been as far away as Columbus, IN, Bartholomew County, on bomb scares, or things like that, or disturbances. That is just an everyday thing, just there was an agreement.

Mr. BURTON. I wasn't aware. I didn't know you could go out of the county.

Sewage, you know, that is a big concern. You seem very concerned about that in various parts of the city, because the indication was, Greg, that we were, if not misled, didn't get the whole story from the water company and the utilities about how they would deal with because they are not gravity-fed in its entirety.

What I would like to know is it would be a tragedy if we had an electrical breakdown, because of the grid system or for whatever reason, for a week. And if the sewage that doesn't flow uphill started going back the other way into everybody's house, I mean, it could cause a real health problem. Can you elaborate on what you were saying?

Mr. GARRISON. Here is—this turns out to be the biggest "if" in all of our joint lives. And the problem that I see with the public discourse over the year, whether it is—although I am quick to say that I think the finance—the money and banking area and communications are probably a quantum leap ahead of everybody else. I think that is obvious from the kind of answers you got this morning. These guys at this end of the table were much more specific about what they can do, what they tested and where they were than these guys down here.

The interdependency problems are things that are terrifying. Look for a moment at they lost power in southeastern California because up in Idaho someplace, I think it was, a branch fell——

Mr. HORN. San Francisco they lost power.

Mr. GARRISON. Huge problem. One little mistake. You have those kind of——

Mr. HORN. New York, you will recall, also.

There is one thing we can say out of these blackouts are that 9 months later there is an increase in population.

Mr. GARRISON. I am hoping that is true again, now that there is a correction of it. When you have one of those, you have the makings for a bunch of good one-liners on the Johnny Carson/Jay Leno. When you have got 50 of them or 100 of them, then you have a problem of overwhelming a system.

Assume for a moment that, not our worst fears, but a significant problem takes place. Well, we have what the experts call the rolling brownout, moves around in the circle, which is fed by an IPALCO-provided center plus Public Service Indiana. When they fail, this domino begins to tumble down, and it is indiscriminate. The hospitals are suddenly on generator power. If they have got 3 days or 5 days of generator fuel, they are still running. Are they running their CAT scan? I doubt it, because the thing draws too much power. Are they able to run the surgical suites? That is another question. It is not full service, and I think they will be quick to tell you, we don't just run forever on that much diesel fuel. That generator probably uses 8 to 10 gallons per hour, just one of them.

Look with me at the water problem just for a moment, and this is one that nobody has really wanted to talk about very much. When the electricity goes out in northern Marion County, southeastern Hamilton County, because that's where Dan lives, where I live, where we know what that looks like, at that moment, in addition to all these obvious problems about stoplights and telephone service and whatever else, the electric generator or the electric pumps that sit in places underground 6 or 8 feet, 10, 12 feet deep,

at places like 106th and Cumberland Road, north of my house and all around you, that pump uphill, it runs gravity, I believe, to those lift stations, where it has got to be pumped the rest of the way. Or it is the other way around, I forget which. But I know none of them are gravity-fed. That is why Mr. Beering, I believe his facts are incorrect. Virtually every platted subdivision in the metropolitan area has forced—main service at someplace. Wherever this stuff has got to start going uphill, you got a problem.

What I understand to be the situation from when we represented some people who were having land condemned, when they were building these things, the bad news is that that station quits working, out into the water it goes. A little place behind my cousin's house called Mud Creek, and it is about the width of that table, but it draws a lot of water per year.

Mr. BURTON. Let me interrupt for just a second. I am concerned about the effluent going into the waterways and ultimately into the reservoirs, which would have to be dealt with, but I am also concerned about the backup of sewage into residentials.

Mr. GARRISON. It goes both ways, Congressman. That is our problem. What happens is it goes downstream and gets down to try to protect those homes. It goes into the water supply, and it very quickly overwhelms the Indianapolis Water Co.'s ability to purify it. So there is the problem No. 1.

Other problem is if it is forced main, if it is drawing through and there is no gravity from the houses down, and it backs up, and then pretty soon you got every residence in that area that is incapable of sustaining human life. Looking at 12 to 24 hours before cholera breaks out.

Sounds, oh, my golly, what kind of alarmist have we here? Just basic biology, basic physics. The question is: What happens? Where does it go? It is gravity to the pump, and it is forced from there to the point where it is treated. I believe that is the way the thing works. So your immediate problem is not making the houses uninhabitable, your immediate problem is what happens to the water supply. But over time, if our friend the electric company is right and it takes 7 days to get the juice running again, you may have both problems.

My question next is if that takes place, and sewage is not a problem upstream, going down, what about this water system that has been overwhelmed? Does it run out? Do they turn it off? Does it start pumping impure water? It takes very little time before our friends in the hospital business have got a real problem when people start getting dirty water.

That is the kind of complex view of things that I don't hear.

Now, they sit around, and they make a lot of pretty pictures. But I want to know, did you plan that, Mr. Water Company Man? Mr. Power Guy? Did you talk your way through a 5-day power failure and its impact; not whether your lights work. I could care less. Now, whether my sewage plant works; it, by the way, runs on electricity, too, as does my pump—they push water with electricity. So all those things work together to make us uncomfortable when we hear platitude-laden presentations like you heard today. I was disappointed myself. Three times you asked him before the guy finally

had to 'fess up, A, something around a week; B, I am not sure I even know.

Mr. HORN. Why don't we have the respective utilities see the testimony and add what they would like to with the testimony.

Mr. BURTON. I think the respective utilities have left.

Mr. HORN. No, but, I mean, we will send them the questions and let them file it at this point.

Mr. BURTON. What I would like to do, I think it is a good idea. Greg, why don't we have you give us a list of the concerns that you had and maybe others might have had from listening to their testimony, and then we will send those questions to them and ask for some kind of response.

Mr. GARRISON. I think if you are going to—before you are finished with this huge undertaking, Congressman, really know with some specificity what the facts are, you got to stop talking to lobbyists and the boys at corporate offices. I would be a lot happier with a bunch of guys with pocket protectors sitting here that were running that machinery, because I don't get the same thing I get from them as I get from politicians and from the lobbyists.

We had a lobbyist here this morning. I forget which one. Legislative service guy is a lobbyist. What does he know about electrical power? I mean, it is a real big—one of the things we found in our interviews on my show——

Mr. BURTON. He has been working on this for some time.

Mr. GARRISON. We have stayed away from what you called the blackout crowd. We are sticking in the middle of the fairway, with the Edward Yardeni of the world and with people like Richard Lugar to talk to. We are not getting out there into wacko land at all. The people that we have talked to, very concerned, intelligent people. When they talk to the wrench-twisters of the world, the guys that fix things when they go wrong, they get a real different picture.

For example, the NERC, Northeastern Electrical Reliability Council, that is interesting reading. Brian Vargus was here. I asked him, what would you think of a statistical sample that was less than a substantial fraction of the reported public? Well, they didn't talk to everybody. NERC is basing its grandiose predictions that things are going to be fine on the basis of a bunch of independent reports, not verified. And there is a whole bunch of the little mom-and-pop REMCs that didn't respond at all. Now, I ask you, what happens when half a dozen of those REMCs go black? Ask your friends in the grid about that. Don't ask some lobbyist about it. Ask one of those engineers that runs those things, and you will get a real different answer.

One of the things that happens is they shut them off. Those people go into darkness. You can do that. I mean, that is electromagnetic. As I understand it, that switching is noncomputerized. What shuts off electrical power is electromagnetic, greater than 360 cycles per second or something, and that fast, those people that have a problem are shut down. But if there is a number of them, your problem is just as great as it ever was even if IPALCO is still running. So, I will be happy to ask those questions.

Mr. BURTON. I asked the question last night of the gentleman from IPALCO because I seem to be more concerned about elec-

trical, electricity, because it powers so many other things. And I asked him about the generator, which I asked about today, and his indication was he didn't think that was necessary and warned against people improperly installing them. From your research, and I know you have worked on this on the radio for a long time, that is why I wanted to have you on one of these panels, would you think it would be prudent to have a generator?

Mr. GARRISON. He is wrong, and he is wrong for all the wrong reasons. He is worried about what they call backfeed, which is when the power comes back on with the generator running. But instead of taking that bull by the horns and saying, boys and girls, we may have a problem for a while, if you are going to buy one, don't buy some little $1,500 Honda guy that has got 1,000 that has got 10 kw on it, get one with 10,000 watts.

It is unfortunate what is happening. There is no dissemination of important information. Gasoline is a very poor fuel supply because it goes stale very quickly, and it is not near as—it is volatile, as we know all know from TV, and it is not efficient. It burns faster. Diesel generator is much better. Anybody that buys a 250-watt, a 1,000-watt, 1,500-watt, 2,000-watt generator is just wasting your money. You can't drive your refrigerator with that for very long. And the most important thing is you can't drive anything that generates heat with that small of a power supply. It takes about 6,000 watts, or 6 kw, to be able to drive one resistance heat thing, like your range to cook your food on or your hot water heater.

So, we don't have any information. We got people out there going to Tractor Supply and buying a 1,000-watt generator and thinking they are going to do themselves a favor. It is gasoline-powered. They run out of gas in 12 hours. Now where are they? Diesel is much better.

He is right about one thing. It has got to be installed by the pros. They come with all kind of toys on them. You can buy one that fires itself up every 7 days to test itself. To me that is just more things to go wrong. The switch is $2,000. We didn't know that, except we did a little research and found out; $2,000 for the switch, if you buy the fancy one. But then you can buy the one for $600, you throw on one, turn off the other one, it works just fine. Those are pieces of information nobody has got.

The same guy that is worried about backfeed, doesn't think a generator is a good idea, thinks it will take him a week to get us back. I tell you what, you remember last January? It is cold here. A week with no power, there will be a lot of suffering.

Mr. BURTON. Any other questions?

Mr. HORN. Just one to the law enforcement and fire authorities. You have a State police. Do the universities have separate police departments, their own university police?

Mr. COTTEY. Yes, they do.

Mr. HORN. What other groups beyond the normal geographic area of the city or township or county; how many other police departments are there?

Mr. COTTEY. Outside Marion County, Congressman?

Mr. HORN. Just statewide.

Mr. COTTEY. So many that you have towns, small towns with maybe a town marshal; you have other towns with maybe a town marshal, and three deputy marshals.

Mr. HORN. Well, you have probably got 1,000 different law enforcement groups in Indiana.

Mr. COTTEY. Right, right.

Mr. HORN. Now, you mentioned that you had good communication. I found in Los Angeles, which is L.A. County, has 10 million people; the city of Los Angeles, 3 million; Long Beach is second with maybe a half a million. And the university police we all have, which there are a number of State universities there, this is now 10-year old data, but the fact was they just couldn't communicate with each other because all of the frequencies were on the east coast. Now some of those have been moved. And I just wondered, can the whole police law enforcement group within Indiana really reach each other when the chips are down?

Mr. COTTEY. One of the key things, like I stated, is what the superintendent of the State police is trying to get passed now. That will be a big step forward. But usually what happens, there are 92 counties in the State of Indiana, 92 sheriffs, and most of the smaller agencies work through that local sheriff and that county is the way it usually works.

Mr. HORN. So, can the 92 sheriffs now communicate on one frequency?

Mr. COTTEY. No.

Mr. HORN. You can't?

Mr. COTTEY. No.

Mr. HORN. Are we kidding ourselves that we will have interoperability between jurisdictions? I mean, you are correct when you say fire departments have had this for years, where you share if somebody has a crisis?

Mr. COTTEY. I can say that Marion County and surrounding counties, which is a lot of population in the State, we can communicate. With the other areas, if the State police gets this passed, that will take care of the rest of the small departments throughout the State.

Mr. BURTON. Well, let me end up by saying thank you very much. You have allayed some fears and created a whole lot more. Appreciate that, Greg. I am going to have to get together with you and do some serious talking. And I would like to have the concerns that you have expressed in writing. I know it is a lot of work, but I would like to have that because I will submit those to the relevant utilities and get that information back to myself and the committee.

Mr. GARRISON. Congressman, we are a clearinghouse. What we could do is give you the authorities themselves. There are four or five people who you can talk to, that your staff can interview directly, that will be happy to pick the phone up and answer your questions right now. You will know many of the names. I mean, there are many.

Mr. BURTON. Any of that information we would like to have.

[NOTE.—The information referred to was not available at the time of print.]

Mr. BURTON. I don't have anything else to say, but I want to thank Bill O'Neill on our professional staff for what he has done; Lisa Arafune, the clerk; Matt Ryan; Mike Yang, minority counsel, thank you; Mike Delph on my staff; Tim Davis and Jim Atterholt, all on my staff; and Marilyn Jones, our court reporter, thank you very much. Thank you very much for being here. We stand adjourned.

[Whereupon, at 11:56 a.m., the committee was adjourned.]

○