YEAR 2000 CONVERSION EFFORTS AND IMPLICATIONS FOR BENEFICIARIES AND TAXPAYERS

HEARING

BEFORE THE

COMMITTEE ON WAYS AND MEANS
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

FIRST SESSION

FEBRUARY 24, 1999

Serial 106–91

Printed for the use of the Committee on Ways and Means

U.S. GOVERNMENT PRINTING OFFICE
66–850 CC WASHINGTON : 2001

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402

COMMITTEE ON WAYS AND MEANS

BILL ARCHER, Texas, *Chairman*

PHILIP M. CRANE, Illinois
BILL THOMAS, California
E. CLAY SHAW, JR., Florida
NANCY L. JOHNSON, Connecticut
AMO HOUGHTON, New York
WALLY HERGER, California
JIM MCCRERY, Louisiana
DAVE CAMP, Michigan
JIM RAMSTAD, Minnesota
JIM NUSSLE, Iowa
SAM JOHNSON, Texas
JENNIFER DUNN, Washington
MAC COLLINS, Georgia
ROB PORTMAN, Ohio
PHILIP S. ENGLISH, Pennsylvania
WES WATKINS, Oklahoma
J.D. HAYWORTH, Arizona
JERRY WELLER, Illinois
KENNY HULSHOF, Missouri
SCOTT MCINNIS, Colorado
RON LEWIS, Kentucky
MARK FOLEY, Florida

CHARLES B. RANGEL, New York
FORTNEY PETE STARK, California
ROBERT T. MATSUI, California
WILLIAM J. COYNE, Pennsylvania
SANDER M. LEVIN, Michigan
BENJAMIN L. CARDIN, Maryland
JIM MCDERMOTT, Washington
GERALD D. KLECZKA, Wisconsin
JOHN LEWIS, Georgia
RICHARD E. NEAL, Massachusetts
MICHAEL R. MCNULTY, New York
WILLIAM J. JEFFERSON, Louisiana
JOHN S. TANNER, Tennessee
XAVIER BECERRA, California
KAREN L. THURMAN, Florida
LLOYD DOGGETT, Texas

A.L. SINGLETON, *Chief of Staff*
JANICE MAYS, *Minority Chief Counsel*

Pursuant to clause 2(e)(4) of Rule XI of the Rules of the House, public hearing records of the Committee on Ways and Means are also published in electronic form. **The printed hearing record remains the official version.** Because electronic submissions are used to prepare both printed and electronic versions of the hearing record, the process of converting between various electronic formats may introduce unintentional errors or omissions. Such occurrences are inherent in the current publication process and should diminish as the process is further refined.

CONTENTS

YEAR 2000 CONVERSION EFFORTS AND IMPLICATIONS FOR BENEFICIARIES AND TAXPAYERS

WEDNESDAY, FEBRUARY 24, 1999

HOUSE OF REPRESENTATIVES,
COMMITTEE ON WAYS AND MEANS,
Washington, DC.

The Committee met, pursuant to notice, at 9:06 a.m., in room 1100, Longworth House Office Building, Hon. Bill Archer (Chairman of the Committee) presiding.

[The advisories announcing the hearing follow:]

ADVISORY

FROM THE COMMITTEE ON WAYS AND MEANS

FOR IMMEDIATE RELEASE
January 21, 1999
No. FC–3

CONTACT: (202) 225–1721

Archer Announces Hearing on the Year 2000 Conversion Efforts and Implications for Beneficiaries and Taxpayers

Congressman Bill Archer (R–TX), Chairman of the Committee on Ways and Means, today announced that the Committee will hold a hearing on the Year 2000 or "Y2K" computer conversion efforts, remaining challenges, and implications for beneficiaries and taxpayers. The hearing will take place on Wednesday, February 24, 1999, in the main Committee hearing room, 1100 Longworth House Office Building, beginning at 10:00 a.m.

In view of the limited time available to hear witnesses, oral testimony at this hearing will be from invited witnesses only. Witnesses will include officials of the President's Council on Year 2000 Conversion; the Health Care Financing Administration; the Administration of Children and Families; the Social Security Administration (SSA); the Internal Revenue Service (IRS); the Financial Management Service (FMS); the U.S. Customs Service; and the Bureau of Alcohol, Tobacco, and Firearms. Witnesses will also include private sector organizations who represent program beneficiaries or taxpayers, as well as the U.S. General Accounting Office (GAO) and various Inspector Generals Offices. However, any individual or organization not scheduled for an oral appearance may submit a written statement for consideration by the Committee and for inclusion in the printed record of the hearing.

BACKGROUND:

The United States, with almost half the world's computer capacity and 60 percent of the world's Internet assets, is the most advanced, and the most dependent, producer and user of information technologies. Most computers, computer systems, and telecommunications networks in use in the Federal Government are currently undergoing modifications so that they will be able to continue to function properly in the year 2000 and beyond.

Most computers in use in the Federal Government have stored information for each year in a two-digit format, which makes the year 2000 indistinguishable from the year 1900. Unless they are changed, computer systems and telecommunications networks that are dependent on this two-digit year format can malfunction and cause costly problems for both commerce and government. Modifications have been underway for some time. Federal agencies, for the most part, are currently testing the renovated systems to make sure they will process transactions properly and produce accurate information. The agencies are also developing and testing contingency plans in the event of any failures.

Of particular concern for this hearing are the Federal programs within the jurisdiction of the Committee on Ways and Means, including those administered by the U.S. Departments of Treasury, and Health and Human Services, plus SSA. Among the major programs affected are tax and trade administration, Medicare, and Social Security. The computers serving the programs within the Committee's jurisdiction affect more than 260 million Americans. The revenue programs affect every individual and business taxpayer, and the benefit programs impact the health and well-being of millions. These Americans rely on the vital services they receive and cannot afford to have them disrupted by computer failures, nor can they afford to have the

computers produce erroneous penalty assessments or notices, or refund or benefit checks.

In response to Chairman Archer's request in the 105th Congress, the Subcommittee on Oversight held two hearings and issued a report to the Full Committee on August 19, 1998, on the implications of potential Y2K problems on program beneficiaries and taxpayers (WMCP: 105–10). The Subcommittee report concluded that, with the possible exception of SSA, which was found to be in a good position, services to taxpayers and beneficiaries may be disrupted or otherwise jeopardized by computer systems or telecommunications networks failures unless certain actions are taken by the Administration, Congress, and the private sector. The report made several recommendations to preclude Y2K-related failures, including comprehensive systems testing and contingency planning. Since the report's issuance, the Subcommittee has continued to monitor the agencies' Y2K progress, with the assistance of the GAO and Inspectors General Offices, and has seen considerable progress in the agencies' Y2K conversion efforts.

In announcing the hearing, Chairman Archer stated: "With more than 260 million Americans relying on vital services, we cannot afford to have disruptions because Y2K problems were not dealt with properly or expeditiously. The stakes are too high. We must get the job done, and done right."

FOCUS OF THE HEARING:

The hearing will explore the current status of Y2K renovation efforts, and the remaining challenges that agencies must overcome to ensure continuation of vital services provided through programs within the jurisdiction of the Committee on Ways and Means.

DETAILS FOR SUBMISSION OF WRITTEN COMMENTS:

Any person or organization wishing to submit a written statement for the printed record of the hearing should *submit six (6) single-spaced copies of their statement, along with an IBM compatible 3.5-inch diskette in WordPerfect 5.1 format, with their name, address, and hearing date noted on a label,* by the *close of business,* Wednesday, March 10, 1999, to A.L. Singleton, Chief of Staff, Committee on Ways and Means, U.S. House of Representatives, 1102 Longworth House Office Building, Washington, D.C. 20515. If those filing written statements wish to have their statements distributed to the press and interested public at the hearing, they may deliver 200 additional copies for this purpose to the Committee office, room 1102 Longworth House Office Building, by close of business the day before the hearing.

FORMATTING REQUIREMENTS:

Each statement presented for printing to the Committee by a witness, any written statement or exhibit submitted for the printed record or any written comments in response to a request for written comments must conform to the guidelines listed below. Any statement or exhibit not in compliance with these guidelines will not be printed, but will be maintained in the Committee files for review and use by the Committee.

1. All statements and any accompanying exhibits for printing must be submitted on an IBM compatible 3.5-diskette in WordPerfect 5.1 format, typed in single space and may not exceed a total of 10 pages including attachments. **Witnesses are advised that the Committee will rely on electronic submissions for printing the official hearing record.**

2. Copies of whole documents submitted as exhibit material will not be accepted for printing. Instead, exhibit material should be referenced and quoted or paraphrased. All exhibit material not meeting these specifications will be maintained in the Committee files for review and use by the Committee.

3. A witness appearing at a public hearing, or submitting a statement for the record of a public hearing, or submitting written comments in response to a published request for comments by the Committee, must include on his statement or submission a list of all clients, persons, or organizations on whose behalf the witness appears.

4. A supplemental sheet must accompany each statement listing the name, company address, telephone and fax numbers where the witness or the designated representative may be reached. This supplemental sheet will not be included in the printed record.

The above restrictions and limitations apply only to material being submitted for printing. Statements and exhibits or supplementary material submitted solely for distribution to the Members, the press, and the public during the course of a public hearing may be submitted in other forms.

Note: All Committee advisories and news releases are available on the World Wide Web at "HTTP://WWW.HOUSE.GOV/WAYS_MEANS/".

The Committee seeks to make its facilities accessible to persons with disabilities. If you are in need of special accommodations, please call 202–225–1721 or 202–226–3411 TTD/TTY in advance of the event (four business days notice is requested). Questions with regard to special accommodation needs in general (including availability of Committee materials in alternative formats) may be directed to the Committee as noted above.

NOTICE—CHANGE IN TIME

ADVISORY

FROM THE COMMITTEE ON WAYS AND MEANS

FOR IMMEDIATE RELEASE
January 28, 1999
No. FC–3–Revised

CONTACT: (202) 225–1721

Time Change for Full Committee Hearing on Wednesday, February 24, 1999, on the Year 2000 Conversion Efforts and Implications for Beneficiaries and Taxpayers

Congressman Bill Archer (R–TX), Chairman of the Committee on Ways and Means, today announced that the full Committee hearing on the Year 2000 computer conversion efforts, remaining challenges, and implications for beneficiaries and taxpayers, previously scheduled for Wednesday, February 24, 1999, at 10:00 a.m., in the main Committee hearing room, 1100 Longworth House Office Building, **will begin instead at 9:00 a.m.**

All other details for the hearing remain the same. (See full Committee press release No. FC–3, dated January 21, 1999.)

Chairman ARCHER. The Committee will come to order. Good morning. Is January 1, 2000, going to trigger a global economic recession as economist Edward Yardeni has predicted? Or is it much ado about nothing? Are the survivalists right in preparing for a major catastrophe? Or is the administration's John Koskinen right that we should just prepare as we normally would for a long holiday weekend?

We're here today for a public hearing on the year 2000 computer problem, commonly known as Y2K. I hope that we'll get informa-

tion to help us to answer these critical questions on how to prepare for the new millennium.

Today's hearing will help us all better understand Y2K and how it can impact our lives, and what we can do to protect our own interests. We'll discuss Y2K implications for beneficiaries and taxpayers if the problem is not fixed in time by Federal agencies and those who are involved in the delivery of vital program services.

After all, while Social Security authorizes retirement benefits for the elderly, Treasury actually makes the payments. The authorized payments are either delivered electronically through the Federal Reserve and into beneficiaries' commercial bank accounts or mailed through the Postal Service to beneficiaries' residences. For the elderly to continue to get their benefits in the year 2000 without disruption, the computer systems for the Social Security Administration, Treasury Department, Federal Reserve System, and commercial banks must all be Y2K-compliant and compatible with each other.

With only 310 days to complete the renovation efforts, we expect the agencies have already renovated their systems. We want to understand how they are progressing in the testing of the renovated systems. To do so may involve the actual trading of data or processing of transactions with other organizations like healthcare providers submission of Medicare claims to Health Care Financing Administration intermediaries for processing and payment.

Consequently, we are interested in what outreach efforts have been made by the agencies and what initiative has been taken by the trading partner to ensure Y2K compliance.

We also want to learn what the agencies are planning to do to prevent disruptions to those processes in the event of Y2K-related failures. The contingency plans should consider alternatives for doing business in the event key systems networks or infrastructures are not functioning or not operating property.

With many agencies receiving an increasing amount of information from beneficiaries, providers, taxpayers, or importers electronically, each agency and its corresponding data trading partner will need to have alternative ways to transmit the data in the event of the Y2K-related failure. The alternatives, like reverting to paper processing, need to be properly planned. Resources need to be considered and fully tested to be sure they will serve their intended purpose.

To ascertain how well the government is doing to prepare for Y2K, we have with us today a host of experts. Many work for the administration, many are nonpartisan authorities, and several come from the private sector. The Administration has received all the funding it has requested for Y2K. But I must say, if necessary additional funding is required, it's up to the agencies to inform the Congress so that we can adequately provide those resources.

We will do so, where they are justifiably needed, but we must be told. I look forward to learning how well our government is doing in meeting this challenge. With so little time remaining and so much at stake for 260 million Americans, we must work together to rise to the Y2K challenge and make sure that vital services are not disrupted.

Our first panel of witnesses today includes a gentleman who is no stranger to us after yesterday, Mr. Kenneth Apfel, Commissioner of the Social Security Administration; Hon. Richard L. Gregg, Commissioner for Financial Management Service; Scott Anderson, President and chief executive officer of Zions National Bank, Salt Lake City; Joel Willemssen, Director of Civil Agencies Information Systems, Accounting and Information Management for the U.S. General Accounting Office; Dennis Schindel, Assistant Inspector General for Audit, Office of Inspector General, U.S. Department of the Treasury.

And if you would all please come to the witness table, we will be pleased to get the information which you can give us this morning.

Mr. RANGEL. Mr. Chairman.

Chairman ARCHER. Yes, Mr. Rangel.

Mr. RANGEL. I just know how easy it is not to recognize me, but I just thought I would join in welcoming this panel and to——

Chairman ARCHER. It's almost impossible not to recognize you, Mr. Rangel.

Mr. RANGEL. Well, you know——

Chairman ARCHER. We missed you yesterday.

Mr. RANGEL. Yes, I was hoping you would. [Laughter.]

But I wanted to congratulate you for having the foresight to have these type of hearings, especially in focusing on the departments and agencies in which we have jurisdiction. I think that through this type of leadership, with all of the Committee, Chairmen and Ranking Members, together working with the private sector that we might allay some of the fears that we have in this country, indeed throughout the world.

I'm pleased that the Social Security Administration did lead in correcting the Y2K problems which they would have had in this area. And it's my understanding that some of the other agencies that had initial problems, the Health Care Finance Administration, have made dramatic progress since mid-1998. And so I merely wanted to be recognized to compliment you on your foresight, your vision, and your leadership.

Chairman ARCHER. Thank you. Thank you, Mr. Rangel. I would add also that we have attempted to get representatives from all of the various departments and agencies over which we have jurisdiction before us today. I hope we have not missed any.

[The opening statement of Mr. Ramstad follows:]

Opening Statement of Hon. Jim Ramstad, a Representative in Congress from the State of Minnesota

Mr. Chairman, thank you for convening this important hearing on the Year 2000 (Y2K) Problem.

The possible malfunction of the government's computer systems is a critical issue for all Americans. The magnitude of this potential problem is illustrated by the number of representatives we have here today. All of our constituents have a vested interest in how the different aspects of their government are working to avoid a potential disaster.

Some progress on solving the Year 2000 problem has been made. But with only 310 days until January 1, 2000 it is up to Congress to ensure that we are doing our part to help solve this problem. We need to ensure that the people we represent are not left without the health care and financial services upon which they depend.

I am pleased that this hearing will allow us to examine what the different agencies under our jurisdiction are doing to be prepared for the year 2000 and how they

are coordinating their efforts with the organizations in the private sector with which they work.

Again, Mr. Chairman, thank you for your own leadership in looking into the Year 2000 computer problem by holding this critical hearing.

Mr. Apfel, would you be good enough to lead off? We'll be pleased to receive your testimony.

STATEMENT OF HON. KENNETH S. APFEL, COMMISSIONER OF SOCIAL SECURITY

Mr. APFEL. Thank you, Mr. Chairman.

It's an honor to be back before this Committee, just 15 hours after leaving from my testimony yesterday, and to start off where I finished up last night.

Mr. Chairman, Social Security will be there in 2055. Social Security will be there in 2033. Social Security will be there in 2013. And the Social Security benefit payment will be there in January of the year 2000.

Chairman ARCHER. That is good to hear. [Laughter.]

Mr. APFEL. Thank you, Mr. Chairman.

My agency recognized early on the potential effects of the year 2000 problem and the critical importance of ensuring that our operations are unaffected. The Social Security Administration relies on a vast computer network to keep track of earnings for the 145 million workers, to pay monthly benefits to more than 50 million individuals, and to process 6 million new benefit applications each year.

Because so many Americans depend on our systems operations, we began to take remedial action on the year 2000 problem as soon as we recognized it. For the past several years, we've had some of our top people at work on this issue.

I should point out Dean Mesterharm, 10 years ago, recognized this. He's now our Deputy Commissioner for Systems. Kathy Adams, Dean's Deputy, sitting behind me, has been heavily involved with the endeavors over the years, and has done a remarkable job.

The magnitude of the task that we face cannot be overstated. We had to review systems supported by more than 35 millionlines of in-house computer code as well as vendor products. We had to coordinate all of our efforts with other Federal and State agencies, and with third-party organizations.

But the work has borne results. Today, SSA's benefit system is 100 percent year 2000 compliant. Of course, ensuring delivery of benefit payments in January 2000 and beyond also means that our agency has had to work closely with our partners, who help produce and deliver benefit payments: the Treasury Department, the Federal Reserve, and the U.S. Postal Service.

And since last October, all Social Security and SSI payments have been made through year 2000 compliant systems at both SSA and the Treasury Department. The Federal Reserve is testing payment operations with banking institutions throughout the country, and Social Security transactions have been included in the materials tested.

We have also made strong progress in making non-benefit payment systems Y2K compliant. For example, all 50 State Disability Determination Service systems operations, which support the DDS process, are now Y2K compliant.

More than 99 percent of our data exchanges have been made Y2K compliant. We've begun testing our facilities infrastructure for Y2K compliance.

Let me now turn briefly to the issues of Y2K contingency planning in our program of ongoing monitoring for continued systems compliance. Our business continuity and contingency plan addresses a wide range of eventualities. If a benefit-payment-system problem should occur in January 2000, SSA field offices would provide emergency payment services to beneficiaries with critical needs. And the Treasury Department will issue a replacement check.

It is also important to note that every one of the 1,300 field offices across the country, as well as each State DDS unit, has its own contingency plan for continued business operations, if there are any service disruptions.

The agency's contingency plan also addresses such needs as telecommunications, building operations, and human resources. This plan conforms with the GAO guidelines and, in fact, has been used as the model by both other Government agencies and private-sector organizations.

I would like to cite one other key element of this plan, which we call our day-one strategy. It goes into effect during the rollover weekend of December 31 through January 3 and provides a timeline for tracking critical benefit-related events and ensures that key staff will be available throughout the rollover period.

Now that all of our mission-critical systems are year-2000 compliant, we have taken steps to make sure that we do nothing to introduce possible date defects into these systems. Since we must continue to modify these systems to accommodate regulations, recent legislation, and other required changes, such as the COLA announcement and the actual COLA increase, we have set up an ongoing recertification process.

In addition, as a further safeguard, a moratorium for discretionary changes to our software will be put in place in September 1999. And that moratorium will remain in effect through March 2000.

In conclusion, let me say that I'm proud of the fact that my agency has been at the forefront of Government and private-sector organizations addressing year-2000 issues. I'm confident our systems are ready for this new challenge of the new millennium.

When our offices open on January 3, 2000, we will be prepared to provide full service to the American public with the accuracy and reliability that they have come to expect from the Social Security Administration.

Thank you, Mr. Chairman.

[The prepared statement follows:]

Statement of Hon. Kenneth S. Apfel, Commissioner of Social Security

Mr. Chairman and Members of the Committee: Thank you for inviting me to be here today to discuss the Social Security Administration's (SSA) Year 2000 conversion efforts and the implications for beneficiaries and taxpayers. SSA recognized very early the potential effect on beneficiaries and workers created by the Year 2000

problem. I am pleased to be here today to report on our progress and plans for the future.

IMPACT ON SSA OPERATIONS

SSA relies on a vast computer network to keep track of earnings for 145 million workers, take six million applications for benefits a year, and pay monthly benefits to over 50 million beneficiaries. Because so many people depend on SSA's systems, we began to work on the Year 2000 problem as soon as it was identified in 1989. The magnitude of this project cannot be overstated: we had to review systems supported by more than 35 million lines of in-house computer code, as well as vendor products, while coordinating efforts with State and Federal agencies and third parties.

SSA's ability to provide world class service to beneficiaries, workers and their families depend on a complex infrastructure that is crucial to our ongoing operations. Power, data, and voice telecommunications, along with the Agency's computer operations hardware and software, are essential to ensuring that SSA's business processes are able to continue uninterrupted. Our automated systems are the means by which SSA is able to provide service on demand to the public.

SSA has five core business processes through which we maintain the accuracy of beneficiary records and process and adjudicate claims:

1. Enumeration, the process through which SSA assigns Social Security numbers;
2. Earnings, the process which establishes and maintains a record of an individual's earnings;
3. Claims, the process comprising actions taken by SSA to determine an individual's eligibility for benefits;
4. Postentitlement, the process involving actions that SSA takes after an individual becomes entitled to benefits; and
5. Informing the Public, the process by which we disseminate information about the programs we administer.

I am confident that our systems will function on and after the Year 2000 to ensure that our core business processes proceed smoothly and without disruption as we move into the 21st century. When we open our offices for business on January 3, 2000, we expect to be prepared to provide our full complement of services to the American public with the accuracy and reliability that they have come to expect from SSA.

JANUARY 2000 BENEFIT PAYMENTS

We are happy to report that our benefit payment system is 100 percent Year 2000 compliant. SSA has worked very closely with the Treasury Department, Federal Reserve and the Post Office to ensure that Social Security and Supplemental Security Income checks and direct deposit payments for January 2000 will be paid on time. Since October 1998, payments for both Social Security and Supplemental Security Income programs have been made with Year 2000 compliant systems at both SSA and Treasury.

SSA is working closely with the Treasury Department and the Federal Reserve to identify any Year 2000 problem that might affect direct deposit payments. If a problem should occur in January 2000, the Treasury Department will quickly issue a replacement check after recertification by SSA, and SSA offices will provide emergency payment services to beneficiaries with critical needs.

I do not consider Social Security's job to be done until timely and correct benefits are in the hands of all of our beneficiaries.

STATUS OF SSA'S YEAR 2000 IMPLEMENTATION EFFORTS

I would like to discuss the status of SSA's progress in our Year 2000 implementation efforts.

All of our mission critical systems have been made Year 2000 compliant. These are the systems that support the core business processes I described earlier.

Because they are so vital to our disability claims process, SSA is overseeing and managing the effort of assuring Year 2000 compliance of State Disability Determination Service (DDS) systems. Fifty State DDSs have automated systems to support the disability determination process. As of January 31, 1999, all 50 DDS automated systems are Year 2000 compliant and are being used to process disability claims.

We recognize that it is not enough for our agency to be Year 2000 compliant if all our trading partners are not ready. Therefore SSA has worked with all of our

trading partners, and I am pleased to say that 99 percent of our data exchanges are Year 2000 complaint. We are working with our partners to test the remaining 1 percent and get them implemented as quickly as possible.

SSA has inventoried all of our telecommunications systems and we have a plan and schedule for all fixes and upgrades. Numerous acquisitions have been made that will result in the installation of telecommunications software and hardware upgrades. SSA is also working with the General Services Administration (GSA) in this effort, particularly with regard to testing vendor fixes. SSA's goal is to have all telecommunications compliant by the end of March 1999.

SSA continues to work with GSA in addressing the Year 2000 problem in the areas of our facilities infrastructure. We have inventoried our building systems and testing contracts have been awarded. Testing has commenced in some buildings, with all sites progressing as scheduled.

Our independent verification and validation contractor, Lockheed Martin, completed a comprehensive review of SSA's Year 2000 program and submitted their finding in October 1998. Their report covered all aspects of Year 2000 preparedness activities and found our Year 2000 methodology to be sound and feasible.

FOCUS OF ACTIVITIES IN 1999

Now that all of our mission critical systems are Year 2000 compliant, we have taken steps to make sure we do nothing to introduce possible date defects into these systems. Since we must continue to modify these systems to accommodate regulations, recent legislation, and other required changes, we have instituted a re-certification process that uses a commercial computer software tool. In addition we have instituted a moratorium beginning in July 1999 on the installation of commercial off-the-shelf software and mainframe products. A similar moratorium is in place for discretionary changes to our software beginning in September 1999. The moratoriums will remain in effect through March 2000.

BUSINESS CONTINUITY AND CONTINGENCY PLAN

Obviously, we all hope that there will be no need for backup or contingency plans. However, SSA recognizes that our systems are dependent on infrastructure services, such as the power grid of the telecommunications industry and third parties, which are beyond our control. Therefore, SSA has developed a Business Continuity and Contingency Plan. The plan was first issued March 31, 1998 and it is updated quarterly. The plan is consistent with Government Accounting Office guidelines and is being used as a model by other agencies and private sector organizations.

The plan identifies potential risks to business processes, ways to mitigate each risk and strategies for ensuring continuity of operations if systems fail to operate as intended. The SSA Business Continuity and Contingency Plan addresses all core processes, including disability claims processing functions supported by the DDSs.

As part of our Business Continuity and Contingency Plan, we have in place local plans for each of our field offices, teleservice centers, and processing centers, hearing offices and state DDSs. We have also developed contingency plans for benefit payment and delivery, building operations, human resources, and communications. Our benefit payment and delivery plan was developed in conjunction with the Treasury Department and the Federal Reserve.

CONCLUSION

I would like to conclude by repeating that SSA was at the forefront of Government and private organizations in addressing Year 2000 issues. We are proud of our longstanding reputation as a leader when it comes to providing customer service, and we are confident that we will be prepared to continue that tradition when the new millennium arrives.

I will be happy to answer any questions you may have.

Chairman ARCHER. Thank you, Mr. Apfel, and thank you, also, for precisely complying with the 5-minute time suggestion. And I would alert all other witnesses that we hope you can get your verbal comments to us within 5 minutes and your entire printed statement, without objection, will be inserted in the record. And

any Member of the Committee who wished to insert a written statement into the record, without objection, may do so.

Our next witness is Mr. Richard Gregg, Commissioner of Financial Management Service. Mr. Gregg.

STATEMENT OF RICHARD L. GREGG, COMMISSIONER, FINANCIAL MANAGEMENT SERVICE

Mr. GREGG. Thank you, Mr. Chairman, Representative Rangel, Members of the Committee. Thank you for the opportunity to appear today to discuss the Financial Management Services year 2000 program.

FMS makes payments to well over 100 million Americans each year. We provide facilities and systems for the collection of taxes and other receipts, and provides governmentwide accounting and reporting and debt-collection services for the entire Federal Government.

To provide these services, FMS depends on automated systems. And like most Federal agencies, FMS faces the challenges of adapting its systems to account for the date change to the year 2000. Correcting this problem has been and will continue to be our highest priority.

FMS has made significant progress in addressing the year-2000 problem. The systems that issue over 740-million Government payments, 86 percent of FMS's total payments, are year-2000 ready. The system that collected $1.1 trillion in Federal revenues in Fiscal 1998, is also Y2K ready. And compliance of all remaining FMS critical systems is on schedule for completion by or before March 1999.

I want to assure you that FMS will continue to perform its critical functions in making payments and collecting revenues for the government on January 1, in 2000 and thereafter.

I'd like to now provide a brief update of the current status of our largest and most critical systems. The vast majority of payments made by FMS are Old-Age and Survivors benefits and Supplemental Security Income payments issued on behalf of Social Security. These payments account for over 600-million payments annually, which comprise 70 percent of FMS's payment volume. Our average monthly payment volume is 42-million SSA payments and 6.5-million SSI payments, with a total value of approximately $30 billion.

Since October 1998, SSA and SSI payments have been issued through year-2000 compliant systems.

The FMS systems used to issue 27 million annual EFT payments on behalf of VA, for Veterans Compensation and Pension, and 10 million annual payments on behalf of the Railroad Retirement Board were implemented in December 1998. And the systems that issue the remaining 13 million VA payments will be implemented in or before March 1999.

IRS payments account for over 10 percent of FMS's overall payment volume, with approximately 90 million tax-refund payments each year. Implementation of these systems was completed in July 1998 and all tax-refund payments since that time have been issued through Y2K-ready systems.

The FMS systems used to issue 50 million annual EFT Federal agency salary and travel and vendor payments began implementa-

tion in January with customers serviced by our Kansas City Regional Finance Center. These same systems are now being implemented for customers serviced by our four other payment centers.

And finally, the system that issues 28 million annual OPM annuity payments is finishing validation and certification testing and is scheduled for implementation in March.

The systems that I've just mentioned comprise 97 percent of FMS's payment volume.

With respect to collections, FMS manages the processing of more than $2 trillion in Federal revenues, which include corporate and individual income taxes, customs duties, and Federal fines. The Electronic Federal Tax Payment System, (EFTPS), through which FMS collected $1.1 trillion, or 56 percent of the government's total collections, and 67 percent of total tax collections, was determined to be compliant in December.

The IRS Lockbox, General Lockbox, Plastic Card and other collection systems that account for the remaining 44 percent in Federal Government revenue are targeted for implementation in March 1999.

And FMS debt-collection systems, including the Treasury Offset Program, through which Federal payments to delinquent debtors are offset, are now Y2K compliant.

With regard to government-wide accounting, FMS maintains the central accounting and reporting systems that track the Government's monetary assets and liabilities. Both the STAR central accounting system and the Government On-Line Accounting Link System, GOALS, which serves as the automated telecommunication link for all Federal program agencies to report their accounting and financial transactions for processing into the STAR Central Accounting System, will be Y2K-ready in March 1999. In fact, 13 of the 16 critical GOALS subsystems are now Y2K-compliant.

The information with regard to the Inspector General's report was provided in my formal statement, so I won't go over that at this time.

I would like to just briefly mention our contingency planning, which was also discussed by the Inspector General. FMS has successfully completed contingency plans for all FMS critical systems and non-mission critical systems. Of the contingency plans for FMS internally operated systems, 87 percent are final, meaning that they have been revised and approved after review by an outside contractor. The remaining plans are under review by the contractor to assure that they are comprehensive and address all pertinent risks.

FMS has set its priorities and is integrating system contingency plans with business priorities to make sure the most critical business functions will continue uninterrupted if problems occur. On top of the list are key systems such as Social Security, Supplemental Security and Veterans Affairs payment systems.

Specific risks have been identified and strategies developed to mitigate those risks. For example, we are configuring our systems so payments can be processed in more than one computer center. This will enable FMS to rotate the workload should any Y2K disruptions occur in one area of the country or in one computer center.

In addition, an emergency power generator has been installed to support our largest computer center in case of power outages, and system redundancy has been built into the nationwide network so that alternative routing can be used if there are data-communication problems. We are also working very closely with the Federal Reserve to develop integrated business resumption plans and risk mitigation strategies.

In conclusion, FMS considers preparation for the year 2000 as our absolute highest priority, ensuring that we are able to perform our mission in the year 2000. We will assign whatever resources are needed to ensure we do not fail to accomplish necessary Y2K changes to our computer systems.

Thank you for the opportunity to appear this morning.

[The prepared statement follows:]

Statement of Richard L. Gregg, Commissioner, Financial Management Service

Chairman Archer, Representative Rangel and members of the Committee, thank you for the opportunity to appear today to discuss the Financial Management Service's (FMS) Year 2000 (Y2K) program.

FMS provides payment, collection, government-wide accounting and reporting, and debt collection services to most federal agencies, to individuals who receive money from the government, and to every individual who pays a bill owed to the government. Our services benefit federal agencies, government policymakers, and the taxpayers by promoting efficient financial management practices and facilitating the timeliness and accuracy of payment and collection processes. Additionally, our services allow the Treasury to administer prudent financial management policies, and facilitate centralized management and oversight of delinquent federal non-tax debt collection efforts.

To provide these services, FMS depends on automated systems. Like most federal agencies, FMS faces the challenge of adapting its systems to account for the date change to the Year 2000. Correcting this problem has been and will continue to be our highest priority.

In 1997, FMS began working to make its systems Y2K compliant, completing a full assessment and prioritizing work according to the magnitude of impact on the public, particularly payment recipients. These systems progressed from renovation, in which the code changes are made, through the validation phase, in which renovated systems with Y2K code modifications are tested, into full implementation, in which the renovated and validated systems are put into production. Following implementation, the systems are certified Y2K compliant. For our highest priority internal systems, such as Social Security Administration and Veterans benefit payments, certification occurs only after an independent contractor verifies Y2K compliance by analyzing all test results to ensure that validation testing was successful and comprehensive. If re-testing is necessary, the contractor will provide specific guidance on the necessary steps to correct identified problems and achieve successful validation testing and certification. Post implementation reviews will be conducted throughout this year to further ensure compliance. For our external collection systems, the financial and fiscal agents are self-certifying based on the Federal Financial Institutions Examination Council's guidance.

FMS has made significant progress in addressing the Year 2000 problem. The systems that issue more than 740 million government payments, 86 percent of FMS' total payment volume, are Year 2000 ready. The system that collected $1.1 trillion in federal revenue in FY 1998 is also Y2K ready. Compliance of all remaining FMS critical systems is on schedule for completion by or before March 1999, and FMS will continue to perform its critical functions in making payments and collecting revenues for the federal government on January 1, 2000, and after.

I'd like to now provide a brief update on the current status of our largest and most critical systems. The vast majority of payments made by FMS are Old Age and Survivor Benefits and Supplemental Security Income payments issued on behalf of SSA. These payments account for more than 600 million payments annually, which comprise 70 percent of FMS' payment volume. Our average monthly payment volume is over 42 million (30 million EFT) SSA payments and 6.5 million (3 million EFT) SSI payments with a total value of approximately $30 billion. Since October

1998, SSA and SSI payments have been issued through Year 2000 compliant systems.

The FMS systems used to issue 27 million annual EFT payments on behalf of the VA for Veterans' compensation and pension, and 10 million annual payments on behalf of the RRB were implemented Y2K compliant in December 1998. The systems that issue the remaining 13 million VA payments will be implemented Y2K compliant in or before March 1999. IRS payments account for over 10 percent of FMS' overall payment volume, with approximately 90 million tax refund payments made each year. Y2K implementation of these systems was completed in July 1998, and all tax refund payments since that time have been issued through the Y2K compliant system.

The FMS systems used to issue nearly 50 million annual EFT Federal Agency salary, travel, and vendor payments began implementation in January with customers serviced by our Kansas City Regional Finance Center. These same systems are now being implemented for customers serviced by our other four payment centers. And, finally, the system that issues more than 28 million annual OPM annuity payments is finishing validation and certification testing and is scheduled for implementation in March 1999. The seven systems that I have just described comprise 97 percent of FMS' payment volume.

With respect to collections, FMS manages the processing of more than $2.0 trillion in federal revenues, which include corporate and individual income taxes, customs duties, and federal fines. The Electronic Federal Tax Payment System (EFTPS) through which FMS collected $1.1 trillion or 56 percent of the government's total collections and 67 percent of total tax collections was determined to be compliant in December. The IRS Lockbox, General Lockbox, Plastic Card and other collection systems that account for the remaining 44 percent in federal government revenue are targeted for implementation in or before March 1999. FMS debt collection systems, including the Treasury Offset Program through which federal payments to delinquent debtors are offset, are also now Y2K compliant.

With regard to government-wide accounting, FMS maintains the central accounting and reporting systems that track the government's monetary assets and liabilities. Both the STAR central accounting system and the Government On-Line Accounting Link System (GOALS), which serves as the automated telecommunications connection for all federal program agencies to report their accounting and financial transactions for processing into the STAR Central Accounting System, will be Y2K ready by March 1999. In fact, 13 of the 16 critical GOALS subsystems are already Y2K compliant.

I would now like to address the issues raised by Treasury's Inspector General based on their audit work from May to September 1998. Their report has recommended steps to reduce risk and, in all cases, we are implementing those recommendations. We have strengthened project management; improved testing and data exchange strategies; and put increased emphasis on the development and testing of comprehensive contingency and continuity of operations plans. With regard to their recommendations on compiling more extensive supporting documentation, we believe this is critical and this work will be completed this spring. I believe, however, that it is important to keep the Y2K issue in perspective. Our overriding concern is making sure that federal benefit payments go out uninterrupted. Sometimes making a critical business decision to ensure system readiness means postponing work in other areas such as documentation. This is not to say we find fault with the Inspector General's recommendation. I'm just underscoring the need to balance planning and documentation with system readiness. It's also important to note that the work associated with the Treasury Inspector General's report occurred in late spring and summer 1998 and does not reflect the progress FMS has made during the past five months in ensuring its systems are Y2K compliant.

For example, several initiatives are underway to ensure that all data exchanges between FMS and our trading partners will occur smoothly on January 1, 2000, and beyond. We are finalizing memoranda of understanding (MOU) with federal program agencies to clearly identify all interfacing systems and to indicate which ones are retaining existing formats and which ones are changing formats. For our largest partners such as VA and SSA, we have already agreed to these formats either through MOUs or face-to-face meetings. We are also stepping up our efforts to ensure good communication with our customers. As part of this effort, FMS sponsored a meeting on December 8, 1998, which brought together more than 100 key officials from more than 40 federal agencies to exchange information about testing and compliance issues. We will sponsor another, similar session this spring. In addition, we are continuing to send information to our trading partners on file formats, testing and system status. FMS sent letters in December 1997 and August 1998 to all federal program agencies interfacing with GOALS to indicate that formats were not

changing and to identify agencies interested in joint testing of that system. In addition, our Regional Finance Centers sent letters to their customers last summer indicating that FMS is not changing agency input formats for salary, vendor and miscellaneous payments. We are now following up to determine which agencies are interested in specific interface testing and when they anticipate being ready.

FMS has also successfully completed contingency plans for all mission critical systems (43 internal; 15 external; 4 retired) and non-mission critical systems (17 internal, 1 external). Of the contingency plans for FMS internally operated systems, 87 percent are final—meaning that they have been revised and approved after review by an outside contractor. The remaining plans are under review by the contractor to ensure they are comprehensive and address all pertinent risks. FMS has set its priorities and is integrating system contingency plans with business priorities to make sure the most critical business functions will continue uninterrupted if problems occur. On top of the list are key systems such as the Social Security, Supplemental Security and Veterans Affairs payment systems. Specific risks have been identified and strategies developed to mitigate those risks. For example, we are configuring our systems so payments can be processed in more than one computer center. This will enable FMS to rotate the workload should any Y2K disruptions occur in one area of the country, or in one computer center. In addition, an emergency power generator has been installed to support our largest computer center in case of power outages and system redundancy has been built into the nationwide network so that alternative routing can be used if there are data communications problems. We are also working closely with the Federal Reserve to develop integrated business resumption plans and risk mitigation strategies.

FMS considers preparation for the Year 2000 as our absolute highest priority, ensuring our ability to maintain current operations. We will assign whatever resources are needed to ensure we do not fail to accomplish these changes to our computer systems. Thank you for the opportunity to discuss FMS' plans to complete the work necessary to enable us to meet the year 2000 challenge. I would be happy to answer any questions you may have regarding this issue.

Chairman ARCHER. Thank you, Mr. Gregg. Our next witness is Mr. Anderson, chief executive officer of Zions National Bank, Salt Lake City. And I believe you are representing the American Bankers Association. Is that correct?

Mr. ANDERSON. I am, Mr. Chairman.

Chairman ARCHER. All right. Welcome, Mr. Anderson, you may proceed.

STATEMENT OF A. SCOTT ANDERSON, PRESIDENT AND CHIEF EXECUTIVE OFFICER, ZIONS FIRST NATIONAL BANK, SALT LAKE CITY, UTAH, AND MEMBER, COMMUNICATIONS COUNCIL, AMERICAN BANKERS ASSOCIATION

Mr. ANDERSON. Thank you. Mr. Chairman and Members of the Committee, I'm pleased to be here today to discuss how the banking industry is addressing the Y2K problem. We believe we are on track to meet the many challenges we face.

For my bank, Y2K is the single, most critical issue that we have. And this has been communicated to everyone in our organization, from the tellers to senior management, from our board of directors to shareholders. Nothing at our bank has higher priority, is receiving greater scrutiny or more resources than this important project.

Bankers realized early on though that Y2K is not just a technology issue. Equally important are the business and communication challenges that go along with it. My industry has spent billions of dollars and thousands of man hours to make sure that our systems will work and that our customers will be properly cared for.

At Zions Bank we have two distinct groups working on the Y2K problem. The first is our in-house computer experts, who have completed renovation and are now testing systems, interfaces and end-to-end processes. The other group is businessmanagers who are involved with business-resumption planning, resource allocation, assignment of employee resources, and contingency plans.

One of our greatest challenges is identifying and then addressing all the vendors, suppliers and other businesses that touch us from the outside on a daily basis. Ongoing communication and monitoring of these partners is critical to the success of our Y2K effort.

At Zions, we have an extensive Y2K contingency plan. I brought a copy of the plan for our overall organization. Each of our 200 units have similar plans that look at each detail, that if there is a glitch, what would we do so that we could continue to provide service to our customers. These documents cover such things as immediate responses, command control centers, backup facilities, information centers, and detailed business recovery and resumption plans. We even cover how we will feed our employees.

No one, including me, will be on vacation from Christmas through January 15, 2000. Hopefully, no one will be needed, but everyone will be on-call.

As you know, Mr. Chairman, the banking industry is highly regulated, and bank supervisors have been conducting onsite examinations in every bank and at all key vendors providing data and services to the banking industry. The results of these examinations are very positive. Ninety-seven percent of the banking industry received the highest grade. Only 17 institutions out of over 10,000 received unsatisfactory ratings. Outside vendors ranked high as well.

Being prepared, though, is more than just a banking issue. Success depends on all sectors of the economy, including energy, telecommunications, transportation, and utilities, pulling together to keep the fabric of our community and our economy strong and trustworthy.

Bankers have reached out to these other industries and to our customers to ensure that we will all come through this project and this challenge together, intact, and successful.

The banking industry is confident that it can deliver on time. But the biggest unknown to us and the greatest fear that we have is the public perception and reaction throughout the rest of the year.

The problems created by adverse public reaction or panic could be far worse than actual problems. All of us must join forces to stabilize public opinion and manage expectations.

In focus groups that the ABA has conducted, we found some very interesting things. For example, many consumers didn't know that the Federal regulators were examining banks. This was good news to them. It was good news to them that the Federal Reserve is printing billions of extra dollars. It was also good news to them that bank deposits are insured for $100,000 by the FDIC.

We must be aggressive to dispense these facts, and to dispel fiction. We are concerned, for example, that some groups are advising consumers to withdraw large amounts of cash just to be safe. In fact, it was reported on one news show that a couple took out

$20,000 from their bank and buried it in the backyard, only to have it stolen 2 days later.

The safe side? Hardly.

We use this as an example to our senior citizens to help them make good decisions. The fact is, the safest place for your money is in the bank. These checks that we have are Y2K-compliant. They can be used anywhere. This credit card, with an expiration date of 2001, is Y2K compliant. It can be used anywhere.

The ABA has produced a variety of videos, newsletters, manuals, seminars, and, at Zions, we recently created and had a seminar, which I've given you a transcript of, where we had Senator Bennett come and speak with some representatives from the legal and accounting industries to get out the word concerning what people need to do to be prepared for the Y2K issue.

In closing, Mr. Chairman, let me say that Congress, government, and the regulators have a special role to play disseminating accurate information. Last year's bill helped to encourage information sharing, but must and needs to be done. We urge Congress to enact broader Y2K liability laws, and we pledge to work with toward that goal.

Last year, Zions Bank celebrated its 125th year of servicing the people of Utah and the intermountain West. One hundred years ago, we were making plans for a new century, and we're doing that again today. And we are sure that we will be successful.

Thank you.

[The prepared statement follows:]

Statement of A. Scott Anderson, President and Chief Executive Officer, Zions First National Bank, Salt Lake City, Utah, and Member, Communications Council, American Bankers Association

Mr. Chairman, I am Scott Anderson, President and CEO of Zions First National Bank, Salt Lake City, Utah, and a member of the Communications Council of the American Bankers Association (ABA). The ABA brings together all categories of banking institutions to best represent the interests of this rapidly changing industry. Its membership—which includes community, regional and money center banks and holding companies, as well as savings associations, trust companies and savings banks—makes ABA the largest banking trade association in the country.

I am pleased to be here today to discuss what the banking industry is doing to address the Year 2000 computer problem (Y2K). These hearings are very important because information about the Y2K problem—and what the government and industry are doing to meet this challenge—is critical to maintaining confidence in our economy.

Y2K is really two problems. The first is technology—making sure that software and hardware systems will work on January 1, 2000 and beyond. The second is communication—making sure the public is knowledgeable about the problem and what is being done to solve it. Even if the technical problems are fully resolved, people need to know about it. If nothing is said, the information void will surely be filled with misleading and provocative stories that will create undue anxiety, and lead to bad decisions. The problems created by adverse public reaction or panic could be far worse than the actual problem. The news media, government, private industry, bankers, and all other stakeholders must join forces to stabilize the public opinion, and manage expectations.

The banking industry is working hard at solving both aspects of the Y2K problem. Since 1995, the banking industry has devoted millions of man-hours and billions of dollars to addressing Y2K. The banking industry is well into the testing period for all critical systems, working closely the Federal Reserve and other federal bank regulators. Our progress is right on track. The ABA and individual banks have also done a tremendous amount of work to keep our customers informed about our progress. We believe this communications effort is right on track, too.

At Zions Bank, Y2K has been identified as the single most critical project to be completed this year. Its criticality has been communicated through Senior Manage-

ment, right down to every employee and business manager. Nothing at our bank has higher priority or greater scrutiny than this important project.

At Zions Bank our efforts have been very successful to this point. We are confident in our ability to successfully deliver this project on time. Many of the processing systems have been replaced in the past five years with up-to-date Y2K compliant systems. Most of our core processing systems are supplied by outside vendors and have been remediated by them for Y2K compliance. Each business unity of Zions Bank has a Y2K operational plan specific to their unit, and each has prepared a business resumption plan to cover any contingencies that might arise. We also have detailed plans for both internal and external communications to keep bank personnel, customers, and the media informed about what we are doing before, during and after January 2000.

The banking industry is unique in that it has extensive levels of federal and state regulation and examination. We have worked closely with bank regulators to address all aspects of the Y2K issue. The results of the Y2K compliance examinations have been very positive. We believe it would be very helpful for the bank regulators to discuss publicly the industry's readiness for Y2K.

There are three key messages that I would like to leave with the Committee today:

- The banking industry is on track meeting critical deadlines;
- Educating our customers and the public generally is vital; and
- The safest place for customers' money is in the bank.

Mr. Chairman, before turning to these points, I want to take a moment to focus on why these issues are so important to the banking industry. We take our role in the economy and in each community we serve very seriously. Our business is built on the trust established with our customers over many decades. Maintaining that trust is no small matter to us. When customers put money in my bank, I want them to feel that their funds are secure, accessible when they need them, and financial transactions will be completed as expected. It is, therefore, no surprise that we in the banking industry believe much is at stake in addressing the Y2K problem.

On a larger scale, our national economy relies on a smoothly functioning payment system. It's something we all take for granted today because our payment system is so efficient, accurate and easy to use. Assuring this high level of performance requires the collective efforts of many participants: banks, thrifts, brokerage firms, regional clearinghouses, and the Federal Reserve.

Careful planning, correcting and testing is crucial to minimize any disruptions from the century date change. But we must be realistic: it is inevitable that some glitches will occur. Contingency planning, therefore, must be an integral part of the process. In the case of the banking industry, our contingency plans are examined by the bank regulators. We intend to be as prepared as is possible for any eventuality.

Preparedness, however, goes well beyond the banking and financial sector. The tightly woven fabric of our economy means that businesses, households and government must work together. Success depends upon the efforts of all sectors of the economy, including energy, telecommunications, transportation, public utilities, retail services, etc. Bankers have reached out to other industries, as well as our customers, to ensure that we all come through this challenge intact and together.

I. Technology: The Banking Industry is on Track Meeting Critical Deadlines

Many banks began their Y2K risk assessment efforts as early as 1995. The cost of assessing, correcting, testing and contingency planning will easily exceed $9 billion. The goal of this massive commitment of effort and resources is to provide a smooth transition of banking and financial services into the 21st century with minimal disruptions.

The Y2K strategy involves awareness, assessment, renovation, validation and implementation. Key components of these broad strategic areas include the assessing of business risks, conducting due diligence on service providers and software vendors, analyzing the impact on customers, and assuring customer awareness of progress in addressing Y2K concerns.

Zions Bank has two distinct groups attacking the Y2K problem. The first is our in-house staff of computer experts who have completed renovation, and are now testing systems, interfaces, and end-to-end processes. The other group is business managers and owners that are actively managing the business side of the issue. This includes such issues as vendor management, business resumption planning, resource allocation, assignment of employee resources, and contingency plans.

One of the greatest challenges to business managers is identifying and then addressing the vast number of outside touch-points to a business unit. These include

vendors, suppliers, service providers, and a host of other businesses that touch us from outside on a daily basis. Ongoing communication and monitoring of these partners is critical to the success of the Y2K effort.

Regulatory Oversight

The banking industry is unique in that it is a highly regulated industry at both the state and federal level. Since 1997, the banking industry has worked with the regulators in assessing the extent of the Y2K problem and developing a 3-phase plan of attack.[1] During phase one, completed June 30, 1998, federal bank supervisors conducted on-site examinations of every depository institution and rated them on their remediation plans and written testing strategies. Regulators also conducted on-site examinations of firms providing data processing and system services.

During phase two, supervisors are examining banks for how well the testing of critical systems is progressing and on contingency plan development. This is critical as it measures the success of the remediation efforts. For banks with their own internal systems, testing was to be completed by the end of last year. By March 31, 1999, banks relying on outside service providers should have testing completed. All institutions should also have initiated external testing with customers, other banks and payment system providers.

The results of on-site, phase one and phase two examinations show that the banking industry is right on track meeting its goals. As of December 31, 1998, 97 percent of the industry held the highest rating and only 17 institutions—out of more than 10,000 banks and thrifts—received unsatisfactory ratings. These poorly rated institutions are being closely monitored by the regulatory agencies.

Phase three includes final testing of internal and third-party systems and testing with the Federal Reserve and clearing systems participants. Phase three will run from April 1 through December 31, 1999, with a critical deadline of June 30 for completion of testing validation and implementation of remediated systems. After June 30, institutions will continue to monitor and update contingency plans as may be required by external developments, and monitor customer and counterparty risk. Agency examiners will continue to check on bank testing implementation and contingency plans, and, where needed, with continued on-site reviews.

Testing with the Federal Reserve and clearing system participants is very important. Starting last summer, the Fed established dedicated times for banks to test the operability of systems for Y2K compliance. Systems tested included Federal Funds Transfer, Fed Automated Clearinghouse (ACH) transactions, checks and all other payment systems. Additional testing opportunities are being made available through 1999. As part of this procedure, banks will test, among other systems, direct deposit services—including payroll, Social Security electronic payments, Medicare payments, and other electronic payments—and tax information reporting systems.

Further, we are informed, the Federal Reserve has been testing directly over the last several months with the Social Security Administration.

Credit card systems have already been tested for Y2K compliance and adjustments to software and hardware have been made. Many cards in use today have expiration dates in the year 2000 or beyond. Systems needed to be ready to recognize these cards as valid when they were issued last year. I am happy to report that the transition was made so smoothly and with so few problems that the public was largely unaware that any changes had been made.

---

[1] The Federal Reserve, the Office of the Comptroller of the Currency (which regulates national banks), the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, and the National Credit Union Administration work jointly on key regulatory and supervisory issues through what is known as the Federal Financial Institutions Examination Council, or FFIEC. Through this cooperative regulatory effort, the FFIEC has played an important role in promoting Y2K education and communication among bankers and service providers. For example, representatives of the banking industry trade groups meet on a quarterly basis in Washington with staff members from the various Y2K teams of the FFIEC member agencies. These informative meetings are a chance to discuss ongoing efforts, upcoming programs and publications, and to exchange news on Y2K developments in general. Similarly, several of the Federal Reserve staff members responsible for publishing the Century Date Change Bulletin conduct periodic conference calls with representatives of financial industry trade groups, to exchange information about educational programs and progress being made by the banking industry. The banking agencies are also offering countless regional seminars on Y2K issues, as provided for in the "Examination Parity and Year 2000 Readiness for Financial Institutions Act." We are extremely pleased at these joint efforts and the agencies should be commended for their work in this area.

Contingency Planning

While we believe our systems will be ready for the century date change, we nonetheless are actively developing Y2K contingency plans. One reason contingency planning is so important is because banks rely on a whole host of outside service providers, which are undertaking their own Y2K remediation over which we have little control. For example, utility companies provide electricity for banking offices, branches and ATM machines; telecommunications facilitates customer inquiries of financial records and verifies transactions at ATM machines and at point-of-sale terminals (for credit cards and debit cards) in retail establishments. And banks rely on armored cars to deliver cash to bank branches and ATMs, and other transportation services to deliver checks for clearing at large banks or through the Federal Reserve. We are asking questions of these providers and testing compatibility of remediated systems.

At Zions we have developed an extensive contingency plan that sets up a framework to handle Y2K problems, involving data services, every business unit, and an emergency management team that would oversee the entire process. This document—which required over 250 pages to fully detail—covers immediate response, command control centers, back-up facilities, information centers, and detailed business recovery and resumption plans. We've even thought about how we will feed our employees who work overtime to handle any problems. The very minute after midnight of January 1, 2000, we will have already begun to validate that all applications, software, hardware, systems and infrastructure are operating as expected. No one, including me, will be taking time off time between December 26, 1999 and January 15, 2000. Hopefully, no one will be needed, but everyone is on call.

Having plans to deal with unexpected events is nothing new for the banking industry. Every bank has business recovery plans in the event of natural disasters such as hurricanes, earthquakes, tornadoes, floods and fires. When those occasions arise, the bank is typically the first business in the community to be back up and running. There are many examples of this:

• The two-dozen banks in the Grand Forks, North Dakota area got their banks up and running in April 1997 within days of the worst flooding by the Red River in this century. Banks reopened in trailers, truck stops and grocery stores to keep the cash flowing.

• In Des Moines in 1993, one bank avoided disruptions by moving most of its 750 employees to temporary offices after rising waters flooded out four of its mortgage operations' downtown buildings. And as a levee threatened to burst down-river in Kansas City, Missouri, one bank CEO rented a tractor trailer and with his 23 employees, trucked vital bank records and equipment to higher ground.

• After Hurricane Andrew roared through south Florida, bankers hauled in portable generators, transferred employees from other parts of the state and quickly made available several billion dollars in storm-related emergency loans.

• Banks recovered quickly after the World Trade Center bombing in New York, too. Despite heavy smoke, employees at one bank's international operations remained at their computers processing payments to corporations around the globe. Within hours the bank shifted its processing to a remote disaster-recovery location where, over the weekend, employees worked around the clock to complete the processing.

• Most banks reopened within a day or two of the powerful 1994 Los Angeles/Northridge earthquake. One bank's credit-card processing facility near the epicenter suffered structural damage, so the bank moved to vacant offices downtown, leased busses to transport some 520 employees to the new location and provided child-care subsidies to offset the longer work day.

• When fire swept through the 62-story First Interstate headquarters building in Los Angeles in 1988, key bank employees quickly implemented the bank's new $1.5 million disaster plan in an underground command center seven blocks away. The CEO said later that the only customers affected by the huge fire were those who banked in the headquarters' first-floor branch.

• A detailed disaster plan made it possible for bank customers to continue to get cash and make deposits after a $75 million Thanksgiving fire in 1982 hit the Minneapolis headquarters of what is today Norwest Bank. Two days later a Norwest ad read: "It takes more than a five-alarm fire to slow us down."

ABA has published its own guidance for banks to follow as they proceed through the contingency planning process, *ABA Millennium Readiness Series, Year 2000 Contingency Planning Program Management.*

II. Beyond Technology: Maintaining Consumer Confidence

The steps banks are taking now are intended to make sure our systems will work when the calendar changes. Perhaps the bigger challenge is maintaining public confidence. We believe that Congress has a critical role to play, as do bankers, in keeping consumers informed about what is being done and what they can do to prepare for the century date change. People want and need to know that their money will be safe, their records secure and their banks open to serve them next January.

Consumer education is vital. Recent focus group research by ABA indicates that consumers, while concerned about Y2K, are not overly alarmed by the prospect of the calendar change. However, we know there will be tremendous speculation between now and January 1 about what will work and what will not work. Many consumers we met with did not know that the federal financial regulators are examining every bank multiple times to test compliance on the full range of systems, software, backup and other contingency plans. The fact that bank regulators are watching over banks' Y2K efforts is good news to consumers. The fact that the Federal Reserve is printing tens of billions of extra dollars and is working to expedite cash delivery to banks from the current three days to same-day delivery is also good news to consumers. And the fact that deposits are federally-insured up to $100,000 and backed up by the full faith and credit of the federal government is good news as well.

One unique factor affecting the Y2K issue that is different than other historical events, is the advent and widespread usage of the Internet as an information medium. News reported on the Internet surrounding the Y2K issue ranges from sensible advice and preparation, to absolute propaganda. One problem with the proliferation of the Internet is the inability of many consumers to separate fact from fantasy. Many people have not realized that not everything printed on the Internet is true. There is much irrational, irrelevant and misleading information being circulated regarding this issue. Therefore, there must be an equally aggressive effort to dispense facts and dispel fiction.

This raises another critical point. Several well-intentioned organizations are advising consumers to withdraw extra cash "just to be on the safe side." In fact, it is anything but the safe side. People need to think twice about how much money they want to be carrying around with them and keeping in their house. Personal safety is each individual's responsibility. Exploiting the year change will tempt many people, from champagne vendors to petty thieves, who are well aware that people will be withdrawing extra money. There has already been one publicized report of $20,000 withdrawn from a bank in preparation for Y2K, buried in the backyard—and stolen. The safe side? Not at all.

At Zions Bank, this story disturbed us tremendously. We thought that this would be a good example to reach out to our customers to help them make good decisions. I've attached to this testimony a copy of the letter we are sending to Zions customers.

The message is simple: The safest place for customers' money is in the bank. It is much harder to steal, and it is FDIC-insured. The consumers we spoke to in our focus groups were concerned about the accuracy of their bank records and getting access to their cash. In terms of accuracy, customers get statements of their accounts monthly. Banks reconcile their books daily and have extensive backup records to preserve the financial data. In addition, banks will be taking extra precautions with manual reports and backups during the calendar change. At Zions, in addition to regular monthly statements, we will provide to any of our customers, year-end cut-off statements for them to use as a point of reconciliation should it be necessary.

How much cash will people need? Probably about as much as they would need on any other holiday weekend. Personal checks are Y2K-compliant and will work anywhere—in the bank and at a wide range of retailers and service providers, both in- and out-of-state. If people are still concerned about their cash needs, they can put a little extra money in their checking account—their FDIC-insured checking account. Would you want to be carrying around a lot of extra cash? Would you want your elderly relatives to be carrying around a lot of extra cash? I know I do not.

There are steps consumers can take to prepare for the change:

- Read the information their bank sends them about Y2K. Call the bank if they have any questions at all. Trust, but verify, in other words.
- Hold onto bank statements, bank receipts, canceled checks and other financial records, especially for the months leading up to January 1.
- For customers that bank on-line, make sure home computers are Y2K-ready. Check with computer and software manufacturers for details on how to do this.
- Copy important financial records kept on home computers to a back-up disk.

• Do not give money to anyone who promises to "keep it safe" through the date change.

• Withdraw only as much cash as would be typical for any other holiday weekend.

For our industry's part, ABA is communicating with bankers, consumers and the media. We have produced three informational videos for banks to use with their customers—one designed for retail customers, a second for a bank's tellers and other front-line personnel, and a third for small business customers. We send a monthly fax newsletter to banks, which contains updates, helpful tips and shares ideas that have worked for other banks. We have provided ads, a Y2K customer communications kit to help bankers reach out to their customers, telephone seminars on a wide range of aspects of the Y2K challenge, a Y2K Project Management Manual and a Y2K Contingency Plan Manual. The latest piece in this continuing series is a Y2K Instruction Booklet containing tips to help banks comply, communicate and cope. ABA's web site—ABA.com—provides our members with other Y2K resources and information.

In December, ABA ran a full-page ad in USA Today and beamed a video news release via satellite to more than 700 television stations around the country to reach out directly to consumers. The news release included part of an interview with John Koskinen, chairman of the President's Council on Year 2000 Conversion, who has said the banking industry is "ahead of the curve" in Y2K preparedness.

ABA has also been holding media briefings jointly in Washington with the other financial trade groups, and around the country in collaboration with the state bankers associations. We are also doing special media tours, making bankers available to discuss Y2K issues on TV and radio.

Customer communication is a must for every bank in the country. After all, every customer wants to know about their particular bank. No one knows how consumers will behave leading up to January 1, and we will continue to conduct research to track their behavior and their level of concern. One thing is sure: they need information, sound advice and reassurance—from their bank, the banking industry, the federal banking regulators, and the U.S. Congress.

III. More Can Be Done: Legislative Initiatives Needed

Congress, government and regulators have a special role to play in disseminating accurate information and creating an environment for open discussion. The bill enacted last Congress—Year 2000 Disclosure Act—was a first and extremely important step in this direction. It helped set a tone for talking openly and honestly about the problem by encouraging information sharing. Further, it ensures that disclosure of Y2K-related technical information will not become the subject of lawsuits.

Congress can make a difference this year as well. In particular, we urge Congress to consider broader Y2K liability issues, such as disruption liability, punitive damages, class actions, and litigation reduction. The cost of doing nothing may be considerable. As I noted above, the industry has already spent billions of dollars on Y2K remediation efforts. Industry consultants further project that $2 million could be spent on litigation for every $1 million spent on system remediation.

The ABA, working with a multi-sector coalition, has identified several desirable legislative reforms that would help address these concerns.

• Limit Y2K litigation to actual damages, and place limits on consequential or punitive damages, unless parties have agreed otherwise by written contract.

• Provide for a "reasonable efforts" defense for parties that meet a good faith or due diligence standard.

• Require federal preemption for all Y2K legal and equitable claims, unless parties have agreed otherwise by written contract.

• Abolish joint and several liability and create a federal comparative negligence rule to apportion liability among multiple parties.

• Discourage and channel class action lawsuits through minimum claim requirements, notice procedures, and creating federal diversity jurisdiction.

There are additional provisions being considered which would: encourage the use of alternative dispute resolution to resolve Y2K disputes without resorting to litigation; require a "cure period" prior to commencing legal action, allowing parties time to remedy Y2K disruptions; require mitigation of damages by claimants; and place limits on attorneys' fees.

We would be happy to work with Congress to pass legislation in this important area.

CONCLUSION

Mr. Chairman, the banking industry has every reason to be working diligently in meeting the Y2K challenge, and is doing so with a wide ranging response that sets an example for other industries to follow. Financial institutions across the U.S. are executing Y2K project plans that are vast in scope, complexity and scale. The banking industry is taking the century date change very seriously, with the goal of achieving Y2K readiness clearly in sight. But the banking industry alone cannot deliver "business as usual" in January 2000. There must be parallel commitments by all other sectors of the economy so that they can become equally prepared. We encourage Congress to continue its oversight of the broad range of business and government sectors that together are essential to producing Y2K readiness in the American economy.

["Countdown to 2000: Preparing Your Business for Y2K" will be retained in the official Committee records.]

ZIONS FIRST NATIONAL BANK
Salt Lake City, Utah, Month DD, 1999

(*Personalized* Name and Address)

Re: Year 2000 Readiness Disclosure

Dear (*Personalized* Name):

Recently, the morning news of NBC-TV's Cleveland affiliate reported that a couple took $20,000 out of their bank and buried it. Apparently, they feared that the upcoming change in the Year 2000 ("Y2K") would mean their money wasn't going to be safe, and that they wouldn't be able to access it if they needed it. In a matter of only a few days, they discovered it missing from where it had been buried. The couple was quoted as saying, "Next time, we are going to keep our money in the bank."

News reports about the Y2K challenge have made some people nervous; a few have considered taking or have already taken irrational actions, like burying their money or stuffing it in a mattress. Undoubtedly, some of these will pay dearly for not trusting their bank.

Zions Bank has been serving the financial needs of our clients for over 125 years, since our founding by Brigham Young in 1873. Because of our conservative policies, we have been a strong, consistent financial resource to the people of Utah and Idaho—through all kinds of adversity. Zions Bank has been preparing for the Year 2000 for some time, now, as described in the enclosed brochure. We have upgraded our computer hardware and software, and our testing of the changes has been very satisfactory, thus far. We plan to continue such testing throughout 1999, to ensure that our systems satisfactorily meet our needs.

Zions Bank will be prepared for the change to Year 2000. Your money in Zions Bank will be safe throughout the Y2K transition, and you will be able to access it conveniently and in a variety of ways, as you have always done before. We are also working closely with our regulatory agencies and the American Bankers Association as they strive to ensure that direct deposit of social security and other federal recurring payments will not be disrupted.

As a valued Zions Bank client, please know that we are making every effort to minimize—or even eliminate—interruptions to our service due to Y2K problems. We value your relationship. And we don't want you to be victimized like the couple who buried their money. We hope you will continue to rely on the bank you can trust.

Sincerely,

A. SCOTT ANDERSON.

Chairman ARCHER. Thank you, Mr. Anderson. Our next witness is Mr. Joel Willemssen, representing the GAO. Mr. Willemssen, welcome and we'll be pleased to receive your testimony.

STATEMENT OF JOEL C. WILLEMSSEN, DIRECTOR, CIVIL AGENCIES INFORMATION SYSTEMS, ACCOUNTING AND INFORMATION MANAGEMENT DIVISION, U.S. GENERAL ACCOUNTING OFFICE

Mr. WILLEMSSEN. Thank you, Mr. Chairman. Thank you, Members. Thank you for inviting us to testify today on SSA's year 2000 program. As requested, I'll briefly summarize our statement and in doing so address some of the prior issues that we pointed out at SSA in our report that we issued on their year 2000 program, discuss what kind of actions they have taken in response to our recommendations, and then where SSA stands today.

Our earlier report on SSA's Y2K program noted that the agency had made significant progress in assessing and renovating mission-critical mainframe software that enables it to provide benefits to the public. SSA first recognized the Y2K challenge 10 years ago and was therefore able to respond early. With their knowledge and experience, SSA is recognized as a Federal leader on Y2K.

While SSA deserved credit for its leadership, we had previously identified three key risk areas within their Y2K program. One concerned the compliance of systems for State Disability Determination Services. Second was the need to focus on the compliance of SSA's data exchanges with other organizations. Third was the need for SSA to develop business continuity and contingency plans that would be available in the event of system failures.

SSA agreed with our recommendations in these areas, and agency efforts to implement them have either been taken or are under way. For example, SSA has enhanced its monitoring and oversight of State disability systems by establishing a full-time project team, designating project managers and coordinators and requesting biweekly status reports.

SSA reported in its most recent Y2K quarterly report that all automated State systems have now been renovated, tested, implemented, and certified Y2K compliant as of January 31.

In the date exchange area, SSA is reporting as of January 31, 98 percent of its external exchanges have now been made compliant.

Turning to contingency planning, SSA's made major progress. In addition to developing an overall framework for business continuity, the agency is now in the process of developing local contingency plans. SSA is scheduled to complete the development of all of its contingency plans by April 30 and to complete testing of these plans by June 30.

As the Commissioner pointed out, SSA is also to be commended for adopting a detailed day-one strategy that will lay out its procedures for the period between late December and early January, 2000. SSA also plans to minimize changes to its systems that have been certified as year-2000 compliant by not allowing other discretionary changes to be made.

Overall, we've seen significant progress in SSA's efforts to become Y2K compliant. Several of SSA's actions constitute best practices that could and should be adopted governmentwide.

At the same time, SSA cannot let up with its Y2K efforts. It must ensure that all of its data exchanges are made compliant and tested, it must complete the development and testing of contingency plans, and in those cases where it needs to modify already-

compliant software, it will need to retest and recertify those changes.

That concludes the summary of my statement. And after the panel is done, I'll be pleased to address any questions you may have.

[The prepared statement follows:]

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

Mr. Chairman and Members of the Committee: We appreciate the opportunity to join in today's hearing and share updated information on the readiness of computer systems that support key benefits programs to function reliably in the next century. As you know, successful Year 2000—or Y2K—conversion is critical if programs such as Social Security are to provide accurate services and benefits without interruption. Millions of Americans rely on such monthly payments.

In a previous report and testimony, we described the efforts that the Social Security Administration (SSA) was making to ensure that its information systems are Year 2000 compliant.[1] This morning I would like to briefly summarize our findings and recommendations from that report, describe actions taken on those recommendations, and provide our perspective on where SSA stands today.

SIGNIFICANT EARLY PROGRESS MADE, BUT THREE KEY AREAS OF RISK IDENTIFIED IN SSA'S YEAR 2000 PROGRAM

Our previous report and testimony noted that SSA had made significant early progress in its efforts to become Year 2000 compliant. SSA first recognized the potential impact of the Year 2000 problem in 1989 and, in so doing, was able to launch an early response to this challenge. SSA initiated early awareness activities and made significant progress in assessing and renovating mission-critical mainframe software that enables it to provide Social Security benefits and other assistance to the public. Because of the knowledge and experience gained through its Year 2000 efforts, SSA is now a recognized federal leader in addressing this issue. Among other responsibilities, SSA's Assistant Deputy Commissioner for Systems chairs the Chief Information Officers Council's Committee on the Year 2000 and works with other federal agencies to address Year 2000 issues across government.

While SSA deserves credit for its leadership, our earlier report and testimony pointed out that three key areas of risk nonetheless threatened to disrupt its ability to deliver benefits payments. One major risk concerned Year 2000 compliance of mission-critical systems used by the 54 state Disability Determination Services (DDS) that provide vital support to SSA in administering its disability programs. Specifically, SSA had not included these DDS systems in its initial assessment of systems that it considered a priority for correction. Without a complete agencywide assessment that included the DDS systems, SSA could not fully evaluate the extent of its Year 2000 problem, or the level of effort that would be required to correct it.

A second major risk in SSA's Year 2000 program concerned the compliance of its data exchanges with outside sources, such as other federal agencies, state agencies, and private businesses. In addressing the Year 2000 problem, agencies need assurance that data received from other organizations are accurate. Even if an agency has made its own systems Year 2000 compliant, the data in those systems can still be contaminated by incorrect data entering from external sources. SSA has thousands of data exchanges with other organizations, including the Department of the Treasury, the Internal Revenue Service, and the states. For example, each month SSA relies on its data exchange with Treasury's Financial Management Service (FMS) to process and disburse 50 million benefits payments totaling approximately $31 billion. Other exchanges may involve data reported on individuals' tax-withholding forms or pertaining to state wages and unemployment compensation. Unless SSA is able to ensure that data received are Year 2000 compliant, program benefits and eligibility computations that are derived from the data provided through these exchanges may be compromised and SSA's databases corrupted.

Third, the risks to SSA's Year 2000 program were compounded by the lack of contingency plans to ensure business continuity in the event of systems failure. Busi-

[1] *Social Security Administration: Significant Progress Made in Year 2000 Effort, But Key Risks Remain* (GAO/AIMD–98–6, October 22, 1997) and *Year 2000 Computing Crisis: Continuing Risks of Disruption to Social Security, Medicare, and Treasury Programs* (GAO/T–AIMD–98–161, May 7, 1998).

ness continuity and contingency plans are essential. Without such plans, agencies will not have well-defined responses and may not have enough time to develop and test alternatives when unpredicted failures occur. Federal agencies depend on data provided by their business partners as well as on services provided by the public infrastructure. 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. At the time of our October 1997 review, SSA officials acknowledged the importance of contingency planning, but had not developed specific plans to address how the agency would continue to support its core business processes if its Year 2000 conversion activities experienced unforeseen disruptions.

We recommended that SSA take several specific actions to mitigate the risks to its Year 2000 program. These included (1) strengthening the monitoring and oversight of state DDS Year 2000 activities, (2) expeditiously completing the assessment of mission-critical systems at DDS offices and using those results to establish specific plans of action, (3) discussing the status of DDS Year 2000 activities in SSA's quarterly reports to the Office of Management and Budget (OMB), (4) quickly completing SSA's Year 2000 compliance coordination with all data exchange partners, and (5) developing specific contingency plans that articulate clear strategies for ensuring the continuity of core business functions.

ACTIONS BEING TAKEN TO MITIGATE YEAR 2000 RISKS

At the request of this Committee's Subcommittee on Social Security and the Senate Special Committee on Aging, we are currently monitoring SSA's implementation of our recommendations and additional actions it is taking to achieve Year 2000 compliance. SSA agreed with all of our earlier recommendations, and efforts to implement them have either been taken or are underway. Testing of systems to ensure Year 2000 compliance is vital, and we are continuing to evaluate the effectiveness of the agency's efforts in this area.

SSA has enhanced its monitoring and oversight of state DDSs by establishing a full-time DDS project team, designating project managers and coordinators, and requesting biweekly status reports. The agency also obtained from each DDS a plan identifying the specific milestones, resources, and schedules for completing Year 2000 conversion tasks. Further, in accordance with our recommendation, SSA in November 1997 began including information on the status of DDS Year 2000 compliance activities in its quarterly reports to OMB. SSA reported in its most recent quarterly report (February 1999) that all automated DDS systems had been renovated, tested, implemented, and certified Year 2000 compliant as of January 31, 1999.

In another critical area, data exchanges, SSA has identified its external exchanges and has coordinated with all its partners about the schedule and format for making them Year 2000 compliant. As of January 31, 1999, SSA reported that 98 percent of all of its external data exchanges had been made compliant and implemented, and that it was either in the process of testing those exchanges that remained noncompliant or was waiting for its partners to make the exchanges compliant.

Among SSA's most critical data exchanges are those with FMS and the Federal Reserve for the disbursement of Title II (Old Age, Survivors and Disability Insurance program) and Title XVI (Supplemental Security Income program) benefits checks and direct deposit payments. SSA began working with FMS in March 1998 to ensure the compliance of these exchanges, and recently reported that the joint testing of check payment files and the end-to-end testing from SSA, through FMS and the Federal Reserve for direct deposit payments, had been successfully completed. Further, SSA stated that it began generating and issuing Title II and Title XVI benefits payments using the Year 2000 compliant software at SSA and FMS in October 1998.

Turning to contingency planning, SSA has instituted a number of key elements, in accordance with our business continuity and contingency planning guidance.[2] It initially developed an overall framework for business continuity that presented an effective high-level strategy for mitigating risks associated with the Year 2000. For example, the plan identified SSA's core business functions that must be supported if Year 2000 conversion activities experience unforeseen disruptions; potential risks to business processes and ways to mitigate those risks; and milestones, target dates,

[2] *Year 2000 Computing Crisis: Business Continuity and Contingency Planning* (GAO/AIMD–10.1.19, March 1998 [exposure draft], August 1998 [final]).

and responsible components for developing local contingency plans and procedures for SSA's operating components.

SSA is now in the process of developing local contingency plans to support its core business operations. It has also received contingency plans for all state DDSs. Among the plans that SSA reports as being completed at this time is the Benefits Payment Delivery Year 2000 Contingency Plan, developed in conjunction with Treasury and the Federal Reserve to ensure the continuation of operations supporting Title II and Title XVI benefits payments. SSA is scheduled to complete the development of all of its contingency plans by April 30, 1999, and to complete the testing of all plans by June 30 of this year.

As noted in our guide, another key element of a business continuity and contingency plan is the development of a zero-day or day-one risk reduction strategy, and procedures for the period between late December 1999 and early January 2000. SSA has developed such a strategy. Among the features of this strategy is a moratorium on software changes, except for those mandated by law. SSA plans to minimize changes to its systems that have been certified as Year 2000 compliant by not allowing discretionary changes to be made. The moratorium will be in effect for commercial-off-the-shelf and mainframe products between July 1, 1999, and March 31, 2000, and for programmatic applications between September 1, 1999, and March 31, 2000. Such a Year 2000 change management policy will significantly reduce the chance that errors will be introduced into systems that are already compliant.

Other aspects of SSA's day-one strategy are the implementation of (1) an integrated control center, whose purposes include the internal dissemination of critical data and problem management, and (2) a timeline that details the hours in which certain events will occur (such as when workloads will be placed in the queue and backup generators started) during the late December and early January rollover period.

SSA is also planning to address the personnel issue with respect to the rollover. For example, it plans to obtain a commitment from key staff to be available during the rollover period and establish a Year 2000 leave policy. Such a strategy, developed well in advance of the turn of the century, should help SSA manage the risks associated with the actual rollover and better position it to address disruptions if they occur.

SSA WELL-POSITIONED FOR THE YEAR 2000, BUT SOME WORK REMAINS

Overall, we have seen significant continuing progress in SSA's efforts to become Year 2000 compliant. The agency reported that, as of January 31, 1999, it had completed the renovation of all mission-critical systems so targeted, and implemented them in production. The actions that SSA has taken to mitigate risk to its Year 2000 program have demonstrated a sense of urgency and commitment to achieving readiness for the change of century, and will no doubt better position SSA to meet the challenge. Moreover, several of SSA's actions— such as its implementation of a day-one strategy—constitute a best practice that we believe should be followed governmentwide.

It is important to note, however, that SSA still needs to effectively complete certain critical tasks to better ensure the success of its efforts. For example, SSA must ensure that all of its data exchanges are made compliant and tested. It must also complete the development and testing of contingency plans supporting its core business processes. In addition, where the agency may be required to modify compliant software in accordance with legislative mandates, these modifications will have to be retested and recertified. Our ongoing review of SSA's Year 2000 actions shows that the agency has established deadlines for completing its remaining tasks, and is actively monitoring its progress.

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

Chairman ARCHER. Thank you, Mr. Willemssen. Our last witness in this panel is Mr. Dennis Schindel. "Schindel" or "Schin-dell?"

Mr. SCHINDEL. "Schin-dell."

Chairman ARCHER. Who is with the Office of the Inspector General for the Department of the Treasury. We are pleased to have you with us today, and you may proceed.

STATEMENT OF DENNIS S. SCHINDEL, ASSISTANT INSPECTOR GENERAL FOR AUDIT, OFFICE OF INSPECTOR GENERAL, U.S. DEPARTMENT OF THE TREASURY

Mr. SCHINDEL. Thank you, Mr. Chairman, Representative Rangel, and Members of the Committee. I'm pleased to appear before you today to discuss the Office of Inspector General's oversight of the Department of Treasury's efforts to address the year-2000 problem.

In the interest of time, I'll briefly summarize the results of our work at Treasury and then discuss more specifically the results of our work at the Financial Management Service.

We have been actively engaged in reviewing Treasury's Y2K efforts. We performed work at the department and at each Treasury bureau except the IRS and the U.S. Customs Service. With regard to those two bureaus, we were able to leverage our resources with the General Accounting Office and with the former IRS Inspection Service, now the Treasury Inspector General for Tax Administration.

GAO performed work at Customs, and GAO and the IRS Inspection Service reviewed IRS' Y2K efforts.

The nature of the Y2K problem is such that I don't think that anyone can really say for certain that they will be ready on January 1, 2000. Our work, however, showed that the Treasury Department has done a credible job managing this massive effort.

Treasury has applied significant resources and top-level management attention to the effort and has reduced the risk that a significant Y2K failure will occur within a critical Treasury operation. Out of a total of 321 mission-critical systems, Treasury has reported that as of December 31, 1998, 266 are Y2K compliant. While progress is good, there is certainly a lot more work to be done. End-to-end testing, systemwide testing, and regression testing must be performed to ensure system readiness.

In addition, business continuity and contingency plans must be prepared, re-evaluated, and tested. Treasury has a good infrastructure in place for managing these remaining tasks, which should help ensure that they are successfully completed.

Now let me address our work at FMS. In performing work at FMS, we focused, as we did at the other Treasury bureaus, on the broader issue of how well the overall Y2K conversion effort was being managed. We knew that with a project of this magnitude, one could apply all the personnel, equipment, and expertise that was needed, and still not be successful if it was not well managed. Our experience in working with the bureaus in the early stages of implementing the Chief Financial Officers Act taught us that the most successful bureaus were the ones that first obtained strong commitment from the top and then obtained buy-in and participation from all program managers in all parts of the organization.

The specific areas that we focused on in our work at FMS were project management, system conversion and certification, data exchange, and contingency plans for business continuity. Before I describe the results of our work at FMS, it should be noted that FMS has taken action to address all of our findings and recommendations. In addition, they have started and/or completed a number of their own initiatives to strengthen their Y2K conversion process.

As a result, FMS's management of their conversion effort, their progress in getting systems implemented, tested, and certified, and their contingency planning efforts are much improved from when we conducted our audit work.

That audit work showed that FMS had a project-management infrastructure, a certified Y2K platform, reasonable guidance, a commitment from the Commissioner, and an inventory of mission-critical systems in place to address its Y2K conversion tasks. However, some parts of FMS's management process needed to be strengthened, and certain key parts of the Y2K conversion process needed to be better executed.

For example, the chief information officer had overall responsibility for FMS's Y2K effort through the establishment of the Y2K special projects office. However, we found that summarized project information flowing into the special projects office and ultimately to the department and OMB was not always accurate, reliable, and consistently gathered. This made it more difficult for the special projects office to effectively manage the FMS-wide effort.

FMS has informed us that the completeness and accuracy of project information has now been improved since we conducted our audit work.

We also found that for one of FMS's external systems, that is, systems that are developed and maintained by an outside contractor, FMS needed to improve their ability to assess Y2K compliance. The system that we specifically looked at was the Government Online Accounting Link System, GOALS, which is entirely operated and maintained by a contractor at a contractor's facility.

FMS has significantly limited the amount of test documentation required from the contractor, which would, in turn, limit FMS's ability to review the completeness and reliability of the test results. This potentially increases the risk that GOALS may not be Y2K compliant and FMS would not be aware of it.

FMS has taken a number of steps to address this situation, including performing their own tests of the contractor's certifications.

In all, we made 14 recommendations for improvement. These recommendations address key areas of project management, system conversion, certification strategies, data exchange strategies, and contingency planning. We recently discussed with FMS their efforts to address the recommendations we made as a result of our audit.

FMS has taken positive steps and made progress toward reducing the risk of a Y2K systems failure. As of January 31, 1999, 36 of their 62 mission-critical systems are compliant. FMS anticipates the remainder of their mission-critical systems will be implemented by March 1999. FMS has also initiated coordination with data-exchange partners and started some end-to-end testing.

One of the most significant issues at FMS is processing of Social Security payments. SSA and FMS have worked together to ensure the entire process for providing Social Security benefits, from calculating benefits to making payments, is ready for the century date change. Approximately a month ago, an independent contractor informed FMS that monthly payments to the Social Security payment system are indeed ready for the Y2K date change. This represents a critical step in the Y2K work on these systems, and FMS will continue to test throughout 1999.

While this progress is good, FMS still has a lot of work to do, including end-to-end testing with approximately 30 Federal agencies to provide additional assurance on the GOALS system. Also, although FMS has prepared contingency plans for all mission-critical systems, those plans need to be updated and tested.

I'd like to now briefly describe our plans for additional work throughout the remainder of 1999. Like management, our job is not done with regard to Y2K conversion effort. We plan to perform additional work at the ATF, the U.S. Mint, and FMS to review their progress related to testing and contingency planning, as well as provide coverage on the progress of the Office of Thrift Supervision and OCC, the supervision of financial institutions' Y2K readiness.

Our work at FMS will be performed in conjunction with GAO.

And finally, we will continue to monitor reported progress by all the other Treasury bureaus and the Department.

In conclusion, I'd like to say, that Treasury has expended a great deal of effort trying to fix the Y2K problem over this past year. This effort has resulted in a great deal of progress. Treasury's ability to manage and accomplish a successful Y2K conversion is a lot less uncertain today than it was a year ago.

At the same time, no one can sit back and declare victory. A great deal of work remains to be done. If, in the next few months, the results of the remaining implementation or testing of critical systems identifies serious Y2K non-compliance, it could be difficult to put the fixes in place and perform necessary re-testing before the calendar turns. If sound contingency and continuity of business plans have not been adequately tested and are not in place and ready, there may be no way to avoid serious disruption.

The intensity of the current Y2K conversion effort and the top management attention that it has received needs to continue right through to the millennium.

Mr. Chairman, this concludes my remarks, and I'll be happy to answer any questions.

[The prepared statement follows:]

Statement of Dennis S. Schindel, Assistant Inspector General for Audit, Office of Inspector General, U.S. Department of Treasury

INTRODUCTION

Mr. Chairman, Members of the Committee, I am pleased to appear before you today to discuss the Office of Inspector General's (OIG) oversight of the Department of the Treasury's efforts to address the Year 2000 (Y2K) problem. I will focus first on Treasury's overall Y2K conversion effort and then specifically on the efforts at the Bureau of Alcohol, Tobacco and Firearms (ATF) and the Financial Management Service (FMS). I will then briefly discuss the audit work we have planned for the remainder of Fiscal Year 1999.

The impact of a significant Y2K failure within Treasury on the operations of other Federal agencies, state and local governments, and the public is well understood by this Committee and others. The question remaining now is whether we are prepared, and are there any major operations or services that will not be fixed in time to avert a major disruption. Unfortunately, that question will probably not be fully answered until we enter the new millennium. What we can say from our review of Treasury's effort, is that Treasury has done a credible job managing this effort, has applied significant resources and top management attention to the effort, and has reduced the risk that a significant Y2K failure will occur within a critical Treasury operation. In addition, Treasury has provided constant oversight over the bureaus progress and has established working groups with representatives from each bureau. The purpose of these working groups is to exchange information, share best practices, and learn from one another. In addition, Treasury has streamlined the

contract procurement process for key Y2K tasks such as independent verification and validation.

OVERALL TREASURY RESULTS

In its February report to the Office of Management and Budget (OMB), Treasury reported that as of December 31, 1998 a total of 266 out of 321 mission critical systems were compliant. According to the monthly status reports, all bureaus anticipate meeting OMB's March 1999 milestone for implementation, except for ATF and the Internal Revenue Service (IRS) both of which have efforts underway to deal with the slippage. While the progress is good, there is certainly a lot more work to be done. Even if the bureaus have implemented their systems, they must continue to perform testing throughout 1999. End to end testing, system wide testing, and regression testing must be performed to ensure systems are ready for the next millennium. In addition, business continuity and contingency plans must be prepared, reevaluated, and tested. Now let me briefly describe the work we did in reviewing Treasury's Y2K conversion effort and what we found.

Starting over a year ago, we divided our review into three phases. In phase one, we assessed Treasury's compliance with the Y2K requirements of the Federal Financial Managers Integrity Act (FFMIA). This involved looking at whether the Department and individual bureaus had adequate plans for attacking the Y2K problem, were providing OMB with the required status reports, and were meeting the milestones established by OMB. We issued our report on that phase on April 10, 1998 indicating that the Department was in compliance with FFMIA.

In phase two, we assembled teams of auditors to review more in depth the efforts at each Treasury bureau, except IRS and the U.S. Customs Service (Customs). With regard to these two bureaus, we were able to leverage our resources with the General Accounting Office (GAO) and the IRS Inspection Service, now the Office of the Treasury Inspector General for Tax Administration. Both GAO and the IRS Inspection Service performed work at IRS, and GAO also reviewed Customs. I would like to mention that we had an excellent working relationship with both GAO and the IRS Inspection auditors. By working together, we were able to share best practices while enabling Treasury to get an independent audit assessment in every bureau as well as Departmental operations. In addition, we performed an audit to determine how well the Office of the Comptroller of the Currency (OCC) in the early stages of its effort, performed Y2K examinations of banks under OCC supervision.

In performing our work in phase two, we focused on the broader issue of how the overall Y2K conversion effort was being managed. Specifically, we determined if processes existed and were designed to mitigate the Y2K risk to an acceptable level for ensuring all mission critical Information Technology (IT) systems remain operable. Therefore, we are not intending to represent or convey statements that any given system is Y2K compliant or that a system will or will not work into the next millennium. We knew that with a project of this magnitude, one could apply all the personnel, equipment and expertise that was needed and still not be successful if it was not well managed. Our experience in working with the bureaus in the early stages of implementing the Chief Financial Officer (CFO) Act taught us that the most successful bureaus were the ones that first obtained strong commitment from the top and then obtained buy-in and participation from all the program managers. The same is true of the Y2K conversion effort. If it were viewed as principally the responsibility of the Chief Information Officers (CIO) and the IT personnel, then the significant amount of progress that is needed in a relatively short period of time, with no option for an extension, would not likely occur.

We found that the Department and the bureaus established a good infrastructure for managing the Y2K conversion effort and minimizing the risk that a Y2K induced failure would have on its mission critical operations. However, the inherent nature of the Y2K dilemma denies the ability to completely eliminate risk. Despite their best efforts and demonstrated success, the Y2K problem comes with inherent risks that all organizations face and will continue to face. Accordingly, even in those bureaus where no significant weaknesses were found, we developed three suggestions encouraging all Treasury bureaus to sustain efforts in the areas of change management, data exchange, and contingency planning for business continuity to minimize potential disruptions caused by these inherent risks. Specifically, the actions we suggested were:

- Ensure that a disciplined change management process exists that continues to maintain Y2K conversion integrity. Once a system has been certified, steps need to be taken to ensure test integrity is maintained and subsequent changes to the environment or application do not regress Y2K compliance.

• Ensure that data exchange procedures identify and coordinate pivots with exchange partners.[1]

• Ensure the continued development, testing, and reevaluation of contingency plans for each core business function, as well as mission critical systems. Business continuity planning is essential to maintain an acceptable level of core business processes in the event of an unanticipated failure.

In our phase two audit, we did identify four bureaus with significant issues that required prompt action to assist in the success of their Y2K effort. In these four bureaus we made additional specific recommendations to correct the weaknesses we found. We worked closely with bureau officials to promptly alert them to these weaknesses, and we found the officials were very receptive to our recommendations. In most cases, our recommendations were acted upon before we issued our reports.

Since ATF and FMS are two of the bureaus represented at this hearing and were included in our phase two audit work, I will briefly discuss the weaknesses we identified at each of these bureaus, the recommendations we made, and how each bureau has responded. As I stated earlier, GAO performed work at the IRS and Customs and will address those bureaus in their testimony.

ATF RESULTS

I will first start with ATF, which by coincidence was the bureau where we piloted our phase two audit approach. I want to preface my remarks by saying that not only was ATF very responsive to our findings and recommendations, but they were extremely open and cooperative with us from the very beginning of our audit work. This helped accelerate our learning process, and enabled us to share what we learned from ATF with other bureaus. I also want to point out that at the time we performed our work at ATF they too were still learning how to best approach their Y2K conversion effort and manage it effectively. It has been four months since we issued our draft report to ATF and even longer since we first brought our findings to their attention. ATF has taken corrective action on issues we identified during our audit, and, as a result, their management of the process and their progress has greatly improved.

The purpose of our audit at ATF was to determine if an infrastructure for managing the conversion effort and minimizing the risk that a Y2K induced failure would have on its operations had been established. Our specific objectives were to evaluate ATF's Y2K effort for the following: (1) project management; (2) system conversion and certification; and (3) contingency plans for business continuity.

We found that ATF had an infrastructure, skilled resources, and reasonable guidance in place to address its Y2K conversion task. However, somes aspects of managing the effort and coordinating among the various components within ATF needed to be strengthened. Also, while ATF was generally following GAO's Y2K guidance, improvements were needed in some key parts of the Y2K conversion process. For example we identified the need for better coordination and communication between the Y2K project office and the software development staff to accommodate the respective needs of the affected groups within the organization. Originally, we found that while the two groups were dependent on each other for Y2K certification they had not coordinated testing, migration, and certification dates with each other. As a result, the Y2K project office was unable to identify systems that were ready for certification since the two schedules had differences in key system dates. After we discussed this issue with ATF officials, they expedited the reconciliation of their testing schedules from these cross functional areas with Y2K responsibility.

We also found that while ATF had identified its data exchange partners, they had no plans to coordinate the testing of these interfaces with their trading partners. ATF's Y2K Project Management Office has now been assigned responsibility to ensure data exchange testing procedures are incorporated into the compliance testing process.

In our report to ATF[2] we identified four major areas where improvements were needed. These are summarized below. We included nine specific recommendations in our report designed to help ATF strengthen their Y2K conversion effort in each of these areas:

---

[1] The windowing logic technique uses pivots to interpret a two digit year into a four digit year. All year values above the pivot are understood to represent one century; while all values below the pivot are understood to represent another century. Pivots refer to a number built into system logic to infer the 2 digit century identifier "19" or "20." For example, a pivot of 50 infers 19 as the century identifier for values 50–99 and infers 20 for values 0–49.

[2] *Year 2000 Compliance Effort at the Bureau of Alcohol, Tobacco and Firearms* (OIG–99–021, December 18, 1998)

• Project management should be further strengthened by developing performance measures to ensure accountability and taking the appropriate action to ensure continuity in contracted support.
• System conversion process and certification plans should be further strengthened by coordinating cross-functional activities; formalizing the Y2K compliance testing procedures; minimizing concurrent development; and improving configuration management for maintaining conversion integrity.
• Data exchange testing strategies should be improved by including the necessary coordination with data exchange partners.
• Contingency planning should be further strengthened by accelerating the timeline for developing and testing contingency plans and developing the plans on a prioritized basis.

We recently met with ATF to determine what progress they have made since our field work. Although they have made significant progress in all areas (implementation, certification, and contingency planning) and have implemented most of our recommendations, ATF still has a lot of work ahead of them. They have three mission critical systems that are not expected to be implemented until May, July, and August of this year. Testing still needs to be performed with critical data exchange partners and business continuity plans must be prepared and tested for each core business function. If subsequent testing shows that some systems are not ready, there will be very little time to correct and retest these systems. ATF is aware of the tight time frame and narrow margin for error. They have the infrastructure in place that should enable them to effectively address this increased risk.

FMS RESULTS

I will now focus on our observations at FMS. The purpose of our audit was to determine if FMS had established an infrastructure for managing their conversion effort and minimizing the risk that a Y2K induced failure would have on their operations. Our specific objectives were to evaluate FMS' Y2K effort for the following: (1) project management; (2) system conversion and certification; (3) data exchange; and (4) contingency plans for business continuity.

Similar to ATF, FMS has taken action to address all of our findings and recommendations. In addition, they have started and/or completed a number of their own initiatives to strengthen their Y2K conversion process. As a result, FMS' management of their conversion effort, their progress in getting systems implemented, tested, certified, and their contingency planning efforts are much improved from when we conducted our audit work.

That audit work showed that FMS had a project management infrastructure, a certified Y2K platform, reasonable guidance, a commitment from the Commissioner, and an inventory of its non-information technology mission critical systems in place to address its Y2K conversion task. However, also like ATF, some parts of FMS' management process needed to be strengthened and certain key parts of the Y2K conversion process needed to be better executed. For example, the Chief Information Officer (CIO) had overall responsibility for FMS' Y2K effort through the establishment of the Y2K Special Project Office (SPO). However, we found that summarized project information flowing into the SPO and ultimately to the Department and OMB, was not always accurate, reliable and consistently gathered. We also observed that while the SPO had prioritized FMS' mission critical systems, the application of resources and a level of effort consistent with these priorities was not being managed from an FMS-wide perspective. FMS informed us that both of these areas have been substantially improved since we conducted our audit work.

We also found that for FMS' external systems, that is, systems developed and maintained by an outside contractor, FMS needed to improve their ability to assess Y2K compliance. One such system is the Government On-line Accounting Link System (GOALS) which is entirely operated and maintained by contractors at the contractor's facilities. FMS had significantly limited the amount of test documentation required from the contractor which would limit FMS' ability to review the completeness and reliability of the test results. This potentially increases the risk that GOALS may not be Y2K compliant and FMS would not be aware of it. FMS has taken a number of steps to address this situation, including performing their own tests of the contractors certifications.

A complete summary of the issues we reported to FMS in our February 10, 1999 draft report are presented below. In addition to this draft report, we provided FMS with the detailed results of our evaluation of nine mission critical (IT) systems.

• Project management should be further strengthened by performing more quality assurance reviews to ensure reports are reliable; establishing priorities from an

FMS-wide perspective; and using performance measures to enforce adherence to FMS guidance.

• System conversion and certification strategies should be further strengthened by managing and coordinating test schedules and resources; reviewing test results and ensuring adequate testing documentation; requiring additional testing or other procedures to compensate for lack of test documentation on externally maintained systems; and ensuring a disciplined change management process exists for maintaining conversion integrity.

• Data exchange strategies should be improved by completing the data exchange inventory; establishing and completing agreements with data exchange partners; identifying and coordinating pivots; performing testing with FMS' data exchange partners; and establishing accountability for performing data exchange procedures.

• Contingency planning should be further strengthened by reevaluating, accelerating, and prioritizing the development and testing of contingency plans; defining incremental tasks to facilitate the preparation of contingency plans; incorporating data exchange risks in contingency plans; and preparing business continuity plans to ensure all core business processes continue to function at an acceptable level.

We made 14 recommendations and 1 suggestion for corrective action. These actions are designed to strengthen FMS' Y2K conversion process and, upon implementation, we believe FMS' risk of any Y2K induced failure will be reduced.

We recently discussed with FMS their efforts to address the recommendations and suggestions we made as a result of our audit. FMS has taken positive steps and made progress toward reducing the risks of Y2K system failures. As of January 31, 1999, 36 of their 62 mission critical systems are Y2K compliant. FMS anticipates that the remainder of their mission critical systems will be implemented by March 1999. FMS has also initiated coordination with data exchange partners and started some end to end testing. Despite this progress, FMS still has a lot of work to do, including end to end testing with approximately 30 Federal agencies. Although FMS has prepared contingency plans for all its mission critical systems, they still need to update and test business continuity plans.

One of the most significant issues at FMS is processing Social Security payments. FMS maintains payment systems that each year make 860 million payments with a dollar value of more than $1 trillion on behalf of the Social Security Administration (SSA), the Department of Veterans Affairs, the IRS, and other agencies. FMS systems issue more than 600 million Social Security and Supplemental Security Income payments each year on behalf of SSA—roughly 70 percent of all FMS payments.

SSA and FMS have worked together to ensure that the entire process for providing Social Security benefits—from calculating benefits to making payments—is ready for the century date change. In October 1998, FMS began to issue monthly Social Security payments on systems that had been fixed and tested while it awaited independent verification of its testing, test results, and documentation to ensure that these systems were, in fact, Y2K compliant. Approximately a month ago, the independent contractor informed FMS that monthly Social Security payment systems are indeed ready for the Y2K date change. This represents a critical step in Y2K work on these systems, and FMS will continue to test throughout 1999.

OIG Phase Three Work

In Phase three, we plan to perform additional reviews at selected bureaus to review their progress related to testing and contingency planning as well as provide coverage on the progress of the OCC and Office of Thrift Supervision (OTS) supervision of institutions. Finally, we will continue to monitor reported progress by the bureaus and the Department.

Our continuing review will be done at ATF, U.S. Mint, and FMS. The first part of our work will focus on the results of independent verification and validation and then on contingency planning. Our work at FMS will be performed in conjunction with GAO. It is critical that bureaus perform independent verification and validation to ensure adequate testing was performed. Without adequate testing, it is possible that a system could fail without warning. A review at one bureau revealed that a system was certified as Y2K compliant, but the auditors found that not all code was identified or renovated. If this was not corrected prior to the system's critical date (i.e., January 1, 2000), the system could fail. This issue was brought to management's attention, and the bureau took prompt action by bringing in an independent contractor to review 100% of the code.

In addition, the second part of phase three will focus on business continuity efforts. OMB established a March 1999 milestone for agencies to have fully implemented systems. Based on our audit work and review of the bureaus' monthly sta-

tus reports, we have identified two bureaus that are unlikely to meet this milestone: (ATF and IRS). ATF has 3 of 24 mission critical systems that will be implemented after March 1999; while IRS has 7 of 133 mission critical systems that will be implemented after March 1999. Therefore, it is even more imperative for these bureaus to have comprehensive contingency plans in place.

It is also imperative that bureaus which exchange data with international partners have reliable contingency plans in place. Early indications are that international partners have made slower progress than the United States in converting their systems; therefore, there is a higher risk that problems may occur when transacting business internationally. In each bureaus' report, we stressed either through a recommendation or suggestion the importance of contingency planning to all bureaus in the event that the milestone dates were not met or unanticipated problems were identified with the operation of an implemented system. The uncertain and uncontrollable international situation raises contingency planning for systems with international exchange data to the same critical level of concern as actual conversion of mission critical systems.

CONCLUSION

It would be an understatement to say that a great deal of effort has been put into solving the Y2K problem over this past year. However, that effort has resulted in a great deal of progress. Treasury's ability to manage and accomplish a successful Y2K conversion is a lot less uncertain today than it was a year ago. At the same time, no one can sit back and declare victory. A great deal of work remains to be done. If in the next few months the results of the remaining implementation or testing of critical systems identifies serious Y2K non-compliance, it could be very difficult to put the fixes in place and perform the necessary re-testing before the calendar turns. If sound contingency and continuity of business plans have not been adequately tested and are not in place and ready, there may be no way to avoid serious disruption. The intensity of the current Y2K conversion effort and the top management attention it has received needs to continue right through to the millennium.

Chairman ARCHER. Thank you, Mr. Schindel.

The Chair is grateful to all of you for your presentations today. I must say, generally, they come across as being comforting, which I am very pleased to hear.

Can any one of you think of any reason why the areas of operation within your supervision or purview would be disrupted as we enter the new millennium? Is there any reason why any necessary functions would be disrupted by this Y2K problem at the beginning of next year?

Mr. Apfel.

Mr. APFEL. Mr. Chairman, that's really the purpose of our contingency plans. If there are areas of potential disruption, how would we overcome those problems? Not how would we change the systems, but how would we get around and get what we need to get done, done. And some of that involves moving people to work, and moving work to people. But if there were potential disruptions, that's really the focus of what contingency planning is throughout all of Government, to focus on the areas where we could have potential problems and how to overcome those problems. In other words, if there is a power shortage in our Baltimore headquarters, our contingency assures a week's worth of power on our own to operate our computers to make sure that we can handle the workload.

So that's really what the whole focus of contingency planning is, to take a look at the "what-ifs" and decide how we will resolve the issue.

Chairman ARCHER. That's very good to hear too. So if Y2K does happen to cause any problems, you do have contingency plans so that your necessary services will continue without disruption. Is that a fair statement?

Mr. APFEL. That is a fair statement.

Chairman ARCHER. And I would say to all of you who are involved with the Federal Government, because I don't think we are going to provide any resources to Mr. Anderson out of the Federal Treasury, but for those of you involved with the Federal Government, are you satisfied that the Congress has provided adequate resources to solve the problems in the operations over which you either supervise or have within your purview?

Mr. GREGG. Mr. Chairman, speaking for FMS, we have sufficient funds to do what we need to do. We just need to keep focusing on Y2K and get it done.

Chairman ARCHER. And to all of you, is there any area where you need additional funds?

Mr. APFEL. No, sir.

Chairman ARCHER. OK. Then the record will show that the answers were unanimously "no" to that question. Those are the only questions I have. Mr. Rangel.

Mr. RANGEL. Yes. The distinguished Majority Leader, Mr. Armey, was concerned that some of our financial institutions might not be prepared to support the progress that is being made by the Social Security Administration in getting benefit checks out. And he's written to the President of the United States about this issue. And I just wondered whether anyone could satisfy his concern?

Mr. ANDERSON. If I can speak. The banking industry is on track in meeting its deadlines. And we have gone through extensive tests, both of our internal systems and with the Fed, to ensure that the payments will come to the Fed, from the Fed they will come to the bank, and from the bank they will be credited to the proper individual account. If there are glitches, we have contingency plans as well so that we can stand behind our Social Security recipients to make sure that they get through this all right.

Mr. RANGEL. Mr. Anderson, would you be kind enough to send a note to that effect to Mr. Armey because he has concerns like this. It bothers me. [Laughter.]

Mr. ANDERSON. I'd be glad to.

Mr. RANGEL. Thank you so much. Thank you, Mr. Chairman.

[Mr. A. Scott Anderson submitted his testimony to Richard K. Armey, House Majority Leader.]

Supplement to the Testimony of A. Scott Anderson; on behalf of the American Bankers Association

During the February 24 hearing, Representative Mark A. Foley (R–FL) asked that Mr. Anderson provide a discussion of the consequence to U.S. financial institutions should Y2K glitches occur in transactions with their foreign trading partners. The requested discussion follows.

The issue of global Y2K risk has been of major concern to all financial institutions that do business across borders. Aside from testing and preparing contingency plans for their domestic operations, financial institutions have been closely examining their international exposure, and assessing the Y2K readiness of their global partners. For example, consider this excerpt from the testimony of State Street Corporation, to the Senate Commerce Committee on February 9, 1999:

In much of our business, we act as an agent or true financial intermediary in a complex, interconnected chain of financial transactions. As a middleman, we inter-

act electronically with securities depositories, broker/dealers, banks, stock exchanges, telecommunications and utility providers, our customers and investment data services in more than 80 countries.

Our business exposes us to the readiness, or failure, of multiple parties beyond our control. Regardless of how well we have prepared our own information systems technology for Y2K, our ability to deliver services remains dependent upon the state of readiness of thousands of other service providers.[1]

It is precisely this interdependence of multiple parties engaged in cross-border transactions that makes it difficult to determine the overall risk level of such activities as trade finance, currency exchange, and investment settlement services. However, each financial institution that provides these important services is continuing to verify and monitor the Y2K progress of major overseas counter-parties, such as those mentioned in the referenced testimony. At the same time, financial institutions are developing contingency plans to continue their existing services in foreign markets should they face Y2K-related disruptions.

Chairman ARCHER. Mr. Crane.

Mr. CRANE. Thank you, Mr. Chairman. I want to commend Commissioner Apfel, especially for the recognition of this problem earlier, I think, than your counterparts in getting up to speed and providing that example. And my understanding is, the person who pioneered that was Kathy Adams. And is Kathy here?

Mr. APFEL. Kathy is right behind me. Dean Mesterharm also. And John Dyer.

Mr. CRANE. Congratulations, Kathy.

Mr. APFEL. I would like to take full credit for it, but it started many, many years before I became Commissioner.

Mr. CRANE. You're in deep "kimshe" if you try.

Mr. APFEL. That's right. [Laughter.]

Mr. CRANE. Let me ask one question though. And that is while you're up to speed, do you have any concerns about the post office's readiness?

Mr. APFEL. No, sir. The Postal Service is virtually complete in its operations. And again, if there is a localized problem, the same notion of moving people to work and moving work to people is in their contingency plan. If there were a problem in a certain area, the idea would be to work around it to assure the delivery of the mails.

I think you should hear that directly from the Postal Service, but we are very comfortable with our efforts that have been going on with the Postal Service in this endeavor.

Mr. CRANE. That's comforting. Well, I thank you so much. And I yield back the balance of my time.

Chairman ARCHER. Mr. Shaw.

Mr. SHAW. I would like to continue that line of questioning with regard to the delivery of the checks, and I would like to also speak to Mr. Anderson about this particular matter. What about foreign banks, American living abroad who are receiving Social Security checks. I'd like to direct this question both to Mr. Anderson and Mr. Apfel as to what would happen to them? Have we done a survey to see how they can cope with this? Anybody, either one.

Mr. APFEL. I would like to start that.

Mr. SHAW. All right.

[1] Marshall Carter, Chairman & CEO, State Street Corporation

Mr. APFEL. This is an area that I think needs greater attention over the course of this year. That's part of what our contingency planning is focusing on. If we can't get the sufficient assurances in the international arena, then we're going to have to determine alternative systems for delivery at that time.

This is one of the areas I think the U.S. banks are in a much stronger position than some in the international arena. So this is one of the areas that our contingency planning is focusing on this year.

Mr. ANDERSON. If I could just add to that, Congressman. I serve as a senior adviser to the President's Y2K Council, and that is one of the issues that we are very concerned about. We are confident that we can get the wires to those other banks, and we need to make sure that they can then credit it to the appropriate parties overseas. We have a number of our customers that do a tremendous amount of wires each day to people serving all over the world, and we have been working with those customers to develop contingency plans if in fact the wires can't get through, that we can get them the cash through other means.

One of these means is through the ATM card, where they could then access the cash overseas using the ATM card.

Mr. SHAW. This is very important not only for the beneficiaries who need these funds but also it is very disturbing as to the tracks that we leave down to prove that we did deliver these checks in compliance with the instruction of the recipient. And I think that we need to really go back and be sure there is a very good audit trail to prove that we did send the money, and that this was the choice and the designated recipient of the money made by each of the beneficiary of the Social Security system. And I think this is very important that we look into that because there could be some real glitches that we didn't prepare for.

I have just one other question that I want to ask Mr. Apfel. And I ask this with full recognition the tremendous job that you all have done at Social Security, and Kathy, and continuing under your leadership. But I do have a question. Our Subcommittee asked for certain documentation to be given to the General Accounting Office and that they do certain audits and report back to the Subcommittee. We understand that there is a problem with receiving some of the requested documents. If you comment on that or if you would get back to me if you're not prepared to comment on that, we do want to fulfill our obligation to do our oversight in that area.

Mr. APFEL. And this is in the Y2K area?

Mr. SHAW. That's what I understand.

Mr. APFEL. I am unaware of a problem in this area. We will look into it immediately and have someone contact your office today.

Mr. SHAW. If you would check with the General Accounting Office and see what they have requested that you haven't provided. And we would appreciate your expediting that.

Thank you. Thank you.

Chairman ARCHER. Mr. Coyne.

Mr. COYNE. Thank you, Mr. Chairman. Mr. Gregg, what contingency plans does FMS have should any of the direct deposit electronic systems fail?

Mr. GREGG. We have several, Mr. Coyne. First of all, we have a nationwide telecommunications network that runs out of our Hyattsville, Md., office. It has the capacity to shift work around the country. If we did have a power problem in one part of the country, we could shift payments processing to another location.

We also have a backup telecommunications facility in Kansas City. Both of our telecommunications faacilities have power generators that could operate if we had some kind of power problem in those locations.

In addition to the telecommunication network, we have three computers that can each process the full volume of our payments for any given month. So if we had a problem, say, in Austin, Texas, we could shift all the work that would normally be going out of Austin to either Hyattsville or Philadelphia, and make the payments through those facilities. I'm talking about electronic payments.

Someone mentioned earlier about the possibility of a problem with the Postal Service. If, in fact, we had some problem with the Postal Service in one part of the country, we could actually shift work and have the checks printed at another one of our regional finance centers, where they may not be having a problem with the Postal Service.

So we have quite a few contingencies to address problems that could occur. We are doing everything we can to, hopefully, reduce that risk. But we do have a good contingency plan in case something does happen.

Mr. COYNE. Are paper benefit checks available as a backup?

Mr. GREGG. Yes they are. Well, they are in terms of our ability to shift check production from one place to another. I'm very confident, extremely confident, that the electronic processes will work. We have about 70 percent of our overall payments now made electronically. The reason I'm confident is, first of all, Social Security on one side of us has been ready for some time. And, on the other side of us, we have the Federal Reserve, who started on this project about the same time as SSA. They have also shown great leadership. They have been testing with the commercial banks that receive electronic payments for some time and they will continue to test throughout this year. I'm very confident that those will work.

If we did have some isolated problem, and in my view it would be only a few banks here and there, if we did have an isolated problem, we would work with Social Security and quickly get out a replacement check for that individual.

Mr. COYNE. Thank you.

Chairman ARCHER. Mr. McCrery.

Mr. MCCRERY. Mr. Apfel, just one question. You use an example in your testimony or maybe in response to a question about the electric power going off, say, in Baltimore and you had a contingency plan that would allow you to generate your own power for a week. Is that a real-life example or was that just——

Mr. APFEL. That is a real-life example. Our data operating center, which is central to our nerve center, has its own power source.

Mr. MCCRERY. But only able to generate power for 1 week?

Mr. APFEL. We have the fuel on hand to power it for a week. Not that it would shut down in a week.

Mr. MCCRERY. OK. Well that's good because I was wondering if you were that confident that a problem of that scope, the failure of a utility company, for example, to generate power, could be solved that quickly. Do you have any thoughts on that in your contingency planning as to the ability of other entities to identify problems and solve them quickly?

Mr. APFEL. I think the overall power grid issue is a broader issue that I believe John Koskinen will be speaking to. He was supposed to testify first, but there have certainly been significant improvements in this area. The one area that we felt that was centrally important that we have covered in case of a localized outage was our data center because that is clearly the center of our operation. That is taken care of.

If a local power company—we've heard about the Austin local power—went out, what we would have to do in that situation, again, would be to redirect around it. We have 1,300 field offices. So that capacity to move work throughout the country around a localized problem is part of our contingency planning.

Now that's clearly part of the local contingency plans that we're developing now and will be finalized by the end of March, just those forms of localized problems, and how to work around them and get our work done.

Ultimately, the goal is how do we get the work done if "blank" happens? And that's what the contingency plans do.

Mr. MCCRERY. OK. Thank you.

Mr. ANDERSON. Congressman, could I add to that?

That's one of the issues that we've looked at very carefully in the banking industry. What would we do? And in our particular bank, we have a backup generator for our main computers that will take us through for 2 weeks. In addition, we will have trailers with their backup generator in the trailer that we can move around if there's outages in certain areas to continue to service the customers. And in the end, we are prepared to do it with lanterns, the old fashioned way, with flashlights and so forth.

Mr. GREGG. Mr. Congressman, I want to get on the generator bandwagon here. We also have a generator in our Hyattsville office, which is our largest center. We installed it 8 or 9 months ago. And it will run our whole operation for any length of time as long as we have the fuel. It has worked very well when we have had power problems due to the weather we have had over the 7 or 8 months since it's been installed. The generator has really worked flawlessly.

Mr. MCCRERY. Mr. Chairman, I yield back, but maybe with all this talk of extra use of fuel, we can get oil prices back up to help us out in the oil patch. [Laughter.]

Chairman ARCHER. That would be beneficial in our part of the world in any event. Mr. Collins.

Mr. COLLINS. Thank you, Mr. Chairman.

Mr. Apfel, I'm encouraged by your comments this morning about how well prepared you are for January 1, 2000, and that you had the foresight, and your predecessors had foresight many years ago, to look into this problem. I'm also encouraged by your reaction to this situation that you're going to be forthcoming with some very

good recommendations as to structural change for the Social Security system itself, as we discussed last night.

I only have one question for you. And that is, these "what-ifs." What if there is a real problem at the end of this year and the beginning of the first two or 3 days of next year, and those checks don't show up. Were you to, in your local offices, regional offices, receive the calls that are going to come from our office? Do you have a good contingency plan for that one? That's one I'm really worried about because I know that we will be overrun with calls and visits, and I know in the Atlanta region office they do a very good job of helping us today with situations, but that might be a massive one. Do you have contingency plan to handle us?

Mr. APFEL. To handle?

Mr. COLLINS. Us, as a Congress. Our calls to you in reference to constituents?

Mr. APFEL. Absolutely. Part of the local office contingency planning is—let me go to two things. First of all, our day-one strategy is for every field office, every facility, every hearing office that we have, to have people in those offices during the weekend to go through a series of real-life situations to ensure that systems are working. We have a command center in Baltimore to be able to handle that information. And that goes all the way to such things as embedded systems.

Let's say you have an electronic lock system. You want to make sure that electronic lock system is working because you don't want to get locked out. So clearly there's a whole series of things that each one of our facilities will be doing.

In addition, we'll have about 40 of our field offices that will actually be making transactions to assure that those actual transactions can take place. By the time we open the doors after the holiday, we will have assessed exactly where, if there is a problem somewhere, that problem would be. If there is a problem in a certain area in your district, we would notify your office to let you know what our contingency plans would be and how to handle that work.

Mr. COLLINS. Before the light changes, if you have any recommendations for my office through the Atlanta regional office so that we can assist you, please call with those recommendations because we want to fully prepared too.

Mr. APFEL. Very good, sir.

Mr. COLLINS. Mr. Anderson, right quickly. You mentioned the contingency plans that you have and you're encouraging and trying to educate your customers to keep their moneys in the bank. The Federal Reserve Chairman also made the same statement; however, he is printing some $200 billion extra to stockpile. I had a constituent just earlier this week who told me that he is stockpiling his own little contingency of cash as well as other things for January 1, and he's a businessperson, very well educated. So your education system is not getting down to the grassroots in all places.

Mr. ANDERSON. That is absolutely right, Congressman. And this is why I think we all have to pull together, the industry, the association, and the government, in getting out the message. We've had customers come in and pull out their life savings. And in talking

with them, they are going to take it home and keep it until after the change of the year.

I think back to my mother. I would hate my mother to do that. I would be worried about her personal security and safety. I'd be worried that something would happen to the money and then she would be destitute. She wouldn't have anything. And I think it's these fears that we really need to address, and let people know that they will be taken care of.

I'm confident that the ATM system will work. And where you can go in there on January 1 and draw out money. You have your checks. You can use your checks. You don't need to just have cash. You can use your credit cards. And so I am confident that things will be all right.

But we do have to get the message out.

Chairman ARCHER. Mr. Kleczka.

Mr. KLECZKA. Thank you, Mr. Chairman.

Commissioner Apfel, let me re-ask a question that was asked by Congressman Coyne. You gave the one scenario of the power outage, and that's been talked about at length here. Let me broach this scenario. Let me ask a question first: What percentage of your benefit checks are direct deposit, or benefit payments are direct deposit? About 70?

Mr. APFEL. About, yes.

Mr. KLECZKA. About 70. OK, which is a hefty amount. Let's assume for a moment that one or two banks in the system that accept direct deposits for some reason have a glitch, and the consumer, the beneficiary cannot access those dollars on January 3, is it? What is, January 1 is on what date, Saturday?

Mr. ANDERSON. Yes.

Mr. KLECZKA. OK, on January 3. What is that contingency plan because that is something that is going to be asked of us repeatedly throughout the year?

Mr. APFEL. The specific contingency plan: Our facility will be working with that financial institution to determine immediately whether, in the next 48 hours, the situation would be resolved so that it could be deposited electronically.

Mr. KLECZKA. And the answer to that question is it cannot. Then what?

Mr. APFEL. Step two is the arrangement to determine whether a second financial institution could make the electronic transfer. If we could not, then step three, we would be working with the FMS to cut a paper-based check. And step four, if there is an emergency, if someone said I am destitute, our field offices are prepared at that time to immediately cut a check.

So we have a several-step process.

Mr. KLECZKA. So what is the longest period of delay that a constituent, say in my district, would suffer if they went to the bank on Monday for a withdrawal, the transfer was not showing up, how long before that person could get their actual dollars?

Mr. APFEL. If the person is not in an emergency situation, it could be about a week. However, if there is a financial problem, if they really needed the cash immediately, our field offices would be prepared to cut that check immediately.

So step one, the first 48 hours with a financial institution to determine whether it can be done. Step two, it's whether there could be another alternative financial institution. If that is immediately ruled out, then cut the paper-based check. And in the case of emergency, the immediate check cut by our field office.

Mr. KLECZKA. I'm assuming you're going to be asked those questions repeatedly over the next 300 and some days. What I would ask you to do is revise the system and move off that 1 week because that will clearly cause panic with some people. So there's got to be a system where, whether or not it's an emergency, it's my money. And I went to the bank on Monday and I want $200. There's got to be some system in place where within a 24-hour or 48-hour period, that person has access to those dollars.

OK?

Mr. APFEL. In an emergency situation, the answer is absolutely yes.

Mr. KLECZKA. "Emergency" is it's my money and I want it.

Mr. APFEL. Yes.

Mr. KLECZKA. OK?

And that's what we're going to be getting in calls to our office. And it might be to pay a bill, it might be just to go shopping—I don't know. But with that person, it's an emergency to them. You know? It's not a life or death, but——

Let me also restate a point made by Mr. Anderson, which I think is probably the crux of the entire problem. And in your statement, as you well know, you indicate the biggest, the bigger challenge, is maintaining public confidence. We believe that Congress has a critical role to play as do bankers in keeping consumers informed about what's being done.

We had a hearing yesterday on an important issue on Social Security, and there were three or four cameras in the room. In fact, one is sitting right in front of you to get your fact shot. Today they are not there. And clearly, you know, I don't know where you put it in the importance of things as far as Y2K and Social Security. I think both are very important issues, but we don't have the public exposure to your comments today like we do for other hearings here. And I think it's incumbent upon Congress to make sure that we don't cause the panic. Because it's great sport bringing an agency before various Committees if one of the administrators indicates that we're not really up to speed. That word is going to get out right away, and naturally the public is going to be very concerned.

So I think the burden of consumer confidence and making sure that the perception that the sky is not falling comes from this body, the Congress itself. And the agencies are not surprised at this. They have been working for years in some cases. We know that billions and billions of dollars have been spent on the problem. And what I try to do when I go back home, in fact we write a weekly column for the local newspapers. And the one about 2 weeks ago was on Y2K and that the government is coming up to speed and there's no reason for panic. The bankers and financial institutions are there. And hopefully through that type of educational process, my consumers, or my constituents, won't be the ones buying gold and starting to hoard consumer products, be it food, water, whatever.

But let me ask this panel, and I don't know who wants to answer it. But we see the stories repeatedly on TV where there are now conventions or seminars on weekends where people are told to start squirreling away water and canned goods. Some of these things are even for sale at these seminars. We've heard the stories of people pulling their money. My nephew asked the other day whether or not he thought, or I thought it was a good, for him to get some gold. You know.

Paint me a scenario where all the food stores in the country, Giant, Safeway, Kohls, and the like would not be open at all, that our money would be worthless. I just can't fathom that transpiring, but some people do. And some people are out to make a buck by encouraging that type of thinking. Could somebody here tell me, or try to paint me the worst-case scenario, where I cannot access any food products whatsoever for a period of time, or the money supply that I have either saved or whatever is worthless, and without gold we're all in deep trouble?

Mr. ANDERSON. Mr. Congressman, I applaud your comments, and I do think we need to get the word out. I can't think of an instance where that would happen. And in fact, if you go back over history, those who have been the doomsayers in the past and said invest in gold, that's probably been the worst investment that they could have. Again, I'm convinced that the banking side will be ready, that the safest place for people's money is in the bank. People need to be careful about some of the hysteria and some of the fraudulent schemes that are out there to take money away from people, take advantage of the situation.

Mr. KLECZKA. Thank you very much. And again, thank you for your comments. Hopefully the Members of Congress will be listening to them and heeding that advice.

Thank you, Mr. Chairman.

Chairman ARCHER. Mr. Houghton.

Mr. HOUGHTON. Thank you, Mr. Chairman. Thank you, gentlemen, for your testimony. Good to see you, Commissioner Apfel. I think you're doing a great job. Thanks very much for the things that you're doing for the Y2K problem.

Let me just try to put this thing in perspective. The Y2K issue for the U.S. Government is an issue for the administration, really not for Congress, or not for the Judiciary. And the reason we are involved here is because of the oversight to see how it's going. Are there any weak spots? And I would assume that the President of the United States or any of his lieutenants have said to you, we expect that this will be solved, and be solved expeditiously so that there will be no problem with the U.S. citizenry. And if it is not, and you are worried about it, you let us know.

And, in effect, the word came back that you needed a little less than $3.5 billion, and that came forward through military and nonmilitary supplemental appropriations last year.

So I would assume, irrespective of what the problems are, there are always the "what-if," that this thing is going to be solved and you got enough money. And if it's not, I would like to know it.

Mr. APFEL. Mr. Houghton, I can only speak for the Social Security Administration, but we have fully adequate resources to completely resolve this issue. I think that the importance of this hear-

ing today is to ask that question of every agency. I think these hearings are very appropriate to look at where there are potential problem areas, and what the resource implications are. From a Social Security perspective, Mr. Houghton, I can assure you that we have the resources and the plan in place to handle this.

Mr. HOUGHTON. Well now, let me just go on to Mr. Schindel. Mr. Schindel, you wrote a sentence which is a sentence I've never seen before: "Treasury's ability to manage and accomplish successful Y2K conversion is a lot less uncertain today than it was a year ago." Tell me, what does that mean?

Mr. SCHINDEL. Congressman, what that means is that a year ago, I think that most of the agencies and Treasury were where a lot of other agencies were. They would have liked to have gotten started a lot sooner. So last year there were a lot of plans in place. An infrastructure was put in place to start managing the Y2K conversion, but we didn't have a lot of actual renovation and conversion of systems going on. That has substantially improved or increased since that time.

Mr. HOUGHTON. But, Mr. Schindel, if I could just interrupt, if I were the operating officer of the United States, and you said that to me, that would worry me. I expect you to do this job. And we don't get paid off on effort. And I understand some of the past problems, but we need to be sure that things are going to be all right. And I know you're in the auditing business, and I know that's important, but it is not a reassuring sentence.

Mr. SCHINDEL. Well, I think what it's meant to communicate is that between now and January 1, 2000, there's still some work to be done. But everybody is engaged in doing that. And until that work is completed, additional testing is done, there is still the potential that some systems could be Y2K non-compliant.

Mr. HOUGHTON. Mr. Chairman, I've just got one other question, if I could ask it.

Chairman ARCHER. Of course. Go right ahead.

Mr. HOUGHTON. All right. I'd like to ask this of Mr. Anderson. You say in your testimony in the last paragraph conclusion, that the banking industry alone cannot deliver business as usual in the year 2000, there must be parallel commitments by all other sectors of the economy. Are there any reasons to doubt that there are not?

Mr. ANDERSON. Mr. Chairman, or Congressman, we are looking at that very carefully, and we are dealing with our vendors and our service suppliers with our utilities and the telecommunication providers to ensure that they are taking appropriate actions and that the service that they are providing us will be made——

Mr. HOUGHTON. I'm sure you are, and that is very reassuring. However, do you see any real soft spots out there that we should be concerned with?

Mr. ANDERSON. Overall, I'm very confident. There may be glitches, but I think we will be able to overcome them so that the service to the individual consumer at least coming into the bank will not be interrupted.

Mr. HOUGHTON. Thank you, Mr. Chairman.

Chairman ARCHER. Mr. Tanner.

Mr. TANNER. Thank you, Mr. Chairman.

I was interested in your opening statement, Mr. Anderson. My grandfather was in the banking business back during the Depression. This fellow came in 1 day and withdrew all his money and said I just can't trust the banking system. A couple weeks later he came back, put his money back in. My grandfather asked him, what did you change your mind for?

He said, well I buried it in the backyard and I wore a path checking on it. He said any fool could have found it. [Laughter.]

My question following up on Mr. Houghton. Your comments, all of you, have been reassuring as has been said. What about your suppliers and those with whom you have Y2 compliant computer interaction that you must depend on. I mean, it's all right for you to be Y2 compliant, but those with whom you interact by computer, if they are not, the old adage, it takes two to tango in this business. Could you all comment on where you are with that and if you see any problem. Thank you.

Mr. APFEL. Mr. Tanner, it's a major priority that our partners, and there's not just one, there's lots, are connected to us and that everything is compliant. We identified 2,000 data exchanges, that's 2,000 partners. We must be able to assure that those systems are working in a positive interconnected way. Within Social Security, we've fixed all but 13 of those 2,000. The last 13 are not mission-critical, but we still want to get that resolved, and we will over the next 3 months. One of the key aspects of any agency is to determine what its data exchanges are, identify them, rank them, determine their mission criticality, and then go in and actually get it done. That is something that we have done. It's clearly one of the major undertakings that we went through over the course of last year.

Mr. ANDERSON. I may just add, from a banking point of view, we've gone through and made extensive inventory of all of the vendors and service providers that deal with banks, from systems and software providers to elevator operators and maintenance people, and we've gone back to each of them and tested their systems. Also, I should mention, and this should give the public a great deal of relief, that the Federal banking regulators are looking not only at banks but also at the major key vendors that provide data and technology services to banks. And they have found that 95 percent are compliant. In addition to that, we are working with them and doing our own testing with each of those vendors.

Mr. GREGG. The only thing I would add is what I said before. We have considerable redundancy built into our system so if we did have a problem in one location we could operate elsewhere. And we also have plans to have additional check stock on hand, more than we would normally have, just in case there was some kind of problem.

Chairman ARCHER. The gentleman's time has expired. Mr. English.

Mr. ENGLISH. Thank you, Mr. Chairman. Commissioner Apfel, I want to compliment you. Your testimony today is most reassuring, and it's a great testament to your proactive efforts to deal with this Y2K problem.

Referencing the remarks made by my friend and colleague from Wisconsin, I think it is incumbent on us to get the good word out,

particularly to Social Security recipients, that you have done a very good job of insulating them from potential disruption. And let me say, as my colleague from Wisconsin said, I wish C-Span were here today because I think this is a message that really needs to get out with the public.

I have one brief question that you can probably comment on relative to Mr. Willemssen's written testimony. He identified three key risk areas. One of them was having to do with support from the 54 State Disability Determination Services. I am wondering, are you now satisfied that those 54 State services are now on track to be Y2K compliant and to support your efforts to keep the disability program on track?

Mr. APFEL. The answer to that, Mr. English, is yes. It's not only on track, it's done. The disability determination services (DDS) systems have completed their operation. I would also point out that the General Accounting Office also laid out three areas that we needed to continue to work on. One was data exchanges, and as I indicated, we have another 13 non-mission-critical systems to do. So I think we are very much on track in that area. The second one was any new systems changes that we make need to be recertified, if we do make any systems changes. And, of course, there will be some, given say, the COLA announcement. We intend to do that. That is our plan, which is consistent with GAO's recommendation. And third, there is the need for contingency plans, which we are on track to do.

Their original report identified the DDS activities as being critical, which they are, but I again assure you those activities are done.

Mr. ENGLISH. Thank you. Thank you again for your testimony.

Chairman ARCHER. Ms. Johnson.

Mrs. JOHNSON of Connecticut. Thank you, Mr. Chairman. I think it is fair to say that, given the human resources that you have dedicated to this problem and the monetary resources, and the general inventiveness of the American people when faced with a challenge like this, you are going to be able to meet across the board in the public and private sector the Y2K problem head-on. And the problems that we are going to encounter are going to be narrow and localized, I think, across the Nation.

There are two things specifically that I would like inquire about. First, Mr. Apfel, when the Social Security system began end-to-end testing, which I think was before you became the head of the office——

Mr. APFEL. Well the end-to-end testing was actually completed 2 to 3 months ago.

Mrs. JOHNSON of Connecticut. OK. On your first test run, how many problems did you find? On your second test run, how many problems did you find? How many runs did it take of end-to-end testing, which is an extraordinary challenge in and of itself, before you got to where you felt the system really was going to serve you, was reliable?

Mr. APFEL. There were some problems identified, and I will get you for the record a list of the specifics. There were not very many. Back last July and August, a lot of the runs were started to determine the efficacy of the system. There were a few minor problems,

and I will for the record document those for you so that you have them.

The Social Security Administration initiated detailed planning discussions with the Financial Management Services of the Treasury Department of Year 2000 end-to-end testing in March 1997. The software changes were implemented at SSA and Treasury in August–September 1998. We feel that the key to our success was that we allowed adequate time (a year) for planning, requirements, development and internal testing before we conducted the agency to agency validation with Treasury and the Federal Reserve. the validation ran from March 1998 through July 1998, with files being passed to the Federal Reserve for final validation during July.

During the planning for testing and validation, we recognized that it was necessary to provide time for reruns. It usually takes several runs to complete a validation successfully, and one should not plan on one test run being sufficient. Both agencies allowed adequate time for internal testing and the result was that the software we used for the March–July 1998 agency-to-agency validation produced few problems.

There were two areas where we encountered challenges, but they both had to do with setting up validation rather than the quality of the software:

1. Naming the test files (data set names) in order to get the files through both SSA's and Treasury's TOP SECRET telecommunications security systems.

2. Keeping SSA's validation data base synchronized with Treasury's data base required a great deal of effort and more time than we had anticipated.

Both of these challenges were overcome, and we were able to complete the testing within our original schedule.

But by the end of that period of time, we were confident that we could move to independent external testing. And that is what took place with FMS, with the Fed, end-to-end testing from us through FMS into the Fed.

Mrs. JOHNSON of Connecticut. Now when you—the problems that you found in your early systems testing, what was the effect of those problems? Did they infect other areas, or were they very system-specific or site-specific? In other words, did a problem in one office bring down the system throughout the country?

Mr. APFEL. No. It was not like we discovered that one field office has a particular problem. It was an integrated test to look at the comprehensive delivery of that system.

Mrs. JOHNSON of Connecticut. But in looking at that, did you find that then one problem in one aspect of the system would bring, would stop the whole system?

Mr. APFEL. No, we did not. It was——

Mrs. JOHNSON of Connecticut. Because I think what we're going to face is, very significant departments, I have in mind Medicare, not beginning end-to-end testing until October or November or 1999. So it's important as you go throughout, and unfortunately my time has expired and some of you might want to come back to this, what you expect when you get to end-to-end testing in other agencies in terms of whether the problems will be isolated and how we will manage them and what are the implications of end-to-end test-

ing beginning so late in a number of significant services across the government.

Thank you, Mr. Chairman.

Chairman ARCHER. The Chair would appreciate it, and we still have a number of Members to inquire. The Chair would appreciate it if Members would make every effort to stay within the 5 minutes because we have a lot of witness today before we get through. And having said that, the Chair recognizes Ms. Thurman.

Mrs. THURMAN. Thank you, Mr. Chairman.

Mr. Anderson, let me ask a question. A lot of people through the Internet, think the sky is falling over this issue; how are you reaching your customers to let them know that you don't believe there will be any interruption within their service?

Mr. ANDERSON. We're doing a number of things. We've developed a comprehensive plan for our customers that we actually started about a year ago. We've had four mailings to them. This includes statement stuffers that explain the problem, explains what the bank is doing. It also gives them suggestions on what they can do to prepare for themselves.

This is a problem that not only the banks have but they may have at home. And so if they're on the Internet, they need to make sure, for example, that their home computer is Y2K compliant, and they need to make sure they have backup to the data on there. The ABA has videos, they have statement stuffers, they have ads, they have seminars that are available that the banks can use throughout the area.

I would also personally encourage you and all Members of Congress to meet with your banks and go on a tour of their facilities and see that they in fact are getting ready for Y2K. And get the publicity that that would bring. That would be a tremendous benefit.

Mrs. THURMAN. Do you see a possibility, or is there a potential problem if people do start making a run on the bank toward the end of 1999? What could happen?

Mr. ANDERSON. Well, I think that's one of the reasons why the Federal Reserve has said that they are printing $50 billion in extra cash so there will be plenty of cash in the system. But what we really want to do is through communication, to let our people know, our customers know, that in fact that's not the smart thing to do. And that in fact, their money is safer in the bank than in the ground or under their mattress. [Laughter.]

Mrs. THURMAN. And I'm glad to hear that because I am a little concerned about that just from what you hear on radio talk shows and some of the things people are doing to prepare.

Mr. Apfel, have you had many people within the Social Security system who are recipients asking about changing from electronic transfer to a mail, based on this issue at all?

Mr. APFEL. No. The increase continues in electronic transactions. So we're not seeing a number of people wanting to go back to paper, which I think could be a real mistake. Moving an electronic transaction is really the safest for beneficiaries and cheapest for cost. So its a very good thing.

Mrs. THURMAN. That's why I want this discussion because I think the American public does need to realize that.

Mr. Anderson, last question, I know you represent the bankers, but what about independent, rural, and bankers of that nature. Do you see them in the same mode as you, as the American Bankers Association as versus independents?

Mr. ANDERSON. Yes. In fact, the banking regulators have examined all banks, and of all banks, 97 percent they found have received the highest rating. Only 17 out of the 10,000-plus have had any problems.

Mrs. THURMAN. Thank you.

Chairman ARCHER.

Mr. Weller.

Mr. WELLER. Thank you, Mr. Chairman, and, Commissioner, it is good to see you again. You probably feel like you haven't left because of the hearing going late last evening.

Mr. APFEL. I slept here last night. [Laughter.]

Mr. WELLER. I appreciate your good work.

I would actually like to address my question to the spokesman for the banking community, and I really want to commend your efforts focusing on communication and education for your customers because, as folks back home slowly become more and more aware and concerned about the year 2000 problem, there are going to be folks that are going to be afraid. And your efforts to reassure your customers will be important, particularly as we may expect those in the entertainment industry to produce TV shows and movies that may cause some concern, and hopefully not panic, but take advantage of this landmark time.

The question that I have for you is, you noted in your testimony that at the end of each month that financial institutions issue a monthly report. Has some thought ever been considered into issuing your usual monthly statement on December 31, but also printing a second one on January 1 after midnight so that your customers can take their December 31 statement and compare that to their January 1 statement and see whether or not there are any changes of differences that should not be there?

Mr. ANDERSON. That is a very good comment, and we have considered it. What we are doing at Zion's Bank, at my bank, is that in the December statements that are mailed out, we will have a card that will ask the customers if they want an additional cutoff statement that will come actually as of December 30. And those who want one, we will prepare it. We will also let them know that they can go to any ATM machine throughout the month of December, and they can get a mini-statement which gives them their last 10 transactions and their balance. And so, with that information, we feel they should be confident that when they get their January statement that they can match it up, and, if there are any issues, they can come back and we can correct them.

That is the nice thing about the banking industry, we do have a lot of backup information that helps us identify and correct problems when they occur.

Mr. WELLER. But you are saying that service would just be available in December and would not be available in January, because, after midnight is January.

Mr. ANDERSON. Right.

Mr. WELLER. Would that service be available after January 1?

Mr. ANDERSON. Congressman, we haven't thought of doing it on January 1. Normally the statements start going out on the third of January, so they will be getting their statements toward the first of the month. As we have looked at the problem, we thought it important that they have a cutoff statement as of the end of the year that they can compare to their statement that comes out in January.

Mr. WELLER. But the January statement is usually the December 31 printout, isn't it?

Mr. ANDERSON. Right. But usually the statements for November come out the first of December, and then the next statements would come out the first of January. And, as we have done focus groups with our customers, we have found out that what they want to know, is, as of the end of December, what is their balance. They want something more current than the November 30 statement that came out the first of December. They want something close to the end of the year so that when they do get their statements in January, they can compare it to to see if there are any glitches.

Mr. WELLER. I realize I have run out of time here, but the point that I am trying to make is that the end of December is midnight. The concern that I have heard back in Illinois is what happens after midnight. They want a January statement. They are anxious to know what their bank balance is on January 1, after midnight, compared to December 31. So, I would ask that you take a look at it—figure out some way that people have an opportunity to compare what happens after midnight versus what was in the account before midnight.

Mr. ANDERSON. That is a good suggestion. We will do that.

Chairman ARCHER. As is generally true, the gentleman from Illinois is correct, he is out of time. [Laughter.]

Mr. Lewis.

Mr. LEWIS. I have no questions, sir.

Chairman ARCHER.

Mr. Foley.

Mr. FOLEY. Thank you, Mr. Chairman.

About 2 months ago we were in Brussels discussing, with our European counterparts, the Y2K problem, and there seemed to be a lack of interest in pursuing corrective remedies. In fact, they seemed to give it short shrift when we discussed it. Can you give us an illumination from the banker's perspective about that type of concern that we may have, and, due to the global nature of our economy, due to the currency changes, the introduction of the Euro, and all the other things that may become important, do you see that having an impact? Even though we, domestically, may be ready, what happens with our European counterparts?

Mr. ANDERSON. That is a very good question. That is a very complicated question, and, if it is all right, I would like to respond in writing to you on that, for the record.

Mr. FOLEY. OK. Commissioner?

Mr. APFEL. Mr. Foley, I would think that Mr. Koskinen would be the perfect person for that question. From a Social Security perspective, our focus here is the 300,000 individuals who receive payments overseas. About 100,000 of those are direct deposit and

about 200,000 are through the mail. That is where we are developing our contingency plans.

I don't think that I have the expertise to comment on the broader issues that you raise, sir.

Mr. FOLEY. Does anybody else on the panel have a comment?

Mr. WILLEMSSEN. If I may comment, sir.

From a worldwide perspective, those countries generally considered to be furthest out front, in addition to the United States, include the United Kingdom, Australia, Canada, and a couple of other countries. Beyond that, you really have a next lower tier. Even some of the industrialized countries, such as Germany and Japan, are not, from a readiness perspective, where we and some of those other leaders are.

I think, particularly in the banking area, Japan was considered to be lagging somewhat, and that may have been one of the reasons for some of the delays in some of the international bank testing that was planned for later this year. I understand that they are now in the midst of catching up, and I don't know if you want to add to that in terms of the testing that is planned for later this year from an international perspective.

Mr. FOLEY. I would be delighted to receive written response, because I do think that it has some real implications with arbitrage, currency fluctuations, changes of various and sundry objectives.

And then there will be further—my time is about up—but I would also like to look at the Defense Department's Y2K issues and how it interacts with defense capabilities and the information that we share with our allies.

Thank you, Mr. Chairman.

Chairman ARCHER. The gentleman's questions are very probative, but the Chair would advise members that our effort here today—and we have got a long list of witnesses—is to concentrate on those areas that are within our Committee's jurisdiction. I hope that we can limit the questioning to that.

Mr. Hulshof.

Mr. HULSHOF. Mr. Anderson, as you can gather from all the questions being propounded in your direction, we have been hearing a lot from our constituents about the efforts that you have made. I do want to commend you. Mrs. Thurman asked about the education efforts that you have made to your customers, our constituents, regarding Y2K and why this should not be a problem.

Let me take it just one step further, have you also, in this education effort, communicated to your customers things that the banking industry has learned in dealing with this Y2K problem that they find of benefit? Maybe that is not the role of your industry, but perhaps things that you could communicate to your customers as to how they might be in their personal work or home become Y2K compliant?

Mr. ANDERSON. Well, we have. We have tried to provide them information and a checklist of things that they should do. ABA has provided that information to all banks.

For example, we have encouraged our customers to keep copies of their bank statements and their receipts and their loan payments so that they have a record. You see, this is a good chance for our customers to get organized from a financial point of view

so that if there are glitches, they can come back and correct it. It is always easier when they have the data there in front of you.

We have told our customers that we are providing and we are doing backups, so that, if there is a glitch, we can go to our backup files and pull out information and make corrections as necessary.

Mr. HULSHOF. Mr. Gregg, what a difference a year makes. A year ago, when this Committee convened, and we talked about the efforts, obviously as we have talked about already, the situation regarding financial management services was a concern to a lot of us. And, God forbid that we be here a year from now, still talking about Y2K because those generators will have been running, I think, for 2 months, instead of 2 weeks, as we have talked about.

Has FMS worked with IRS or other Federal agencies to do end-to-end testing as you have done with the Commissioner and the Social Security Administration, and, if so, have any of those processes been certified as Y2K compliant?

Mr. GREGG. We have plans to do the same thing with IRS and VA that we did with Social Security. The systems, as I mentioned, for most of the payments for VA are already running on Y2K-compliant systems, and, since last July, the IRS payments have been going out on Y2K-compliant systems. But we do plan to do some more testing with the major agencies over the next few months.

Mr. HULSHOF. OK.

That is all I have, Mr. Chairman. I yield back my time.

Chairman ARCHER.

Mr. Portman.

Mr. PORTMAN. Thank you, Mr. Chairman.

Mr. Apfel, I am the father of two elementary school students who bring home their report cards every now and then. I am rather efficient at looking at report cards, and I want to give you a star for your GAO Subcommittee report card this time around. Except, you went from an A+ to an A, and you like to see improvement.

But I guess that your other agencies haven't done quite as well, and we are going to hear from the IRS later today. For the last couple of years, we have been following the IRS very closely on this Committee and on the Subcommittee. And I remember a statement being made about 18 months ago that it was a marathon that needed to be run at a sprinter's pace.

I guess my question is really to Mr. Gregg, and to Mr. Schindel would be with regard to the IRS—and we will hear from them later directly—but do you believe that the sprint is continuing and that they are going to make the deadline?

Mr. SCHINDEL. We have not done work directly, out of the Treasury IG's office on IRS. That was done by GAO and the IRS inspection service. But, in our meetings with them, and in the information that they have fed us, the IRS is proceeding on target. Of course, they have a massive, and perhaps a bigger, renovation effort than a lot of other agencies, hundreds of thousands of lines of code, but they are making progress.

Mr. PORTMAN. With regard to Social Security, Mr. Apfel, are you here today to tell us that you are confident that recipients in the year 2000 will indeed be receiving their benefits?

Mr. APFEL. Yes, sir, I am.

Mr. PORTMAN. And, Mr. Willemssen, do you agree with that? Do you have that confidence with regard to the Social Security program?

Mr. WILLEMSSEN. I have as high of a degree of confidence as you can have without giving a 100 percent guarantee. That is why I would also say we focus on contingency plans because we can't give an absolute guarantee that there won't be some systems failures, and, in the event of those failures, they need those backup plans.

Mr. APFEL. That is an absolute correct response. That is the purpose of our contingency plans.

Mr. PORTMAN. Another question—and I appreciate your confidence—with regard to resources. Again, in the last Congress, we added significant resources to the Y2K effort, in part because of Social Security and IRS and other agencies. Are you comfortable with the amount of resources that this Congress has provided and that this Committee is supporting?

Mr. APFEL. From our perspective, we have sufficient resources for this issue.

We did not receive money from that supplemental, incidentally. We funded that entirely through our ongoing operations.

Mr. PORTMAN. But do you believe that your resources are sufficient?

Mr. APFEL. Absolutely. But if that changes at any time, I would absolutely let you know immediately. But I am very confident.

Mr. PORTMAN. I am sure that you will.

Thank you, Mr. Chairman.

Chairman ARCHER. The Chair believes that all members present have inquired. And, as a result, the Chair is extremely grateful for you all giving us some insight into your involvement in the Y2K problem, and we are also very comforted to know that we are moving forward to where we will not have any disruption, and, if there is any failure, there are contingency plans so that services, the essential services, will be there in January of next year. And that, to me, is the important message that you have given us today.

So you gentlemen are excused.

Mr. Apfel.

Mr. APFEL. Just one small point: Chairman Shaw asked about some information that was to be provided by the Social Security Administration to the General Accounting Office. I indicated that I would look into it. The answer is that the information has already been provided to the General Accounting Office, and that issue is resolved. I wanted to say that for the record.

Chairman ARCHER. Thank you very much. And again, I thank all of you.

And while Mr. Koskinen is moving to the witness chair—it is the Chair's intention to recess at 12 noon for 1 hour at lunch and to return at 1 o'clock, so witnesses and members can adjust their schedules accordingly.

Mr. Koskinen, you are really sort of the umbrella organization working for this entire problem and working for the President, as I understand it, and I believe that your official title is Chairman of the President's Council on Year 2000 conversion. Is that correct?

Mr. KOSKINEN. That is correct, Mr. Chairman. I am also fondly known as the bag holder. [Laughter.]

Chairman ARCHER. Well, you have an enormous responsibility. And, I am sorry that we had to proceed before you got here this morning, because I know that you have a tight schedule, and I appreciate your staying with us. I hope that members will expedite their questions.

We are very pleased to have you with us, and I hope that you can limit your verbal presentation to 5 minutes. Your entire written statement, without objection, will be printed in the record. We will be pleased to have your testimony. You may proceed.

STATEMENT OF HON. JOHN A. KOSKINEN, ASSISTANT TO THE PRESIDENT, AND CHAIRMAN, PRESIDENT'S COUNCIL ON YEAR 2000 CONVERSION

Mr. KOSKINEN. Thank you, Mr. Chairman, and my apologizes for the traffic delays that caused me to show up here late.

I am pleased to appear before the Committee to discuss the activities of the President's Council on Year 2000 Conversion, and the status of public and private-sector efforts to address the year 2000, or Y2K, problem.

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

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

Working group outreach efforts are designed to increase the level of action on the problem and to promote the sharing of information between entities. The outside organizations in each sector have also agreed to conduct Year 2000 readiness surveys of their members which they share with us and the public.

As you just heard, we have also created a Senior Advisors Group to the President's Council, comprised of Fortune 500 company CEOs and heads of national public-sector organizations representing our working groups. The Group provides the Council with an additional perspective on Y2K challenges that cut across sector lines and recommends how industries can best work together in these critical areas.

You have already heard from one member of that group, and you will hear from the other, Mr. Brown of BJC Healthsystems, who represents the hospital industry. Mr. Anderson, who you heard from earlier, represents the banking industry. We appreciate the willingness of these gentlemen and their organizations to work with us to address the Year 2000 problem.

Our first challenge is to ensure that Federal systems are prepared for the Year 2000. These are the systems for which we are

responsible and have the authority to fix. I am pleased to report that the Federal Government continues to make strong, steady progress in solving its Y2K problems. According to the most recent agency data, as of January 31, 1999, 79 percent of all Federal mission-critical systems are now Year 2000 compliant—more than double the 35 percent compliant a year ago. The data also show that, of critical systems requiring repair work, 96 percent have been fixed and are now being tested.

The President has established an ambitious goal of having 100 percent of the government's mission-critical systems Y2K compliant by March 31, 1999, well ahead of many private-sector system remediation schedules. Although much work remains to be done, we expect that close to 90 percent of the government's mission-critical systems will meet the March goal, a tribute to the hard, skillful, and dedicated work of thousands of Federal career employees.

We also expect that all of the government's mission-critical systems will be Year 2000 compliant before January 1, 2000.

The Social Security Administration, whom you just heard from has been a leader in Federal agency Y2K efforts. SSA is virtually done with its work and is now focused, appropriately, on contingency planning. The Treasury Department, including the IRS, the Customs Service, and the Financial Management Service, has some of the most complicated systems in the Government which serve millions of Americans. New managers, particularly at the IRS and FMS, have done a very effective job of managing the process. At the IRS, Commissioner Rossotti, has helped his agency to master what many thought would be an insurmountable task. And we are confident that the IRS will have completed most of its work on mission-critical systems by the end of this March. You will hear more details from HCFA about the challenges that they face as they move forward.

Our second challenge is to work with the Federal Government's interface partners, primarily the States, as they work to ensure that their systems are ready for the Year 2000. States administer over 160 Federal programs that provide some of the most recognizable Federal services, such as unemployment insurance, Medicaid, and food stamps. As a general matter, most States are making good progress in remediating their systems. And, according to the National Association of State Information Resource Executives, several States have reported that they have completed Y2K work on more than 70 percent of their systems.

Unfortunately, not every State is doing as well. The same NASIRE survey indicates that a handful of States report that they have not yet completed work on any of their critical systems. For its next quarterly report, to be released next month, OMB has asked Federal agencies to provide information about each State's Y2K progress on 10 key, State-administered Federal programs such as Food Stamps and Unemployment Insurance.

The third challenge for the President's Council was to reach out beyond the Federal Government and its partners to those organizations whose system failures could have an adverse effect on us all. Last month, we issued our first quarterly summary of assessment information across these key sectors. And I would like to conclude by making three key points about what we know thus far.

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

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

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

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

We believe, therefore, that everyone working on this problem, at the Federal level, at the State and local level, and in the private sector, needs to provide the public clear and candid information about their Year 2000 activities. That is why we are making industry surveys available to the public. That is why the OMB reports on Federal agency progress are provided not only to Congress but to the public. That is why we have created a toll-free information line for consumers and constituents across the country. And that is why we will provide the details of the Government's Y2K contingency planning and will encourage others to do the same. A corollary principle is that everyone working on this problem has a responsibility that their comments accurately reflect the factual information available and that they avoid over generalizations that will only play into the hands of those who want to create panic for their own gain.

We remain committed to working with this Committee and the full Congress on this critical issue, and I would be pleased to answer any questions that you might have, Mr. Chairman.

[The prepared statement follows:]

Statement of the Hon. John A. Koskinen, Assistant to the President, and Chairman, President's Council on Year 2000 Conversion

Good morning. I am pleased to appear before the Committee to discuss the activities of the President's Council on Year 2000 Conversion and the status of public and private sector efforts to address the Year 2000 (Y2K) computer problem.

Mr. Chairman, I would like to start by thanking you and the other members of the Committee for your ongoing interest in the Y2K problem and its potential implications for beneficiaries and taxpayers.

Businesses and governments across the country are engaged in vigorous efforts to ensure that systems are prepared for the date rollover. It is a vast challenge, and not every system will be fixed by January 1, 2000. While progress is being made in the public and private sectors, continued efforts are necessary if we are to achieve our shared goal of minimizing Y2K-related disruptions.

THE THREE-TIERED APPROACH

The Y2K problem is a layered problem. It's not enough for the Federal Government, or any organization, to fix its own systems. Organizations also need to be con-

cerned about the progress of partners they exchange data with and depend upon as well as progress among other organizations whose failure could have a significant effect upon their operations.

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

The Council's more than 30 agencies, including several independent regulatory agencies, work together to exchange information on agency Y2K progress and shared challenges. They also coordinate interagency testing efforts for programs that rely upon multiple agency systems and assist each other with contingency planning efforts.

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

We have also created a Senior Advisors Group to the President's Council, comprised of Fortune 500 company CEOs and heads of national public sector organizations representing our working groups. The Group provides the Council with an additional perspective on Y2K challenges that cut across sector lines and recommends how industries can best work together in critical areas. You are scheduled today to hear from two members of this Group. Scott Anderson of Zions National Bank represents the banking industry and Fred Brown of BJC Health Systems represents the hospital industry. We appreciate the willingness of these gentlemen and their organizations to work with us to address the Year 2000 problem.

Materials describing our working groups and the Senior Advisors Group are available on the Council's web site—*www.y2k.gov*.

FEDERAL AGENCY PROGRESS

Our first challenge is to ensure that Federal systems are prepared for the Year 2000. These are the systems for which we are responsible and have the authority to fix. Consequently, it is the area about which we have the most information. Agencies report quarterly to the Office of Management and Budget (OMB) and Congress, and the OMB summary reports on agency Year 2000 progress are available on the Council's web site. I am pleased to report that the Federal Government continues to make strong, steady progress in solving its Y2K problems.

According to the most recent agency data, as of January 31, 1999, 79 percent of all Federal mission-critical systems are now Year 2000 compliant—more than double the 35 percent compliant a year ago. These systems have been tested and implemented and will be able to accurately process data through the transition from 1999 into the Year 2000. The data also show that, of critical systems requiring repair work, 96 percent have been fixed and are now being tested.

The President has established an ambitious goal of having 100 percent of the Government's mission-critical systems Y2K compliant by March 31, 1999—well ahead of many private sector system remediation schedules. Although much work remains, we expect that close to 90 percent of the Government's mission-critical systems will meet the March goal, a tribute to the hard, skillful, and dedicated work of thousands of career Federal employees. Monthly benchmarks with a timetable for completing the work will be available for every critical system still being tested or implemented after March. And we expect that all of the Government's critical systems will be Y2K compliant before January 1, 2000.

Although you will hear more from all of them later today, let me say a few words about some of the agencies that are of particular interest to this Committee—the Social Security Administration (SSA), the Treasury Department, and the Department of Health and Human Services (HHS).

As you know, Mr. Chairman, the Social Security Administration has been a consistent leader in the Federal Government's Year 2000 efforts. SSA chaired the first interagency committee on Y2K in 1995 and has been an active participant on the President's Council, sharing useful guidance with the other agencies on best practices for remediation, testing, and contingency planning. In December, after we were

informed that Treasury's Financial Management Service (FMS) had completed its work in this area, the President announced that the Social Security payment system is now Y2K compliant. And according to the most recent data, SSA has now completed work on all of its mission-critical systems.

The Treasury Department, which includes the Internal Revenue Service (IRS), the Customs Service, and the Financial Management Service, has some of the most complicated systems in the Government which serve millions of Americans. In particular, the IRS and FMS have faced difficult Y2K challenges. But the new managers in those agencies have done a very effective job in managing the process. At the IRS, Commissioner Rossotti has helped his agency to master what many thought to be an insurmountable task, and we are confident that the IRS will have completed work on most of its critical systems by the end of March.

HHS continues to confront some of the most unique information technology challenges in the world. The Department's efforts are complicated by the fact that the Medicare system is very dependent on the private sector for its operations. The Health Care Financing Administration (HCFA) has had to work in concert with roughly 60 large insurance companies who were not all initially responsive to the need to meet Government goals that, in most cases, required compliance earlier than their private sector customers. But they are making progress. And although significant systems work and contingency planning will remain after March, most Medicare contractors are expected to complete renovation and testing by the Government-wide goal. HCFA is also making substantial progress on its internal systems, as you will hear from Administrator Min DeParle.

INTERFACE PARTNERS

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

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

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

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

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

Our joint Y2K efforts with the States are bearing fruit. Working together, we last month overcame one of the first major examples of a "look ahead" Y2K problem. The Unemployment Insurance program, a major Federal-State partnership administered by 53 State Employment Security Agencies (SESAs), encountered the Year 2000 problem on January 4. Since new claims are calculated on a 12-month basis, State systems had to process dates going into January 2000. The Labor Department had been working closely with all the States to ensure that they could continue to proc-

ess claims and provide benefits through this transition, particularly the 16 SESAs that had not completed all of their Y2K system renovation before January 4, 1999. Thanks to this collaborative effort, these SESAs were prepared with, and are now using, temporary fixes to their systems so that they can continue to accept claims and process benefits while they complete their remaining Y2K work. The Department has also instituted special reporting procedures for the Unemployment Insurance program to identify any early problems. Reports have been received from all States and indicate that no Y2K-related service disruptions have occurred.

BEYOND THE FEDERAL GOVERNMENT

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

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

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

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

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

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

If the head of an organization has fixing the Y2K problem as a top priority, that organization is by definition going to be better prepared—even if it cannot fix all of its systems before January 1, 2000. It is organizations where the leadership is convinced that the problem doesn't apply to them or that they can simply fix systems when they break that are of most concern.

Of all the industry sectors, health care presents some of the most difficult outreach challenges. As you know, it is a diverse industry that covers everything from hospitals and long-term care facilities to pharmaceutical companies and retailers. Many health care providers and companies are free-standing entities and are not active participants in national organizations like the American Hospital Association (AHA) and others with whom the Council has working relationships. The diffuse nature of the industry has prompted us to divide the outreach responsibilities of the Council's Health Care Working Group into three main areas—medical devices, health care facilities, and pharmaceuticals.

Under the leadership of the Food and Drug Administration, and with active participation by the Department of Veterans Affairs and the Defense Department, the Government has been collecting and publishing information about the Year 2000 compliance of medical devices. Companies were initially reluctant to take part in this process, but the level of participation has increased significantly in the last few months. Fortunately, the vast majority of medical devices do not have Year 2000

safety concerns, and many are not affected by the date rollover. Nonetheless, we are concerned about and are focused on providing to all health care providers information about the small number of devices with Y2K problems that could compromise patient safety.

HHS is working with the AHA, the Joint Commission on Health Care, and others to assess the status of Y2K efforts within health care facilities and to encourage information sharing within this segment of the health care industry. At this juncture, we are particularly concerned about smaller health care facilities, many of whom may lack the resources to deal with the problem.

Under the leadership of the VA, the Council is working with the pharmaceutical associations, who have been focused on developing assessments of industry preparedness. We will also be gathering more information about the pharmaceutical supply chain, which fortunately does not operate on a strictly just-in-time inventory system and has reserve capability built into the process. We are looking forward to working with these groups to provide information to the public about the adequacy of prescription drug supplies as we move toward the end of this year.

AREAS OF RISK

Following the logic that our greatest risk lies in organizations where for one reason or another the leadership does not have the Year 2000 problem as a high priority, I believe that at this time our greatest risks are in three areas: smaller government entities, small businesses, and internationally.

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

Many small- and medium-sized businesses are also taking steps to address the problem and to ensure not only that their own systems are compliant but that organizations they depend upon are ready for the Year 2000 as well. But a significant number of small- and medium-sized businesses are not preparing their systems for the new millennium. A recent National Federation of Independent Business (NFIB) survey, released this month, indicates that as many as one-third of small businesses using computers or other at-risk devices have no plans to assess their exposure to the Y2K problem. The survey also indicates that more than half of small firms have not yet taken any defensive steps. The NFIB and other small business surveys have found that having adequate resources for addressing the problem is not the concern. Rather, a significant number of small businesses appear to taking a "wait and see approach" on whether or not their systems will be affected by the Y2K problem. We are trying to get them to understand that this is a high-risk strategy.

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

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

Internationally, the Council worked with the United Nations to organize in December a meeting of national Year 2000 coordinators from around the world, perhaps the most important Year 2000 meeting to date. More than 120 countries sent representatives to New York. The delegates at the meeting agreed to work on a regional basis to address cross-border issues (e.g., telecommunications, transportation). They also asked the steering committee we had created to help organize the meeting to establish an international mechanism for coordinating regional and global activities, including contingency planning. Earlier this month, the steering committee announced the creation of the International Y2K Cooperation Center, which will support regional activities and international initiatives in areas such as telecommunications and transportation. The World Bank will support the advisory and planning activities of the Center through voluntary donations.

CONTINGENCY PLANNING AND EMERGENCY RESPONSE

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

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

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

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

THE BALANCING ACT

Let me close by noting that we all continue to confront the challenge of encouraging organizations to take the Y2K problem seriously, remediate their systems, and prepare contingency plans without causing a public overreaction that is unnecessary and unwarranted.

Our strategy is based on the premise that the public has great common sense and will respond appropriately when they have the necessary information.

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

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

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

Chairman ARCHER. Thank you, Mr. Koskinen.

Is there any reason why any essential Federal services will be disrupted in January in the year 2000?

Mr. KOSKINEN. There is no reason to expect, based on the information that we have now, that there will be any national failures. But, as I noted, we are concerned about some small- and medium-sized organizations in the private-sector and in the public-sector that are not paying appropriate attention to the problem. And we think that the risks of outages, if there are any, will be at the local level—with local power plants, local telecommunications companies, local water treatment companies.

Chairman ARCHER. Are there contingency plans to wire around any possibility of disruption in those areas?

Mr. KOSKINEN. Contingency plans are being developed for the vast critical systems that we all depend on nationally. But, again, our concern is organizations that are not paying appropriate attention to the problem at the local level. If organizations are not paying attention to fixing the problem, it is likely that they are also not paying attention to ensuring that they have appropriate workarounds.

Chairman ARCHER. At the Federal level, has the Congress given all of the resources necessary to solve this problem?

Mr. KOSKINEN. Yes. The Congress has been very supportive both financially and, last year, with the passage of the Information Readiness and Disclosure Act which is designed to increase the flow of voluntary information about fixes as well as about readiness.

Chairman ARCHER. Should you find that there is any other desperate need that occurs this year, we invite you to let us know immediately so that we can attend to it.

Mr. KOSKINEN. Thank you, Mr. Chairman, I appreciate that. And I would reiterate again that we have had nothing but the closest and the most supportive cooperation from the full Congress.

Chairman ARCHER. And we want to keep it that way from our part of it.

Mr. Coyne.

Mr. COYNE. Thank you, Mr. Chairman.

Mr. Koskinen, I wonder if you could expand upon your response relative to reports that one-third of small businesses that use computers in their businesses have not assessed their exposure to the Y2K problem, and that about one-half have not taken any defensive steps to this point. I know that you touched on it, but I wonder if you could expand on this?

Mr. KOSKINEN. We just had a trilateral meeting with the Year 2000 coordinators from Canada and Mexico on Monday and Tuesday of this week. And their experience, as is ours, is that the issue with small businesses is actually a problem around the world. Smaller organizations tend to assume that this problem doesn't effect them because they are not running major main frames. Or, increasingly, as they become aware of the problem, their judgment is that they will wait and see what breaks and fix it afterward. We are doing everything we can to advise them that is a very high-risk strategy because if they wait until it breaks and then try to fix it, they may be at the end of a very long line of people who took a similar action.

So we, along with the SBA and the Commerce Department, did a national Y2K action week for small businesses in October. And the SBA, the Agriculture Department, and Commerce's Manufacturing Extension Partnership are planning another full-court press at the end of March to hold seminars and provide technical information to all the small businesses that we can get to show up at the meetings. Our problem is—not that small businesses don't have the resources—many are basically saying that they will just wait and see.

Mr. COYNE. You have sort of imposed a 90-percent completion by March 31 of your efforts in your testimony there. I wonder how you are going to notify Congress whether or not you are 90-percent compliant by March 31.

Mr. KOSKINEN. OMB has provided, for the last 2 years, quarterly reports to Congress. The March report actually reflects progress as of January 31. The next report will contain information as of April 30. But for the agencies with the major challenges, we have been getting monthly reports. The reports for March 31 will be in to OMB in mid-April, and we will make that public and advise you as to where the agencies are.

Mr. COYNE. And, at that point, you expect to be 90-percent compliant? Hopefully, 100 percent?

Mr. KOSKINEN. No, I think that we will be over 90 percent. We expect that there will be a handful of mission-critical systems in several agencies that will be monitored on a monthly basis, but there is no indication that they won't be ready, all of them, well in advance of the Year 2000.

Mr. COYNE. What are your concerns with regard to State and local governments' computer systems?

Mr. KOSKINEN. Our concern, again, as I noted in my formal testimony, is in those organizations where the head of the organization does not have the problem as a high priority. So, we have been stressing, not only to Governors, but to county executives, mayors, and city managers, that the Year 2000 problem has to be their priority because that is the only way you can send appropriate signals to the people in your organization. It is more than just an IT problem, it is a management problem. The cities and towns that think they need only to focus on software problems have not understood the impact that this may have on water treatment plants, on local community hospitals, or on local 911 systems.

So, our risk and concern is not with those organizations working hard on the problem. Our risk and concern is for those who have decided for one reason or another, that they are not going to pay attention.

Mr. COYNE. Thank you.

Chairman ARCHER. Mr. Crane.

Mr. CRANE. Thank you, Mr. Chairman.

Mr. Koskinen, how do you respond to Edward Yardini and others who predict an international economic crisis that will result from Y2K, and what else can be done that is not being done to prevent such a crisis?

Mr. KOSKINEN. I have talked to Mr. Yardini, and, as I have made clear several times, he knows a lot more about economics than I ever will. He is very thoughtful and constructive. But he is really

the only major economist that takes that position. I have met several times with the Council of Economic Advisors staff and the NEC, and the recent Economic Report of the President noted that the consensus of economists is that this problem will have a relatively modest effect on GDP now, no more than two or three-tenths of a percent.

We all know that the proof will be in the pudding, but at this juncture, there is no indication on the basis of what we know either internationally or domestically, that we will have a major economic recession or worse as a result of Y2K problems. That does not mean that there will not be problems. It simply means that those problems, particularly internationally, will not by themselves send us into a recession.

Mr. CRANE. And what can Congress do that it is not doing already to help ensure that there are no major Y2K-related failures? And I am thinking in terms of funding and legislation authorizations, oversight.

Mr. KOSKINEN. I think that oversight hearings like this one are very productive and important in terms of providing more information to the public. As noted earlier, one of our issues is to try to get the public to understand exactly where the risks are and where they are not. But at this juncture, we do not have a need for any other major legislative initiatives.

We appreciate Congress' support last year for the information sharing act. At this juncture, I think the responsibility for Federal systems is on us and on each of the cabinet Secretaries. Increasingly, one of the messages that we are trying to drive home is that the head of every organization in the public sector and the private sector has a responsibility for their systems. We can reach out and try to encourage them. We can try to support their efforts. We can give visibility to where we think there are problems, but the ultimate responsibility rests with every chief executive officer, and every mayor, county executive, and Governor.

Mr. CRANE. You touched upon the possibility that at the local level some are dismissing the possibility of a crisis. It may not be a national crisis, and yet it could provide serious hardship to a lot of people. Is there a way that you could prepare a warning list in some of those targeted areas and try and guarantee that it gets distributed to newspapers and the media for publication to try and alert people at the local level to ask those questions? Are we doing what needs to be done, and are we going to be spared that?

Mr. KOSKINEN. It is a very good question. It is, in fact, the focus of a lot of our activity. The Federal Emergency Management Agency has been working with the State and local emergency managers. FEMA is in the process of holding 10 regional meetings for State and local emergency managers, and we have put the State Year 2000 coordinators in those meetings to start to look at what the risks are and to send that message out. Later this spring or in the early part of the summer, we want to provide to local officials tool kits for, in fact, conducting what we call "Community Conversations" or "Townhalls." These would be gatherings where, in communities across the United States, citizens and elected officials could sit down with the local service providers—their banker, their power company, their telecommunication company—and discuss the state

of readiness. Not necessarily that they are done with their work, but where they are in the process. And I think that if we can get more of those dialogs and conversations going at the local level we will bring to the surface the issue and the nature of the problems.

Mr. CRANE. Well, if you could get the alert signs to us, too, because that is a message that we can take home for town meetings and, at least, raise the question ourselves.

I want to congratulate you for what you have done.

Thank you, Mr. Chairman.

Chairman ARCHER. Does any other member wish to inquire?

Mr. Hulshof.

Mr. HULSHOF. Thank you, Mr. Chairman.

I recognize that Ms. Golden will be up momentarily to talk about HHS, but I noted that in your testimony, Mr. Koskinen, that you mentioned that HHS has some unique challenges facing them especially as far as this Committee's jurisdiction regarding HCFA. Could you just talk about that a little bit?

Mr. KOSKINEN. Yes.

Obviously, HCFA processes billions of dollars of payments, and hundreds and millions of transactions each of which are separate. So HCFA's systems are some of the largest and most complicated in the world. Now the process, as you all know better than most, is that Medicare system is actually run for us by the private sector. Sixty large insurance companies, in fact, process those claims. So it has taken us some time to move forward, to some extent because we were pushing for earlier target dates than the private sector. We wanted implementation by March 31. Most private-sector companies are looking at completing work this summer. So, it took us some time to get them focused.

We have some unique relationships with those companies that are not the normal Federal contract relationships. HCFA has no authority to have that work done by other information processors. It has to be done by the insurance companies. It also is a situation where the normal contractual rules to end a relationship are more complicated because of special legislative provisions. And we have supported HCFA's recommendations that there be contractor reform legislation that would put contractors in this area in the same boat with all other Federal contractors.

But I am happy to report that, with a lot of hard work by those contractors and HCFA over the last 6 months, we are now confident that system will work. But, as Mrs. DeParle will tell you, even if we have our systems working, and the intermediaries will have their systems working, the question will be whether the providers have their systems working. Will the doctors, the hospitals, and the healthcare facilities actually be able to submit payments to be processed? Those are systems we don't control. We don't have authority over them. Again, back to our concern about local communities, our concern here is about local providers. And you will hear more about that from HCFA in terms of their outreach efforts, but I think that if we are going to have a problem, it will be at that end of the process, not at our end.

Mr. HULSHOF. OK, thank you.

Mr. Chairman, I yield back.

Chairman ARCHER. Mrs. Thurman.

Mrs. THURMAN. Thank you, Mr. Chairman.

I have to tell you that I talked to one of my sheriffs last year, and I need to do a follow-up with him based on this conversation. He was very, very concerned about this compliance with Y2K and how he was going to change his computer system over because there were no grants, there was nothing available to them to help them through the State systems. Are you seeing more of that in your conversations with the State and local people? Monies being available? Because a lot of these people are hitting caps, can't afford it, especially within rural areas.

Mr. KOSKINEN. We are concerned about rural areas. We deliver 20 percent of utilities in this country in rural areas and small towns. There are over 3,000 power companies, over 1,400 telephone companies, so a lot of the problem is not just AT&T and Sprint and the power companies in cities like Washington. A lot of it is at the local level. And we are reaching out through the associations and organizations to reach them.

But, again, as has been our experience with small businesses, our experience at the local level is not that people don't have the resources. We don't have a significant influx of small businesses saying that they need financial help. And we don't have a lot of local communities saying, "You know, if we had some money, we would fix it." We have a lot of local communities who, for one reason or another, have not yet made this a priority.

Mrs. THURMAN. Well, this one, particularly, had made it a priority, but he didn't have any money. He was looking for grants, loans, and other things to try to update this system within his area.

Let me ask you this question. In Gainesville last week, there was an article in the university newspaper. There was a law conference that was addressing the technology issue with Y2K, and he mentioned that there was a particular problem—and I don't know what you are seeing out here, but it is certainly something, I think, to be talked about. "I would wager your business client is doing an inadequate job with Y2K compliance. Business clients need to prioritize their dependency on certain items and establishing ongoing conversation with larger suppliers."

But he also went on to say that encapsulation and windowing were how small business were getting around this, or at least, potentially reacting to this. But these were not really taking care of the problem. It is just kind of delaying the problem.

Are we seeing a lot of that as some safety net out there for folks? They are going to do these things, but then they turn around and it is really not going to be fixed?

Mr. KOSKINEN. It doesn't solve the underlying problem, but it is not a short-term fix in some cases depending on the process.

One way to window is to say that every number after 50 is 1900 and every number before 50 is 2000. So that 00 would be 2000, 01 would be below 50 and would be 2001. So, that would give you a system that would run until 2050.

There are various other windowing techniques. You can roll the clock back to 1972 which is the same calendar year as the Year 2000, and again, you have 28 years.

People who are windowing are using it not as a 6-month fix, but to give themselves a year or two running room to upgrade or totally replace the system that is being windowed.

The complication with windowing is that to the extent that you exchange data, you have got to make sure that the formatting works with the people you exchange date with, which is why you hear so much about the importance of data exchanges.

But a lot of work is being done. Rather than moving the Code from two digits to four, you would, in effect, work around the Code, and, in fact, have the system think it is a year that it is not.

Mrs. THURMAN. So, they could maybe be feeling that they are fixing this but falsely not and particularly, if they have to do a data change——

Mr. KOSKINEN. Everyone knows that you are doing it to fix the problem, but that you are not fixing it out to the Year 3000. What you need to do with windowing, and the people doing it are aware of this, is to ensure that any data exchanges you make are with systems that can adopt and accept the format you use.

Mrs. THURMAN. And you are saying that finances are not the problem with small businesses. Why would they not just go ahead and try to get into compliance with Y2K without using these other two techniques?

Mr. KOSKINEN. The SBA already has a loan program that is available to small businesses. And the explanation as to why they don't take action is that this would be a lot easier problem if you could guarantee that everything would fail because then people would have to fix it.

We don't want small businesses to waste money buying things that they don't need. That's why, for Federal agencies, the GAO and OMB analysis starts with an assessment.

What a lot of businesses are saying is that they don't want to borrow any money, whether it is thruogh a low-interest loan from SBA or somebody else, and that they are busy and they don't know about this. They'll just wait and see. And then if their computer shuts down, they will go and buy another one. "I don't want to spend a few thousand dollars, or even a few hundred dollars now, if I don't have to."

We can't issue an edict in which we say to every small businesses computers are all going to fail. A lot of them will not. What small businesses need to do is make an assessment of what their risks are. Check with their manufacturers. Take advantage of the information that the SBA and others are providing to them, and then make a decision. It is that process that they are not going through.

Mrs. THURMAN. Thank you.

Chairman ARCHER. Does any other member wish to inquire?

Mr. Koskinen, you have taken on a massive responsibility, and I am impressed by your grasp, your knowledge, and what you have done both from an overall standpoint and from a detail standpoint. The Nation is lucky to have you. Thank you for what you have been doing. Thank you for being before us today.

Mr. KOSKINEN. Thank you for your very kind comments, Mr. Chairman.

Chairman ARCHER. Our next witness is the Honorable Olivia Golden, Assistant Secretary for Children and Families with HHS.

Good morning, and welcome, Ms. Golden. We are pleased to have you before us. I think that you probably heard my previous admonition to witnesses that if you can keep your verbal testimony to within 5 minutes, we would appreciate it. Your entire written statement will be inserted, without objection, in the record.

STATEMENT OF HON. OLIVIA GOLDEN, ASSISTANT SECRETARY FOR CHILDREN AND FAMILIES, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

Ms. GOLDEN. Thank you, Mr. Chairman. I will summarize my longer statement for the record.

Thank you, Mr. Chairman, and Members of the Committee, for the opportunity to appear before you today to report on the progress that we have made in ensuring that our automated systems are Year 2000 compliant and to share our outreach efforts to the human services sector.

I am extremely pleased to report to the Committee that ACF has completed our efforts to ensure Year 2000 compliance of all its automated systems. I would like to describe briefly our efforts on these systems and our efforts to work with our State and local partners to address the special problems that they face.

First, ACF's internal systems. Ensuring that all ACF mission-critical systems—grant making, child support enforcement, and information collection and reporting, are Year 2000 compliant, has long been a priority for us.

In 1993, ACF engaged in a business process re-engineering effort which resulted in the GATES system. This system allows ACF to carry out all of our functions related to grant making in one system, and it was designed from its inception to be Year 2000 compliant.

ACF's second major category of mission-critical systems is child support enforcement systems: the Federal parent locator service, the tax refund offset system, the renumeration verification system, and the child support enforcement network. The first three of these systems were repaired to meet Year 2000 requirements, and the fourth was developed as a Y2K-compliant application.

The third, and final, internal system category in ACF involves information collection and reporting. ACF uses two systems to collect and analyze information on certain at-risk populations. We have the adoption and foster care analysis and reporting system, and the runaway and homeless youth management information system. Both of these systems were designed to be Year 2000 compliant.

To further ensure that these systems meet Y2K requirements, ACF hired three independent verification and validation contractors to conduct testing of the systems. IV&V efforts have been completed on all but one of ACF's mission-critical systems, five have received final compliance certifications from the contractors. The IV&V effort for the GATES system has been extremely complex, but we expect to receive the final certification of compliance by the end of March.

And, as an extra measure of protection from unanticipated problems, as you have heard from other agencies, ACF has developed business continuity and contingency plans for all of our mission-critical systems. The plans contain specific information on Year

2000-related problems that might occur to each system and spell out the triggers that would cause a specific remediation action to be invoked.

In addition to ensuring the integrity of our Federal systems, we have focused attention on the effect of Year 2000 problems on providers of human services under programs funded by ACF. I would like to briefly summarize our efforts.

Assistance to States and grantees: ACF supports a wide range of programs that are administered at the State, county and local levels. While we do not play a direct role in the development and operation of the systems needed to support these programs, we are working on a number of fronts to ensure that to the maximum extent possible, human services providers are taking appropriate steps to address the Year 2000 problem. Our shared goal with States and grantees is to ensure the continued provision of human services in our programs in the coming millennium.

To achieve this role, ACF's goal, in addition to ensuring the readiness of our own system, is threefold. First, to heighten awareness. For the past few years, ACF has been involved in actively reaching out to human services providers on the Year 2000 issue. We are seeking not only to elevate the level of attention at the State and local level, but also to glean information about the most useful ways that we can help our partners continue to deliver services in the case of a system breakdown. Detailed information on our awareness strategies is in the long version of my testimony, and I would be happy to provide details in answer to questions.

Second role: access to resources. ACF has assisted States and grantees in gaining access to a range of available resources which will be useful in their efforts to become Year 2000 compliant.

And our third role is to access overall readiness, including a focus on contingency plan development. ACF will continue to use information from our surveys and onsite reviews to assess how we can best work with States and providers that are most in need.

In conclusion, we are confident that all internal systems in the administration for Children and Families are Year 2000 compliant. We are continuing our efforts to assist grantees and other human service providers by conducting extensive Year 2000 outreach.

I would be pleased to respond to any questions. Thank you.

[The prepared statement follows:]

Statement of Hon. Olivia Golden, Assistant Secretary for Children and Families, U.S. Department of Health and Human Services

Good morning Mr. Chairman and Members of the Committee. I am Olivia Golden, Assistant Secretary for Children and Families within the Department of Health and Human Services. I appreciate the opportunity to appear before you today to report on the progress we have made in ensuring that our automated systems are Year 2000 compliant, and to share our outreach efforts to the human services sector. Your attention to this issue is certain to help us in highlighting the importance with which it must be viewed by State, county and local human service providers.

I am extremely pleased to report that ACF has completed efforts to ensure Year 2000 compliance of all its automated systems applications. We initially identified 55 systems as providing mission-critical support to ACF core business processes which require Year 2000 remediation—grant-making, child support enforcement, and information collection and reporting (ten were subsequently retired).

I would like to describe our efforts to ensure compliance in each of these critical systems, including our use of independent verification and validation processes and contingency planning for the unexpected, and our efforts to work with our State and local partners to address the special problems they face.

I. ACF Mission Critical Systems

Ensuring that ACF mission-critical systems are Year 2000 compliant has been a priority for us for several years. I am convinced that this level of attention was essential to our success in completing Year 2000 compliance activities for all our mission-critical systems.

Beginning in 1993, ACF engaged in a business process reengineering (BPR) effort, the aim of which was to consolidate the many ACF grant-making, tracking, and reporting systems into one integrated system. This system, called the Grants Application, Tracking, and Evaluation System or GATES, allows ACF to carry out all the administrative functions related to grant-making via one system. GATES ensures that grants are processed seamlessly, and allows ACF to collect and analyze program performance information. It was designed from its inception to be Year 2000 compliant and is a dynamic system that will continue to evolve to meet ACF's grants-related needs.

This transformation of grant-making systems was a huge accomplishment. Now, all grants, whether entitlement grants like Child Support Enforcement or discretionary grants such as Head Start, are processed using one central system.

ACF's second major category of mission-critical systems is Child Support Enforcement systems. ACF efforts to assist all States and territories in their attempts to establish and enforce child support are supported by four systems:

- The Federal Parent Locator Service (FPLS) which is a computerized national location network that consists of a National Directory of New Hires (NDNH), a centralized repository of W–4, quarterly wage and unemployment insurance claims data, and a Federal Case Registry (FCR) of child support orders. These two databases are automatically matched on a daily basis, providing States with the most timely, accurate information available to locate non-custodial parents for the purpose of establishing or enforcing child support orders;
- The Tax Refund Offset System (TROS) which allows States to intercept Federal tax refunds and other Federal payments due to non-custodial parents who are delinquent in paying child support;
- The Enumeration Verification System (EVS) which allows States to verify the social security numbers of non-custodial parents; and
- The Child Support Enforcement Network (CSENet) which provides a means for States and territories to exchange information needed to work interstate child support cases.

The first three of these systems are housed on a Social Security Administration mainframe computer. These systems were repaired to meet Year 2000 requirements by providing individual lines of code to ensure that all dates use four-digit years in calculations, manipulations, display, input, and reports.

CSENet is a federally maintained network of personal computers (PCs) at 54 State and territorial sites, connected via modems to a federal host personal computer. CSENet was developed as a Year 2000 compliant application. Currently, the PCs upon which this application is run are being upgraded to ensure Year 2000 compliance of all aspects of the network. This upgrade will be completed by March 1999 for most States and, pending completion in the others, a contingency of patches will be made available for the hardware and its operating systems until all of the upgraded hardware is in place.

The third and final internal system category in ACF involves information collection and reporting. ACF collects information on at-risk segments of the population served by our programs, such as children in the adoption and foster care system and runaway and homeless youth.

ACF uses two systems to collect and analyze this information: the Adoption and Foster Care Analysis and Reporting System (AFCARS) and the Runaway and Homeless Youth Management Information System (RHYMIS). AFCARS is housed on a National Institutes of Health mainframe, while RHYMIS is a system consisting of stand-alone PCs that collect and analyze information from approximately 400 grantees. These PCs save electronic reports to diskettes that grantees mail to the Family and Youth Services Bureau for uploading into a composite federal RHYMIS system. Both AFCARS and RHYMIS were designed to be Year 2000 compliant.

A number of these systems exchange information with State systems, such as AFCARS, FPLS, TROS, and EVS. In these cases, we have established bridges to ensure that all data incorporated in our systems from the States' systems are Year 2000 compliant. A bridge screens the incoming data to ensure that they use 4-digit year dates; if they do not, the bridge prefixes the proper century digits to the year date. In turn, as an interim measure, if a State system cannot accept Year 2000 compliant data, a conversion program will format the data field in a way that is usable by the State prior to transmitting the data to the State system.

I'd like to now turn to our Independent Verification and Validation activities and our contingency planning to deal with unexpected systems problems.

II. Independent Validation and Contingency Planning

Independent Verification and Validation (IV&V) is essential for ensuring that the hardware and software associated with a system meet Year 2000 requirements. Using three IV&V contractors, ACF's mission-critical systems were tested on several different levels to ensure that they comply with the Year 2000 requirements for the use of the four-digit year date format and that they would function properly after remediation was completed. IV&V have been completed on all but one of ACF's mission critical-systems; five of those have received final compliance certifications from the contractors: AFCARS, RHYMIS, FPLS, EVS, and TROS.

Although the CSENet IV&V showed that the CSENet application itself is compliant, it also revealed that the hardware and operating system software upon which the application runs need to be upgraded. We are in the process of addressing the needed upgrades.

The IV&V effort for the GATES systems has been an extremely complex undertaking. However, we expect to receive the final certification of compliance by the end of March. The contractor has spent a large amount of time becoming familiar with the system's construction and interfaces with external systems and is currently running a series of date rollover tests as a final step to certification of compliance.

As a result of these rigorous efforts, we are confident that our systems will be fully Year 2000 compliant by the end of March, with the sole exception of CSENet. That system will be compliant when its underlying hardware and operating systems are replaced in September 1999. However, as an extra measure of protection from any unanticipated problems, ACF has developed Business Continuity and Contingency Plans (BCCPs) for all our mission-critical systems. These plans will ensure that ACF will be able to carry out its core business functions until unforeseen problems are resolved. The BCCPs contain specific information on Year 2000 related problems that might occur to each system, and spell out the triggers that would cause a specific remediation action to be invoked.

In addition to ensuring the integrity of our federal systems, we have focused attention on the affects of Year 2000 problems on providers of human services under programs funded by ACF. I would like to briefly describe our efforts.

III. Assistance to States and Grantees

ACF supports a wide range of programs that are administered at the State, county and local levels. While we do not play a direct role in the development and operation of the systems needed to support these programs, we are working on a number of fronts to ensure that, to the maximum extent possible, human services providers are taking appropriate steps to address the Year 2000 problem.

This is very complicated because there are substantial variations in the degree of automation in each program and at each level, ranging from sophisticated. Statewide systems for multiple programs, to simple desktop operation for a non-profit service provider. The sheer number and complexity of these systems makes assessment of the potential Year 2000 problems extremely difficult. The number of entities involved in the provision of human services, from the federal level down to the providers of services in communities, further complicates the picture. An example may help to illustrate this point:

> In one large State, there are numerous systems that are used to administer the human services programs. Four separate systems determine eligibility for the Temporary Assistance for Needy Families, food stamp and Medicaid programs. Many Child Support Enforcement systems are operated at the county level. There is a Statewide system for the child welfare program under title IV–E of the Social Security Act, but services may be tracked by a large number of private service providers at the community level. There is no centralized child care system—multiple information systems exist at the county and local provider level. Head Start grantees operate individual information systems with varying degrees of sophistication. This also is true for grantees in many other programs as well.

For the families that rely on our systems, this staggering level of complexity means that a wide variety of partners in the Federal, State, and local levels must undertake intensive, focused efforts to be sure that families and individuals do not lose crucial services due to Year 2000 computer problems. While ACF has achieved its own Year 2000 compliance, that alone is only one part of the battle to ensure that service is not disrupted. In addition, we must hold States and local entities ac-

countable for seeing that their systems are compliant and that they have viable contingency plans in place, with our support and assistance.

ACF has taken action to make our partners and grantees aware of the critical nature of the problem, and to assist them as they plan and execute their own Year 2000 readiness strategies. As laid out in more detail below, we have provided and will continue to provide information, technical assistance, and help with assessments of grantees' systems. In addition, we plan to accelerate our efforts to do more on-site assessment and participate in States' contingency planning efforts.

In order to get a clearer sense of the status of all these systems, we have requested that States provide us with estimates of Year 2000 readiness for these major programs, the status of their contingency plans, and updates of this information on a regular basis. Although no State has indicated that it will not be Year 2000 ready, a number have indicated that they will not be ready until late in the year. With just over half the States responding so far, several indicate that they are going to finish their fixes later in the year—in the third or fourth quarter. Coming this close to the deadline is a real cause for concern, because systems experts believe that large, complex organizations should be in a testing phase by now. To compound the fact that some States are cutting it so close, approximately a quarter report that they have no contingency plans.

This information, like other reports, indicates that we have reason to be concerned about State and local readiness regarding Year 2000. The recent General Accounting Office (GAO) report on the Year 2000 readiness of State public assistance systems, and the National Association of Counties (NACO) report on the readiness of counties, have raised concerns about the ability of State, territorial, and local governments to deal with this problem. The GAO survey found most States were not as far along with their corrective action plans as they should have been. Similarly, NACO's report, based on a sample of 500 counties, found that up to half of all counties do not have Year 2000 corrective action plans, or budgets to support such plans.

ACF's outreach strategy is designed to inform and support our State and local partners as they move ahead on their critical task of ensuring that their human services systems are not disrupted by Year 2000 problems. Our shared goal is to ensure the continued provision of human services under our programs in the coming millennium. To achieve this goal, ACF's role is to:

- Ensure the readiness of ACF systems, which is complete as described above;
- Heighten awareness of the issue and the impact of taking corrective action to ensure continued service delivery;
- Assist states in gaining access to available resources to support their Year 2000 efforts; and
- Work with our partners to assess the overall readiness of their systems and encourage and support the development of contingency plans.

Heighten awareness

For the past few years, ACF has been involved in actively reaching out to human service providers on the Year 2000 issue. ACF has led the Human Services Outreach Sector, which includes the Administration on Aging, the Health Care Financing Administration (Medicaid), the Health Resources and Services Administration and the Substance Abuse and Mental Health Services Administration.

In addition, I have personally made this issue a top priority in my meetings with State and local officials and have asked managers and staff throughout ACF to do the same. We are seeking not only to elevate the level of attention on the issue at the State and local level, but also to glean information about the most useful ways that we can help our partners continue to deliver services in case of a system breakdown. ACF has taken additional steps to make program providers aware of the problem and of the need to take action, including:

- Establishment of a comprehensive Year 2000 web page (*www.acf.dhhsgov)*, which includes information for both technical and non-technical users, to reach a wide variety of audiences. The website contains guidance on planning and undertaking Year 2000 efforts, samples of documents that will help human service providers catalog their Year 2000 efforts, and software that will help providers assess the readiness of their own systems.
- Development and distribution of a Year 2000 Guide for Human Service Providers, which was distributed last year to over 7,000 human service providers and representative organizations. This document is currently being revised to be distributed to an additional 25,000 human service providers under ACF and other Departmental agencies.
- Establishment of a Year 2000 help-desk which human services providers can access through an internet e-mail address and 1–800 telephone number.
- Insertion of a standard Year 2000 information sheet in all ACF grant awards.

Access to resources

ACF has assisted States and grantees in gaining access to a range of available resources, which will be useful in their efforts to become Year 2000 compliant,

• ACF issuance of an Action Transmittal to States on July 1, 1998, which provided streamlined procedures for acquiring expedited approval of Federal matching funds in the cost of activities undertaken to make State systems Year 2000 compliant.

• Development of a TANF data collection system which is Year 2000 compliant and distribution to States of Year 2000 compliant PC-based software that they could use to collect and maintain information. About 30 percent of States use this software; the remaining 70 percent extract TANF information from their existing mainframe systems and transmit it to ACF in a Year 2000 compliant format.

• Use of existing contractor resources, available in each often HHS regional offices to assist Head Start grantees in assessing their Year 2000 readiness and solving any identified problems. In addition, grantees have been advised that program administration grant funds may be used to make their systems Year 2000 compliant.

Assess overall readiness including contingency plan development

Considerable gaps in information about the status of State systems remain. As I indicated, ACF, along with the Assistant Secretary for Management and Budget at HHS, have surveyed States on their progress in Year 2000 and on-site reviews will be conducted to further assess State systems and the need for States to put contingency plans in place. We will continue to use information from our surveys and these reviews to assess how we can best work with States as they make progress in dealing with this problem.

We also are taking advantage of opportunities provided by our ongoing systems work, where have a more active role, to focus on Year 2000 efforts. In child support, we are closely monitoring State Year 2000 activities as part of all systems reviews and automation funding requests. The latest information we have indicates that fully one-third of these systems are Year 2000 compliant. However, we are requiring that at-risk States produce an acceptable contingency plan to ensure the continued collection and disbursement of child support payments in the event that the State does not complete Year 2000 remediation efforts in time.

In addition, we have completed an in-house assessment for non-State human service providers, such as Head Start and Runaway and Homeless Youth. Based on this assessment, we intend to focus further outreach efforts and provide technical assistance to those providers most in need.

Finally, should systems disruptions occur, we have emphasized the need for contingency plans. At the same time as we are urging all our partners to develop such plans, and offering to support in those efforts, we are investigating whether there is flexibility under our programs that might offer further assistance.

IV. CONCLUSION

In summary, we are confident that all internal systems in the Administration for Children and Families are Year 2000 compliant. The remediation of these systems and independent verification and validation of their functions have helped us to improve the automated support of our core business processes. In addition, we are continuing our efforts to assist grantees and other human service providers by conducting extensive Year 2000 outreach. I can assure you that we are taking all possible measures to secure services into and beyond the new millennium.

Thank you. I would be pleased to respond to any questions.

Chairman ARCHER. Thank you, Ms. Golden.

Is there any reason why these essential services under your supervision would be disrupted by the Y2K problem?

Ms. GOLDEN. Let me give you that answer in two parts.

In terms of our systems which move grants to States and grantees and provide information, we are Y2K compliant, and, as Mr. Apfel said to you, we are developing contingency plans which would address any unforeseen circumstances.

The second part of that question, in terms of whether States can make that assurance to you and to us that all will be able to provide child support services, welfare, and so forth, what I would say is that we need to reach the point where all 50 States can make those assurances. We are not there yet, but I believe that we will be there.

Chairman ARCHER. Is it fair to assume that you have given important notice to the States of how essential this is?

Ms. GOLDEN. Yes. We have been working in a variety of ways. We began a couple of years ago in terms of basic information sharing. We have a Web site. We have a help desk. We have a grant insert with information. We wrote to the States last July to make sure that they knew that we were providing expedited access to matching funds if they needed that in a number of areas. In the child support area where we have been on site doing systems reviews, we have had more intensive involvement.

We are now intending to kick that up a level. We have written to the States. I have written, together with John Callahan, the Assistant Secretary for Management and Budget, to ask for regular updates from the States in terms of the status of their remediation and contingency plans, and we will be working with those materials and expanding our onsite review capacity.

Chairman ARCHER. Has the Congress given you adequate resources for the remediation necessary at the Federal level?

Ms. GOLDEN. Yes. Based on what I know now, we have completed our remediation.

Chairman ARCHER. And again, I would invite you that if you need any on an emergency basis, if something comes up, that you will please notify us.

Mr. Crane.

Mr. CRANE. Thank you, Mr. Chairman.

For the systems that you rely on for the States to develop and operate, what Y2K risks remain, and what are you doing to manage those risks?

Ms. GOLDEN. Well, let me tell you a little bit about how these programs operate and answer that question.

As you know, the child welfare systems, the welfare programs, child support, childcare, are all systems that are operated by the States and, in many cases, counties play a role in them as well. The States and the counties maintain databases and they often set policies. What needs to happen, is that at the State level, as Mr. Koskinen said, the chief executive officer, the Governor, as well as key State staff need to be focused on ensuring that the State system is Y2K compliant and that its relationships with county or local systems meet those requirements.

Right now many States are on track in that respect as Mr. Koskinen said. I think that there are some cases where we need to work with States to ensure that level of focus.

Mr. CRANE. Have you, by chance, seen this report card yet, that has been issued on the various departments and agencies in terms of being up to speed with regard to compliance to all of the potential Y2K problems?

No. 1, on the report card list, is Social Security Administration, although they went down hill in May of last year. They were an A+. They are only an A today.

There are several A's up there. But the Department of Health and Human Services—and this goes back to May 15, August 15, November 13, of last year—made F grades each time, and they are up to C+ today. But on the list here, you can see that C+ is toward the bottom.

What is demoralizing, looking at the list, is that the Department of Defense is C−, and the Department of State, Department of Transportation, and the Agency for International Development are all still making F grades.

At any rate, this was prepared by the Subcommittee on government Management Information and Technology and issued on February 22. It is a concern when we listen to the previous panel and Mr. Koskinen, and it sounded very positive in terms of preparedness and contingency plans. But the report card, if it is accurate, is a little demoralizing.

Is that your assessment, that you would give the Department of Health and Human Services a C+ grade currently?

Ms. GOLDEN. Well, I can only speak to my portion of it. We are the part of the agency that deals with welfare, childcare, child support, and foster care programs. And we have completed our remediation of the internal systems, and we are virtually complete on the IV&V certification. So, we believe that we also are bringing you good news in terms of having accomplished that.

Mr. CRANE. Well, that is reassuring. You do have contingency plans, too?

Ms. GOLDEN. We do.

Mr. CRANE. Just in case.

Ms. GOLDEN. Yes, we do have contingency plans.

Mr. CRANE. Very good.

Thank you so much. I yield back.

Chairman ARCHER. Mr. Coyne.

Mr. COYNE. Thank you, Mr. Chairman.

Ms. Golden, which welfare, childcare, and family assistance systems are at greatest risk due to problems at the State level?

Ms. GOLDEN. Let me try to give you an overview, Mr. Coyne, of what we know at this point, and then we will, of course, be happy to provide more detailed information as we have it later on.

What we know right now is based on State self reports as well as the work that GAO has done and some of our own onsite reviews particularly in child support. What we know at this point is that no State has told us that they will fail to meet the deadline. So, no State is currently sending up that alert.

Second, I do believe that most States have a very high level of focus, and that that is critical and one of the reasons that this hearing is so important.

And third, some States have already accomplished their remediation in child support which is the area that we know the best and have the most detailed information about. More than one-third of States, we believe, are currently Y2K compliant.

But there are some areas for concern, and I think that I would just echo Mr. Koskinen's comment about the critical importance of

keeping a focus at the State and local level. Based on State reports to us, several States are not anticipating compliance until the third or fourth quarter of calendar 1999. And that is an area of concern in relation to these complex systems.

About a quarter of the States that have reported to us do not currently have contingency plans. That is also an area of concern. And I would say that those States which have complicated interaction with county systems, that is an area of concern, as well.

We are still working with individual States, so I don't have State-by-State information that I am completely confident is accurate at this moment, but that is an overview, and we would be happy to share more.

Mr. COYNE. What recourse does ACF have if a particular State fails to pay welfare block grants, TANF benefits? And if they don't transmit child support payments or reimburse foster care providers on a timely basis because the State has failed to renovate its computer system? What recourse does your staff have if that doesn't come about?

Ms. GOLDEN. Well, of course, where I believe we need to be right now is making sure that that doesn't happen, so we have been focusing really intently on making sure that there is awareness at the State level. No State, certainly, would choose to be in that situation. And so, we are focusing on making sure that they have information and that there is a real focus on early contingency planning.

I believe that one of the things that I learned from our successful work within ACF is that you need independent verification, so that if there are some things that you need to fix or to plan around, you can do that.

And so, at this point, I believe that it is fair for us and for you to hold all States accountable for succeeding in delivering those services, and that we need to keep the intense focus over the coming months.

Mr. COYNE. So, at this point, you don't have any plans to have some recourse in the event that they fail? At this point?

Ms. GOLDEN. At this point, all of our energy is on trying to provide information and ensure accountability for succeeding.

Mr. COYNE. Which States are in the best shape relative to Y2K and why are they in better shape than others?

Ms. GOLDEN. I am not sure that I have an answer with names of States, but we could come back to you. I think that it varies across the different systems, that is, depending on whether it is child support, child welfare or TANF. In general, I think that it help if a State has started early. It helps if the State has focus at the highest level. And it helps, because of the interactions between State and county systems in the delivery of many of these services. If a State needs to deal with those, it helps to have had a focus of both high level State and county officials early. So, those are some of the key elements.

Mr. COYNE. So, you don't want to venture into which States have been more successful by naming them. Is that it?

Ms. GOLDEN. I don't, at this point, have a name of a State that has been a model across all the areas. But we can follow up. We

are working on refining our State-by-State information, and we could follow up with you if that would be useful.

Mr. COYNE. Thank you.

Chairman ARCHER. Mr. Jefferson.

Mr. JEFFERSON. Thank you, Mr. Chairman.

Let me follow up on some of the things that Mr. Coyne was asking about.

What assistance are you providing States in their efforts to meet their requirements? That your department is providing today?

Ms. GOLDEN. We have done a variety of things. As you know, we can't do it for the State. The State has to be accountable for improving their system. But there is a wide variety of things that we have been doing and that we plan to do.

In addition to providing information to making sure that there is a Web site and a help desk and information out there, we have taken a number of steps to make sure that States have access to resources. We have written to them to provide an expedited process for getting access to matching dollars in the areas of child support and child welfare. In the area of TANF, of welfare reform, and child care, they don't need help from us because the dollars that they have already received in their block grant can be used for this purpose. But we have provided States with Y2K compliant software for reporting to us in the welfare reform area. So, we've done that.

As we move more into onsite reviews and assessment, what we want to do is work with States in seeing if we can be helpful in contingency planning. For example, we think that in some cases it may be that States can help each other. Here has been a lesson learned in one State with one kind of system, that would be very useful to another State. And so, we are hopeful that we will be able to help in that arena.

Mr. JEFFERSON. I understand, your focus is on making the system work and not in thinking about what happens if it fails to work. But, of course, there can always be some failures in whole or in part, in some limited ways, or in some greater or lesser extent failures here or there.

So, I want to ask, not from the point of view of what does the Department do if they fail, but what do people who are recipients do? Low-income folks who are looking for payments that are delayed?

Ms. GOLDEN. That is a critical question and one that we are intending to work with the States through contingency planning to make sure that there is a way to get the checks out.

Let me tell you where we are on that. We asked all the States to provide us with their contingency plans, and we plan to review them. We have not received them yet, but we will be receiving them and reviewing them and knowing much more in the next couple of months. We expect that we might be able to be helpful because there might be ways that different counties in a State or different States could assist each other if it looks as though there is going to be a problem. And we also, have among our grantees at ACF not only States and counties but also community agencies, and we believe that some of the community agencies have experience providing emergency kinds of assistance, so we want to get them involved in the contingency planning as well.

So, I share your view that the most critical thing here is to make sure that low-income families don't have interruptions in basic services.

Mr. JEFFERSON. Now, what time table do you have to work out these contingency plans that you just discussed with me?

Ms. GOLDEN. We asked the States to provide them to us when we wrote to the States in December. We are anticipating getting them soon. We have not gotten contingency plans from all the States so we expect to be reviewing them over the next couple of months and working with the States.

Mr. JEFFERSON. The concerns that you have related in your prior answers about the compliance of the State systems, do these concerns also go to the smaller units of government like cities and counties or villages that are also involved here? Is there some way that you ask to States to work with them to pass on information or to provide them with technical support? How is this working?

Ms. GOLDEN. That is a very important issue. We have done some work to provide direct information to counties and cities, and their organizations. We have sent out about 7,000 copies of a guide for human services providers. As we work with States on contingency planning, we need to ensure that they are working with local units of government.

I also would note that I appreciate the Committee's focus on this set of issues, and I believe that the members here, given the wide array of States and communities that you represent, may also be able to raise that focus because I do believe that it is central to have State chief executives and local and county chief executives focused on this issue.

Mr. JEFFERSON. Thank you.

Thank you, Mr. Chairman.

Chairman ARCHER. Dr. Golden, we want to express appreciation to you for giving of your time generously today, and we look forward to working with you in the future.

With that, inasmuch as we have a pending vote on the floor, rather than call the next panel and let you start your presentations for a minute or two, we will stand in recess subject to the call of the Chair. The expectation is that we should be back here reconvening in 10 to 15 minutes max.

[Recess.]

Mr. CRANE [presiding]. Would everyone please take their seats?

I would now like to call up our next panel. Julie Pollard, Medicaid Director, Connecticut Department of Social Services, on behalf of the National Governors' Association. Is Julie present? And Joel Willemssen, again, to participate in this panel. And, as I was appropriately taught as a young man, ladies first.

So, we will have Julie make her presentation, and please try and confine your oral presentations to 5 minutes, and your printed remarks will become a part of the permanent record.

Julie, proceed.

STATEMENT OF JULIE POLLARD, MEDICAID DIRECTOR, CONNECTICUT DEPARTMENT OF SOCIAL SERVICES, AND CHAIR, HCFA SYSTEMS TECHNICAL ADVISORY GROUP ON Y2K; ON BEHALF OF THE NATIONAL GOVERNORS ASSOCIATION

Ms. POLLARD. Thank you very much.

I appreciate having this opportunity to be here today, and I have been asked by the National Governors' Association to provide information to your Committee on State Medicaid agency Year 2000 readiness with the Medicaid management information system technology.

Governors, as well as State agency directors and staff, are committed to meeting the challenge of Year 2000 computer problems in order to assure the clients of public services are not adversely affected.

I appreciate having this opportunity to be here today to update you both on Connecticut's progress and on steps being taken to ensure that all States are properly prepared for the Year 2000. As the State Medicaid administrator and chair of the Systems Technical Advisory Group to the Health Care Financing Administration, I have gained an understanding of the complexity of the tasks at hand and an appreciation for the hard work and diligent efforts of the many who are rising to meet the Year 2000 challenge.

First, I will provide you with an overview of my agency in Connecticut. I will then let you know about the State and Federal entities who have been supporting us through this process, and then some closing comments.

The Department of Social Services is the designated single State agency for administration of the approved State plan of the Connecticut Medicaid Program. The Connecticut Medicaid Program currently provides quality healthcare access to approximately 360,000 eligible consumers. A full range of demographics from newborns to elders in rural and urban locales through community-based and institutional settings can be seen in the population that receives our support. They can access a wide variety of healthcare services ranging from traditional medical care provided by physicians, pharmacies, hospitals, clinics and others to the alternative, non-traditional supports found in the Medicaid waiver initiatives. Our connection to that eligible population is through our Medicaid provider community.

Our administrative activities support the processing, authorizing, reporting and monitoring of the medical assistant services that the department pays for as required by Federal and State statutes. During the past State fiscal year, the department paid over 20 million claim details costing over $2 billion to more than 6,000 medical providers and service organizations who are enrolled in our program.

Claims processing, provider relations, Federal and State financial reporting and surveillance utilization review reporting are administered through our MMIS.

Clearly, the dynamic world of information technology has provided many valuable tools that support our daily program operations.

Accordingly, the applications and operating systems of the MMIS have needed to successfully perform yesterday, today, and in the

days and century to come. The challenges encountered along the way secondary to the rapidly changing healthcare landscape, exciting Federal and State initiatives, or a millennium have and will be met. Upon completion, our MMIS Year 2000 project will incorporate, recognize and unambiguously treat the new century and all date fields in the systems, files and functions in order to continue to effectively process all claims, reports, and other output.

The Connecticut MMIS will also be equipped for both outgoing and incoming interfaces with multiple entities, external systems, including those of the Health Care Financing Administration and the Internal Revenue Service.

It is important to note that these enhancements are being completed in a manner that is not disruptive to the current ongoing daily operations of the Medicaid Program. Project approach and overall project management has necessarily been predicated on the fact that our consumers need access to healthcare services that are inextricably tied to providing claims payment support in the healthcare industry. We recognize that responsibility and strive for excellence in that role.

Now, the analysis and implementation of changes to the Connecticut MMIS has been a complex, yet evolving, set of tasks. And while initial research for technical solutions began in early 1997, there has been an ongoing commitment to remaining current to Year 2000 industry practices and approaches which resulted in the fine tuning of our approach in management strategies.

Clearly the input that we received from others, from those both at the State and Federal levels, has provided valuable lessons along the way. The phases associated with our MMIS Year 2000 project at a high level can be categorized as assessment, renovation, testing, and implementation with extensive project management activities throughout (not unlike the Year 2000 conversion model that was put forth in the September 1997 GAO assessment guide.)

Now, we have not pursued our initiative in isolation. Our executive branch, secondary to establishing a centralized Year 2000 Program Office out of our Department of Information Technology, has promulgated a Year 2000 certification process and agency reporting management methodology. Their quality assurance process addresses the issue of certification, and it is designed to be simple and flexible while ensuring that projects critical to the State of Connecticut are completed on time. The Y2K Program Office is also working with each agency to complete that certification process.

In addition, that department anticipated the need for independent validation and verification monitoring. They pre-qualified vendors and established a listing of potential contractors that could be used by State agencies in procuring quality assurance and project management services.

Use of that service has facilitated our acquisition of a quality assurance team that provides independent monitoring and risk assessment of our MMIS project.

This past July, State Medicaid Directors received information regarding HCFA's millennium compliance strategy as it relates to the MMIS. Details regarding steps to be taken by States in certifying to HCFA that the MMIS and mission-critical interfaces are Year

2000 compliant were clarified. Documentation related to contingency planning as well as monthly Y2K status reports to HCFA Regional Offices was requested.

Additionally, HCFA strongly recommended the use of IV&V contractor services and further supported us by providing us with a 75-percent Federal match for such services.

Recently HCFA has acquired services of an IV&V contractor to collect status information on States and on their Y2K activities and to validate the information that is being reported by State Medicaid agencies to their regional offices. Onsite visits are being conducted by HCFA's contractors. They have placed additional demands on State resources. We have worked together to try to avoid duplication of effort. The visits are yet another risk-assessment snapshot providing information for consideration in these final months of Year 2000 project activity.

Now, with hindsight, we might all agree that the best case scenario would have been for those early computer programmers to have ignored management concerns over data storage costs and to have gone ahead and coded a four-digit year format. That would have been the ultimate, no risk Year 2000 solution. But here at the end of the 20th Century, we do have a time of challenge for program managers and technology experts alike as we prepare for the next millennium.

Throughout our daily activities, we strive to achieve effective and efficient delivery of services to our customers to improve the quality of their lives. And I am here to assure you that we are committed to fulfilling our administrative responsibilities to these families and individuals who need our assistance in maintaining or achieving their self-direction and self-reliance and independent living.

Thank you for this opportunity. I would be happy to answer your questions.

[The prepared statement follows:]

Statement of Julie Pollard, Medicaid Director, Connecticut Department of Social Services, and Chair, HCFA Systems Technical Advisory Group on Y2K; on behalf of the National Governors' Association

Mr. Chairman, I have been asked by the National Governors' Association to provide information to your committee on State Medicaid Agency Year 2000 readiness of Medicaid Management Information System technology. Governors, as well as state agency directors and staff, are committed to meeting the challenge of the Year 2000 computer problem in order to ensure that clients of public services are not adversely affected.

I appreciate having this opportunity to appear before you today to share an update on both Connecticut's progress, and on steps being taken to ensure that all states are adequately prepared for the year 2000. As a state Medicaid administrator and chair of the Systems Technical Advisory Group to the Health Care Financing Administration, I have gained an understanding of the complexities of the task at hand and an appreciation for the hard work and diligent efforts of the many who are rising to and meeting the Year 2000 challenge.

First I will provide an overview of how my agency, the Connecticut Department of Social Services, is approaching Year 2000 readiness of our Medicaid Management Information System. Second, I will discuss the Year 2000 support and input that we have received from state and federal entities. Finally, I will offer some closing comments.

CONNECTICUT OVERVIEW

The Department of Social Services is the designated single state agency that administers the approved state plan for the Connecticut Medicaid Program. The Con-

necticut Medicaid program currently provides access to quality health care for approximately 360,000 eligible consumers. The full range of demographics, from newborns to elders, in urban and rural locales, through community-based and institutional settings, can be seen in the population that receives our support. They can access a wide variety of health care services ranging from traditional medical care provided by physicians, pharmacies, hospitals, clinics, and others, to the alternative, non-traditional supports found in Medicaid waiver initiatives. Our connection to that eligible population is through our Medicaid provider community.

Our administrative activities support the processing, authorizing, reporting, and monitoring of the medical assistance services the Department pays for as required by federal and state statutes. During the past state fiscal year, the Department paid over 20 million claim details costing over $2 billion to more than 6,000 medical providers and service organizations enrolled in our program. Claims processing, provider relations, federal and state financial management reporting, and surveillance and utilization review reporting are administered through the use of a federally certified Medicaid Management Information System (MMIS). Clearly, the dynamic world of information technology has provided many valuable tools in support of daily program administration.

Accordingly, the applications and operating systems of the MMIS have needed to successfully perform yesterday, today, and in the days and century to come. Challenges encountered along the way secondary to the rapidly changing health care landscape, such as exciting federal or state initiatives, or a millennium New Year, have and will be met. Upon completion, our MMIS Year 2000 project will incorporate, recognize, and unambiguously treat the new century in all date fields in all systems, files, and functions in order to continue to effectively process all claims, jobs, reports, and other output. Internal functionality will be equipped to deal with appropriate century identification through all its process. The Connecticut MMIS will also be equipped for both incoming and outgoing interfaces with multiple external entities and systems, including those of the Health Care Financing Administration (HCFA) and the Internal Revenue Service.

It is important to note that these enhancements are being completed in a manner that is not disruptive to the on-going daily operation of the Medicaid program. Project approach and overall project management has necessarily been predicated on the fact that our consumers need access to health care services that is inextricably tied to providing claims payment support to the health care industry. We recognize that responsibility and strive for excellence in that role.

The analysis and implementation of changes to the Connecticut MMIS has been a complex yet evolving set of tasks. While initial research of the technical solution began in early 1997, there has been an on-going commitment to remain current on Year 2000 industry practices and approaches with a resultant "fine tuning" of our approach and project management strategies along the way. Clearly, the input received from others, at both the state and federal levels, has provided valued "lessons learned" along the way.

The phases associated with our MMIS Year 2000 project at a high level can be categorized as assessment, renovation, testing, and implementation, with extensive project management activities throughout. (This approach is not unlike the Year 2000 Conversion Model put forth in the September 1997 GAO assessment guide.) The first phase, assessment, was critical to the success of subsequent project activities. Solution strategies were reviewed and validated, scope of work was finalized, tool requirements were determined, and staffing was validated. The second phase of code renovation was conducted parallel to preparations for the testing phase, which includes unit, end to end, and user testing. Implementation follows the testing phase and results in a Year 2000 ready MMIS.

STATE SUPPORT

The Connecticut Department of Social Services has not pursued this Medicaid Year 2000 initiative in isolation. Our Executive Branch, secondary to establishing a centralized Year 2000 Program Office out of the Department of Information Technology, has promulgated a Year 2000 certification process and agency project management methodology. In carrying out their oversight role, the Y2K Program Office in Connecticut has defined a quality assurance process, a set of deliverables, and a project management methodology for agency Year 2000 projects. The quality assurance process addresses the issue of certification, and is designed to be simple and flexible, while ensuring that projects critical to the State of Connecticut are completed on time. The Y2K Program Office is working with each agency to complete the certification process.

As an additional support to state agencies, the Department of Information Technology anticipated the need for independent validation and verification monitoring. They pre-qualified vendors and established a listing of potential contractors to be used by state agencies in procuring quality assurance and project management services in the monitoring of Year 2000 initiatives. Use of that list facilitated our acquisition of a Quality Assurance Contract Team, thus enhancing our MMIS Year 2000 Project management support and providing independent monitoring and risk assessment.

FEDERAL SUPPORT

States have been moving forward with Year 2000 readiness. In recent months there has been heightened external attention as to the status of State Medicaid Agencies in responding to the Year 2000 challenge.

This past July, State Medicaid Directors received information regarding HCFA's Millennium Compliance Strategy as it relates to the MMIS. Details regarding steps to be taken by States in certifying to HCFA that the MMIS and mission-critical interfaces are Year 2000 compliant were clarified. Documentation related to contingency planning, as well as monthly Y2K status reporting to HCFA Regional Offices, was requested. Additionally, HCFA strongly recommended that states contract for Independent Verification and Validation (IV&V) services as a means of obtaining an unbiased view of an organization's systems to provide yet another level of risk mitigation in dealing with Year 2000 issues. HCFA further supported this recommendation by offering to provide a 75% federal match rate for such services.

More recently HCFA has acquired the services of their own IV&V contractor to collect status information on states and their Y2K activities and validate the information that is being reported by state Medicaid agencies to the regional offices. On-site visits conducted by HCFA's contractor have placed additional demands on state resources and we have worked together to avoid duplication of effort whenever possible. The visits provide yet another risk assessment snapshot, providing information for consideration in these final months of Year 2000 Project activity.

CLOSING COMMENTS

With hindsight, we might all agree that the best case scenario would have been for those early computer programmers to have ignored management concerns over data storage costs and coded dates using a four-digit year format. That would have been the ultimate "no risk" Year 2000 solution.

The end of the twentieth century presents a time of challenge for program managers and technology experts alike as we prepare for the next millennium. Throughout our daily activities, we strive to achieve effective and efficient delivery of the highest quality of services to help our customers improve the quality of their lives. I can assure you that we are committed to fulfilling our administrative responsibilities within the context of our agency mission: to serve families and individuals who need assistance in maintaining or achieving their full potential for self-direction, self-reliance, and independent living.

Thank you again for this opportunity to testify on the topic of Medicaid Year 2000 Readiness.

Mr. CRANE. Thank you, Ms. Pollard.

Mr. Willemssen.

STATEMENT OF JOEL C. WILLEMSSEN, DIRECTOR, CIVIL AGENCIES INFORMATION SYSTEMS, ACCOUNTING AND INFORMATION MANAGEMENT DIVISION, U.S. GENERAL ACCOUNTING OFFICE

Mr. Willemssen. Thank you, and thank you for letting us testify on this critical issue of State systems supporting critical human services programs such as TANF, child support enforcement and Medicaid.

For these and other programs, last year we reported on States systems' status. And overall the results were not encouraging. We

found that States were reporting only about one-third of their systems as compliant. The compliance rate ranged from about 16 percent for Medicaid to 25 percent for TANF, 56 percent for child care.

We also found disappointing results in the testing area. Despite the need for thorough testing, States said that they had not developed test plans for about 27 percent of their systems.

In addition to the Year 2000 systems conversions, States must continue to perform routine systems development and maintenance activities as well as implement other systems changes required to support their programs. Eighty percent of the States reported to us that these systems activities had been delayed because of the Y2K compliance efforts.

Since our report in November, Federal guidance and oversight activities for State systems have increased. For example, OMB implemented a requirement that Federal oversight agencies include the status of State human services systems in quarterly Y2K progress reports. For Medicaid, HCFA's administered two State self-reported surveys and conducted several onsite visits.

Unfortunately, overall, State Medicaid system status appears to have changed little. For example, HCFA reported in November that Medicaid systems had shown some progress in renovation, but that the number of States reporting completion of this phase had actually decreased compared to the July August data that we had reported.

To obtain more reliable Y2K information, HCFA has hired a contractor to conduct independent verification and validation of State systems. After conducting another survey, HCFA decided to rely on onsite visits to determine States' status. HCFA reported in the HHS February quarterly report to OMB that, based on seven site visits, some of the dates that States had told us in July August had already slipped.

Next, let me turn to ACF and TANF, child support enforcement, childcare and child welfare. ACF could not provide us with updated information on all State systems for this program since our report. As noted earlier, ACF did send letters and surveys to States asking for system status information. However, as of February 16, only 27 responses had been received. Further, according to HHS, the information provided by the States raised more questions than answers.

ACF is now considering onsite reviews of State systems, and it is considering developing a process similar to the one being used by HCFA or possibly working with HCFA in gathering information.

Overall, in closing, although some States are reporting progress, others are not due to be compliant until later this year. For those States and those systems, contingency planning will be especially critical.

That concludes the summary of my statement. I would be pleased to address any questions.

[The prepared statement follows:]

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

Mr. Chairman and Members of the Committee: Thank you for inviting us to participate in today's hearing on the Year 2000 status of states' automated systems that support federal human services programs, such as Medicaid, Temporary Assistance for Needy Families, and Food Stamps. The federal government and states have

a huge vested interest—financial and social—in related automated state systems. Many of these systems must still be renovated to make the transition to the year 2000.[1] Unless successfully remediated, many systems will mistake data referring to Year 2000 as meaning 1900. Such corrupted data can seriously hinder an agency's ability to provide essential services to the public and ensure adequate accountability over program operations.

Given the magnitude and nature of the programs these automated systems support, the potential problems of failing to complete Year 2000 conversion could be felt by millions of needy Americans. While some progress has been achieved, many states' systems have been reported to be at risk and not scheduled to become compliant until the last half of 1999. Further, progress reports to date have been based largely on state self-reporting which, upon on-site visits, has occasionally been found to be overly optimistic. Given these risks, business continuity and contingency planning becomes even more important in ensuring continuity of program operations and benefits in the event of systems failures.

HUMAN SERVICES PROGRAMS' ESSENTIAL SERVICES FACE RISK OF YEAR 2000 DISRUPTIONS

Failure to complete Year 2000 conversion activities could cause billions of dollars in benefits payments to fail to reach our nation's elderly, needy families, and women, infants, and children. Those newly approved for benefits could face an inability to be automatically added to the recipient file; eligibility for new applicants might not be able to be determined in a timely fashion; eligible recipients could be denied benefits; and payments could be underpaid, overpaid, or delayed. Key state-administered programs that could be affected include the following:

- In fiscal year 1997, Medicaid provided about $160 billion to millions of recipients. A joint federal-state program supported by the Department of Health and Human Services' (HHS) Health Care Financing Administration (HCFA) and administered by the states, Medicaid provides health coverage for 36 million low-income people, including over 17 million children. Its beneficiaries also include elderly, blind, and disabled individuals.
- Temporary Assistance for Needy Families (TANF), child support enforcement, child care, and child welfare programs are likewise critical to the health and well being of needy families. HHS' Administration for Children and Families (ACF) oversees these programs that provide benefits to economically needy families with children who lack financial support from one or both parents because of death, absence, incapacity, or unemployment. In fiscal year 1997, federal and state agencies spent just under $14 billion on cash and work-based assistance. Of this total, almost $8 billion was federal money, while just over $6 billion was state-funded. This program served almost 8 million recipients as of September 1998.
- Food Stamp and the Supplemental Program for Women, Infants, and Children (WIC) programs provide food for millions of Americans. The U.S. Department of Agriculture's (USDA) Food and Nutrition Service (FNS) oversees these programs. In 1998, almost 20 million people received food stamp benefits, while an average of 7.5 million received monthly WIC benefits.

SURVEY OF STATE READINESS TO SUPPORT FEDERAL HUMAN SERVICES PROGRAMS RAISES CONCERNS AND POTENTIAL RISKS

Our survey last year of states' Year 2000 status found that many systems were at risk and much work remained to ensure continued services. Overall, only about one-third of the systems supporting the Medicaid, TANF, Food Stamp (FS), WIC, Child Support Enforcement (CSE), Child Care (CC), and Child Welfare (CW) programs were reported to be compliant.[2] As figure 1 illustrates, the state reported compliance rate ranged from a low of about 16 percent (Medicaid systems) to a high of 56 percent (child care systems).[3]

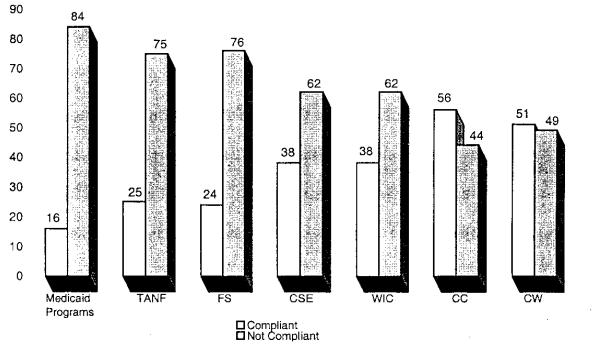
---

[1] The Year 2000 problem is rooted in the way dates are recorded and computed in automated information systems. For the past several decades, systems have typically used two digits to represent the year, such as "99" to represent 1998, in order to conserve electronic data storage and reduce operating costs. With this two-digit format, however, the year 2000 is indistinguishable from 1900 because both are represented simply as "00." As a result, if not modified, computer systems or applications that use dates or perform date- or time-sensitive calculations may generate incorrect results beyond 1999.

[2] *Year 2000 Computing Crisis: Readiness of State Automated Systems to Support Federal Welfare Programs* (GAO/AIMD–99–28, November 6, 1998). We sent a survey to the 50 states, the District of Columbia, and three territories (Guam, Puerto Rico, and the Virgin Islands).

[3] The Office and Management and Budget endorsed a five-phase approach for conducting Year 2000 work, and established target completion dates for each phase. Following awareness, agen-

Figure 1: *Percentage of Systems Reported Compliant—July/August 1998.*[4]



States reported having completed renovation on only about one-third of the systems as of July/August. Of those states that had not completed this phase, many systems (25 percent) were no more than one-quarter complete. For example, 18 states reported that they had completed renovating one quarter or fewer of their Medicaid claims processing systems. These 18 states had Medicaid expenditures of about $40 billion in fiscal year 1997—one-quarter of total Medicaid expenditures nationwide, covering about 9.5 million recipients.

Thorough testing is required to ensure that Year 2000 modifications function as intended and do not introduce new problems. Despite this need, states said last summer that they had not yet developed test plans for about 27 percent of the systems. Further, only about one-quarter of the systems were reported at that time as having completed validation and implementation.

In addition to Year 2000 systems conversions, states must continue to perform routine systems development and maintenance activities, as well as implement other systems changes required to support their human services programs. Eighty percent of the states noted that these systems activities had been delayed because of Year 2000 compliance efforts. Faced with these competing priorities, states reported struggling to manage their workloads, including important initiatives such as tracking and reporting the requirements of federal welfare reform, new HCFA programmatic requirements, and new child support requirements.

UPDATED RESULTS OF STATE HUMAN SERVICES SYSTEMS

Since our report, federal guidance and oversight activities for state human services systems have increased; however, concerns regarding states' systems status remain. Following our report, OMB implemented a requirement that federal oversight agencies include the status of state human services systems in quarterly Year 2000 progress reports.[5] Specifically, it requested that federal agencies describe actions to help ensure that federally supported, state-run programs will be able to provide services and benefits. OMB has further asked that agencies report the date when each state's systems will be Year 2000 compliant, and provide information on any significant difficulties that states are encountering.

Medicaid Systems Remain at Risk

Since last summer, HCFA has administered two state self-reported surveys and conducted several on-site visits and found that overall state Medicaid systems status has improved little. For example, HCFA reported in November 1998 that Medicaid

---

cies were instructed to assess systems (by June 1997), including inventorying, analyzing, and prioritizing them. Agencies then had to renovate their systems, either by converting or replacing them (by September 1998); validate through testing and verification (by January 1999), and then implement the converted or replaced systems (by March 1999). These phases are detailed in GAO's Year 2000 assessment guidance, *Year 2000 Computing Crisis: An Assessment Guide (GAO/AIMD–10.1.14, September 1997).*

[4] The states reported using a total of 421 automated systems to manage these programs. (Several states reported using more than one system to support a program.)

[5] OMB Memorandum for the Heads of Selected Agencies, Revised Reporting Guidance on Year 2000 Efforts, January 26, 1999. The state programs included were Food Stamps, Medical Assistance, Unemployment Insurance, TANF, Child Support Enforcement, WIC, Low Income Home Energy Assistance, Child Nutrition, Child Care, and Child Welfare.

systems had shown some progress in renovation, but that the number of states reporting completion of this phase had actually decreased compared to the July/August 1998 data that was reported to us by the states. It found, further, that 11 states' Medicaid systems were still reported to be 25 percent or less renovated, and about half of the states were 50 percent or less renovated. Only five states—Arkansas, California, Idaho, Illinois, and Iowa—reported their Medicaid systems to be 100 percent renovated. Thus, while OMB guidelines target completion of systems renovation by September 1998, states' self reported data to HCFA showed that about 90 percent of states had not completed renovation for the Medicaid programs as of November 1998.

To obtain more reliable Year 2000 state Medicaid status information, HCFA hired a contractor to conduct independent verification and validation of states' systems. As an initial effort, the contractor and HCFA distributed a survey to all states to ascertain background and Year 2000 status information. However, based on more recent information from on-site visits, the IV&V project leader said that the survey data were not as reliable as HCFA had expected because states tended to overstate their progress. As a result, HCFA has instead decided to rely on on-site contractor visits to ascertain accurate Medicaid systems' status.

HCFA reported in HHS' February 1999 quarterly report to OMB that based on seven site visits, some of the dates' states had reported to us in July/August 1998 had already slipped, underscoring the need for on-site visits to secure more accurate information. For example, according to HCFA, while four states appeared to have made some progress in the 6 months since our survey, three states' status remained the same. Further, HCFA found that one state's Medicaid eligibility system was not as far along as the state had reported in our survey. As of February 17, 1999, HCFA told us they had visited 14 states and that half of those states have shown some improvements. Thus, HCFA and the IV&V contractor plan to make on-site visits to all 50 states and the District of Columbia by the end of this April. For states considered at risk, HCFA will conduct second site visits between May and September 1999 and, if necessary, third visits between October and December 1999. The later visits will emphasize contingency planning to help the states ensure continuity of program operations in the event of systems failures.

Current Status of Systems Supporting ACF Programs is Unknown

ACF is currently surveying the states to determine the status of TANF, child support enforcement, child care, and child welfare systems, however, it does not have current information on states' systems. In response to OMB's requirement to provide updated state systems status in the quarterly Y2K progress reports, ACF sent letters and surveys to state Chief Information Officers asking for such information and asked the states to return the survey by January 31, 1999. As of February 16, 1999, ACF had received responses from 27 states. Further, according to HHS' Year 2000 Program Manager, the information provided by the states raised more questions than answers—some states did not answer all questions or complete the survey for all systems.

ACF is now proposing on-site reviews of state systems for TANF and the child support enforcement, child welfare, and child care programs in all 50 states. ACF sees these reviews as enhancing the available information concerning states' Year 2000 readiness and providing a vehicle through which the agency can provide states with technical assistance. ACF is considering developing a process similar to the one being used by HCFA, or possibly working with HCFA in gathering information.

USDA Has Been Tracking Systems Status for Food Stamps and WIC

The Department of Agriculture's Food and Nutrition Service (FNS) is tracking and reporting on Year 2000 progress for the Food Stamp and WIC programs for all 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands. For both programs, USDA initiated a survey in April 1998, asking states when their hardware, software, and telecommunications supporting automated Food Stamp and WIC systems would be compliant.

FNS updated the survey last December, and noted that 13 of the states' software, hardware, and telecommunications systems supporting the Food Stamp Program were reported as being Year 2000 compliant. Another 15 expected to be compliant by March 31, and another 13 by June 30 of this year. The remaining 13 states reported that they would not achieve compliance until the last 6 months of calendar year 1999—which puts them at high risk of failure if any unforeseen problems are encountered during testing.

Regarding WIC, as of last December, FNS reported that 42 states said their WIC systems were already compliant or would be Year 2000 compliant by June 30, 1999. However, 12 states reported that they would not be compliant until the last 6 months of 1999. For states reporting that they will not be compliant by March 31, 1999, USDA has requested the state to certify in writing that they have a working contingency plan in place that will ensure the delivery of benefits to Food Stamp Program and WIC recipients.

* * * * *

In closing, although some states are reporting progress in achieving Year 2000 compliance, many human services systems may not become compliant until later this year. Consequently, these systems are at a high risk if any unforeseen problems are encountered during testing. Business continuity and contingency plans will thus become increasingly critical for these states in an effort to ensure continued timely and accurate delivery of benefits and services. Federal oversight agencies, through their monitoring activities, plan to likewise continue to emphasize the need for contingency planning to ensure continuity of service.

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

Mr. CRANE. Thank you, Mr. Willemssen.

That report that showed the wide disparity between the States and among the programs within the States is unnerving, and your requirement of another report, a quarterly report, I hope that you can get to us as soon as possible. We hope and pray that there is significant progress.

Mr. Coyne.

Mr. COYNE. Thank you, Mr. Chairman.

Ms. Pollard, does the NGA have any data that contradicts GAO's findings that at least 15 States are less than half way through renovating their welfare block-grant computer system? Do you have any information to the contrary?

Ms. POLLARD. I am not aware of NGA specifically having statistics that would align or rebut those numbers. I am aware, from my interactions with my healthcare financing activities that many States are much farther along now than they were in November 1998, which is the last time, I believe, that a snapshot was taken of Medicaid activity.

Mr. COYNE. Assuming that there are some of those States, let's assume 15, do you have any reason—can you give us any reasons why you think that they are that far behind?

Ms. POLLARD. Well, I think that there could be, perhaps, the point to be made with regard to the definition of "behind." A State that was timing testing, for example, to be in June or July of this

year, may not consider themselves behind. Perhaps someone else could be viewing that as a standard whereby they were saying that testing should be done no later than March which would then lead one to say that June testing is behind.

So, I believe that the way in which the project management is approached by the different States does lead to some lack of clarity as to how those measures are being judged on a national survey level.

Mr. COYNE. What type of contingency plans are the States making to ensure timely payment of TANF benefits, recognizing that some States may not have fully renovated their computer systems by January 1, 2000?

Ms. POLLARD. I can speak to the issues that I am familiar with with regard to the Medicaid management system which is the technology used to reimburse healthcare services.

It is interesting that the issue of contingency planning is spoken of so strongly with Year 2000 readiness. Contingency planning has been a part of system development all along. And through the years, different States at times have gone through development and implementation activities where they have, after a period of time, totally built a new system, turned off the old system, turned on the new system. Those moments don't always happen seamlessly.

So, how one continues to conduct business, how one has business continuity, even if there is a problem with the computer, is part of Medicaid business. For example, interim payments, being able to issue checks and payment for services outside of that particular computer. Later on, being able to reconcile it back in relative to reporting, but being able to issue that money in a way that is separate from the traditional claims payment system is a tool that all States are very much aware of and have used at times when they have done major system changes in the past.

Another example would be when we have a brandnew provider. For example, pharmacy services are very technologically dependent upon the use of drug use review systems. We recently had the experience in Connecticut where a brandnew provider was joining us—nothing to do Y2K per se, but the issue of technology. They were not able to get their system ready in time for when they wanted to start their billing with us. We were able to provide them with funds outside of the system so that their business could continue while the problems were corrected and then we reflected those fund expenditures back into the system at a later time.

So, the issue of business continuity, I think, is well known to Medicaid Program administrators. The use of technology, when it is there, is certainly to our advantage. There are ways to do business without technology.

Mr. COYNE. Thank you.

Mr. CRANE. Mr. Houghton.

Mr. HOUGHTON. Thank you, Mr. Chairman.

Mr. Willemssen, I don't find myself very encouraged by your report. What you, in effect, are saying, and I quote, "many human services systems may not become compliant, and therefore, they are at high risk. In other words, if they find there are glitches,

there is not going to be enough time to change and to correct those glitches."

Is that right?

Mr. WILLEMSSEN. That is correct. That is why it is especially important that we continue to raise the level of concern for these types of systems similar to the way that that kind of concern has been raised historically at Federal agencies.

One point to keep in mind is, if you look at States, you see an incredible amount of variance between States and even within States between programs, and so, it is hard to say that all States are in this category or in that category. But there are pockets of States and programs that are way ahead and others that are way behind. And to the extent that we can continue to surface the issues and make sure that everyone is on board within the limited time remaining, I think that we can reduce that risk.

Mr. HOUGHTON. Well, that is a good goal, but you know you have 50 States and they are all individual little fiefdoms under themselves. You say that we must raise the concern, who is "we"? It is not us. It is the States themselves. And the question is, how does this interact?

Mr. WILLEMSSEN. We, in terms of the report that we issued, I think that we assisted in raising the concern level. So, I use it in that vein.

I think that the approach, for example, that HCFA is using in conducting onsite visits through its independent verification and validation contractor is a good model that other organizations such as ACF may want to emulate to get better ground data on exactly where that State and that program is at.

Mr. HOUGHTON. OK, well, these agencies in the States they are going to be ready or they are not. So, if they are not, then what happens? Is there something that the Federal Government has to do? Or what about the funding of——

Mr. WILLEMSSEN. That is, again, why we would—as mentioned here, we continue to emphasize the need for contingency planning. There has to be some backup mode.

Mr. HOUGHTON. If there is high risk and some of these human services systems may not meet the test, do you find that in the cases where you are most worried that there is contingency planning?

Mr. WILLEMSSEN. I find that generally speaking they are under development. As was mentioned, contingency plans and disaster recovery plans often exist for general computer systems environments. Do those plans exist for the most part from a Year 2000-induced failure scenario? No. Not at this point. Not based on the work that we have done.

Are they under development? Yes, generally. But there is little time left, and that is why we have to continue to rachet up the attention. The words that were spoken earlier by Ms. Golden, that has to continue to be the focus.

Mr. HOUGHTON. So, one State, in terms of some human service area, falls by the wayside; they don't do it. It is January 20, and we are all in trouble. How does that effect the recipients of Federal funds?

Mr. WILLEMSSEN. It could affect it. If nothing is done and the backup is not in place, the recipient may get an inaccurate accounting of what is owed them, or may not get the payment on time.

If I may give you an example. State unemployment insurance systems have already gone through a failure scenario. State unemployment insurance systems had a failure date in early January 1999, and, in fact, there were four whose systems failed and had to have a contingency plan. That contingency plan was putting in a, so-to-speak, make-believe date in order that checks could be processed.

So, there is already some experience in this. The Department of Labor took a very proactive stance, as well as Mr. Koskinen, in making sure that those failures were minimized. I would theorize that you will probably see similar things going on later in 1999 in this human services arena.

Mr. HOUGHTON. Mr. Chairman, I don't know what we do to follow up on this session. Obviously we are all very concerned. But, if Mr. Willemssen says that there are States that are at risk, and further more, they don't have a contingency plan, we ought to know about this.

Mr. CRANE. I couldn't agree more. You can provide that to us, right?

Mr. Willemssen. Yes, sir, we can provide that information.

Mr. HOUGHTON. Thank you very much.

Mr. CRANE. Well, I thank you, and I thank Ms. Pollard, and I thank you, Mr. Willemssen.

And, with that, the Committee will stand in recess until one.

[Whereupon, at 12:13 p.m., the Committee recessed, to reconvene at 1 p.m., the same day.]

Mr. COLLINS [presiding]. OK, we will get under way here.

The next panel consists of Hon. Charles O. Rossotti, Commissioner, Internal Revenue Service; Mr. Paul Cosgrave, Chief Information Officer with Internal RevenueService.

Gentlemen, we appreciate you all serving on the panel with some private-sector people. Thank you very much.

Mark A. Ernst, executive vice president and chief operating officer of H&R Block; William J. Dennis, Jr., senior research fellow, National Federation of Independent Businesses; Mr. James R. White, Director of Tax Policy and Administration Issues, General government Division, U.S. General Accounting Office.

We thank you, gentlemen, for being here with us today, and Mr. Rossotti, we will begin with you. And each of your statements, full statements, will be entered into the record.

STATEMENT OF HON. CHARLES O. ROSSOTTI, COMMISSIONER, INTERNAL REVENUE SERVICE

Mr. ROSSOTTI. Thank you very much, Mr. Collins. I'd just like to briefly summarize my written statement and then turn it over to Mr. Cosgrave.

As of last month, nearly all of the IRS' mission-critical applications systems were Y2K compliant, and were placed back into production for the 1999 tax filing season. About half of these systems have been successfully tested from end to end, from beginning to end, with the clock rolled forward with the new century date. So

we will continue focusing our efforts on these mission-critical applications systems from now until about the end of March. And then from April through the end of 1999, most of our effort will be on completing the integration of these application systems with commercial software products, wrapping up some smaller systems, and, most importantly, completing this really large-scale end-to-end test.

So while this is generally a positive picture, we do want to stress that there is still a great deal of risk and we do have some trouble spots. We believe the next 60 days represent the riskiest period. And that's just because of the massive amount of changes that have been made to our systems in the last year, coupled with the heavy volume of processing that occurs during the peak of the filing season. It may cause some localized problems.

We have organized an internal process to identify and respond to these problems immediately, especially so we can mitigate any possible impact on taxpayers.

We are continuing to allocate major amounts of management time to the Y2K program. We have, of course, a century date change program office, made up of a senior executive director, 53 full-time staffers, and about 1,000 other IRS employees and contractors. This program office conducts weekly status meetings, during which they review every aspect of the Y2K repair activities.

I also want to stress that Y2K is my own personal top priority. I chair a monthly executive steering Committee with representatives of all the key people involved in the program. And we, of course regularly meet with Mr. Cosgrave here and other key executives, to go over particular projects and particular risks.

We also meet periodically with our major partners in the contracting firms that are assisting us to talk about specific issues and stress the importance of it.

I do want to mention that in addition to our internal technical challenges at the IRS, we need to address the question of potential impact on taxpayers of potential Y2K problems that might occur next year after the change of the century. And I think the main point here is that we want to make sure that we at the IRS are in a position so that taxpayers who are attempting to file in good faith and pay on a timely basis are not harmed because of a Y2K computer problem that might be beyond their control.

So, at the present time, of course, the IRS has discretion to abate penalties for reasonable cause, but only limited discretion to abate interest. We are currently working with the Treasury Department to develop abatement policies and recommendations to be prepared to address this issue. And we will certainly keep the Committee aware of our progress and advise of any legislative changes that we think might be needed in this area.

So in conclusion, although significant risks remain, we are confident the IRS will be capable of fulfilling its mission in the year 2000 and beyond. We will keep the Committee informed, of course, of any errors or problems that we experience, and any impact on taxpayers and our actions to alleviate any added burden.

Thank you for this time, and I'd now like to introduce Mr. Cosgrave, our Chief Information Officer, to briefly summarize the status of our Y2K effort and each project.

[The prepared statement follows:]

Statement of Hon. Charles O. Rossotti, Commissioner, Internal Revenue Service

Mr. Chairman and Distinguished Members of the Committee: Thank you for the opportunity to discuss the status of the Internal Revenue Service's (IRS') Century Date Change Conversion program and our progress towards meeting the challenge of the Year 2000.

The IRS has made significant progress in preparing for the Year 2000. As of last month, nearly all of our mission critical systems were made Y2K compliant and were placed back into production for the 1999 Filing Season. Approximately half of these systems have been successfully tested "end-to-end" with the clocks rolled forward. We will continue focusing our repair efforts on mission critical systems from now until the end of March. From April through the end of 1999, most of the effort will be applied to wrapping up some smaller systems and, most importantly, completing the full-scale End-to-End Testing.

While this picture is generally positive, there is still a great deal of risk and some trouble spots. In fact, we believe that the next 90 days represent the riskiest period. The massive amount of changes made to our systems in the last year, coupled with the extremely heavy volumes of processing that occur during the filing season, may cause localized problems. We have organized an internal process to identify and respond to such problems immediately and to eliminate or mitigate any possible impact on taxpayers.

I would like to take the next few minutes to discuss the scope of the Year 2000 conversion at the IRS and address the leadership structure we have in place to manage our progress toward Year 2000 compliance. Then, I would like my Chief Information Officer, Paul Cosgrave, to present some of the more detailed facts about the IRS' Y2K efforts.

PROGRAM SCOPE

The IRS is a vast and complex organization, employing more than 100,000 individuals in service centers, regional offices, district offices, and posts of duty across the United States and around the world. Each year the IRS collects over $1.7 trillion in tax revenue to support the operations of the Federal Government. In order to fulfill its mission of service to taxpayers, the IRS depends on its automated systems to process tax returns, issue refunds, deposit payments, and provide taxpayers basic answers to their more than 170 million inquiries a year which we must respond to 24 hours a day, 7 days a week.

Most of these systems date back to the 1960s and 1970s when programmers were required to use two-digit date fields to represent the year because of space limitations. This is, of course, what causes the Year 2000 problem as we know it. The Year 2000 problem is undoubtedly a top priority at the IRS this year. If we don't fix our programs, our systems could generate millions of erroneous tax notices, refunds, bills, and any number of other financial reporting errors.

Making the IRS' Y2K problem even more challenging is the sheer number of affected information technology systems. The IRS currently houses over 80 mainframe computers, 1,400 minicomputers, over 100,000 personal computers and a massive telecommunications network comprised of more than 100,000 components. There are over 40 million lines of code in 79,000 software programs that support IRS operations. We must also address non-information technology (non-IT) items, such as security systems, heat and air conditioning, and office equipment in over 850 IRS locations.

I will now address our management commitment, and then Paul Cosgrave will address the progress of our work and the current priorities of our Year 2000 project.

MANAGEMENT COMMITMENT

Almost 28 months ago, the Century Date Change (CDC) Program Office was created to manage and execute the IRS' Year 2000 repair activities. The CDC Program Office is comprised of a Senior Executive Program Director and 53 full-time IRS staffers who are supported by over 1,000 IRS employees and contractors. The CDC Program Office conducts weekly status meetings during which the Director reviews the progress of every aspect of IRS Y2K repair activities. The Program Office then uses this information to create a Y2K "dashboard"—a widely used project management tool—which is a concentrated and high-level look at the overall status and progress of all IRS Y2K efforts. Please refer to the attachment, Year 2000 Dashboard Report, for the most recent Y2K "dashboard."

Allow me to assure you that Y2K is an IRS top priority, as well as my own this year. In support of our Y2K repair project, I chair a monthly Executive Steering

Committee with representatives from Treasury, the IRS, the General Accounting Office, and the National Treasury Employees Union. In addition, I meet regularly with the IRS' Chief Information Officer and other key executives to obtain individual project status updates, monitor key risks, and to ensure that all necessary actions are being taken. I also meet periodically with key executives from the major contracting firms that support IRS tax administration systems to emphasize the importance of meeting our Y2K objectives and time lines and to obtain their personal commitment to our needs.

Finally, in order to validate that we are doing everything we can to ensure that the IRS is Year 2000 compliant, we have commissioned independent assessments by organizations such as Booz-Allen & Hamilton, Inc. and Northrup Grumman, Inc. Booz-Allen & Hamilton, Inc. is performing risk identification and assessment on all CDC Program activities, while Grumman is performing a 100% review of our code renovation. They have reviewed 67.5% of our code and have found only one in every 20,000 lines of code that requires reprogramming.

An independent review of our Commercial Off-the-Shelf (COTS) products has also been scheduled. The review of the COTS products is scheduled to begin in March. In addition, we continue to rely on feedback from the Treasury Inspector General for Tax Administration (TIGTA) and GAO assessments on our Year 2000 program.

SIGNIFICANT PROGRESS MADE

Business Systems Conversion

The IRS conducts its operations using custom-developed applications. The total number of "mission critical" information technology systems is made up of 126 application systems and 7 telecommunication systems, of which two of the application systems will be retired. We are focusing our conversion activities on the application systems to ensure their continued and uninterrupted operation. Overall, approximately 40 million lines of code must be made compliant within these mission critical application systems. As of January 31, 1999, the IRS completed 92% of its code compliance work. More specifically, 114 of the 124 mission critical application systems have been made compliant.

Infrastructure

Mainframes (Tier I)—Most of the IRS' mainframe infrastructure was scheduled to be Y2K compliant by January 31, 1999. Some COTS products associated with mainframes are still being evaluated. Y2K compliant versions of these products will be fully implemented before the start of our final, integrated test.

Minicomputers (Tier II)—Approximately 1,400 minicomputers and their associated systems software (operating systems, databases, etc.) must be replaced or upgraded to be Y2K compliant. As of January 31, 1999, the infrastructure supporting 14 of the 27 Tier II mission critical systems is Y2K compliant. The balance of Tier II infrastructure conversion is scheduled for completion by July 1999 with the exception of 4 mission critical systems, whose infrastructure will be compliant by September 30, 1999. While any delay in implementation is of concern, the affected systems have been identified as having minimal or no impact on filing season activities. We are confident that these systems will be ready for the final, integrated test.

Personal Computers (Tier III)—We are currently upgrading our inventory of personal computers and laptops. Our goal is to achieve Y2K compliance by July 31, 1999 by retiring our obsolete PCs, moving to modern, Pentium-class platforms throughout the agency, and implementing a Y2K compliant standard suite of software. This effort will not only make us Y2K compliant, but will also eliminate the vast numbers of old, incompatible software products in existence at IRS.

Telecommunications

The IRS' telecommunications network, critical to operations, is supported through the Treasury Communications System (TCS) contract. The network conversion is a significant challenge given the need to upgrade or replace thousands of components within the TCS network, as well as additional custom IRS networks that include another 30,000 components. Our telecommunication equipment was made compliant in January with a few exceptions. Some telecom support equipment for collection has been deferred until after the peak of the filing season. The completion of our Voice Messaging System upgrade will continue into March.

External Trading Partners (ETPs)

The IRS, like other organizations, relies on its ability to exchange information with other organizations, or trading partners. For example, the IRS must be able to receive electronic tax returns that are prepared by various tax practitioners or

exchange data with organizations like the Financial Management Service who prepares refund checks. The IRS is working closely with its trading partners and requiring them to certify that their interfacing systems will comply with the IRS' expanded date format. Over 70% of the 406 files exchanged externally that needed to be compliant have been converted. The balance is scheduled for completion by July. We are also conducting assessments of our critical trading partners' systems to ensure that they are Y2K compliant. Meanwhile, information exchanges are being tested throughout the conversion process and will be included in the final integrated test.

Our work on the Electronic Federal Tax Payment System (EFTPS) is an example of our success in this area. EFTPS is one of the major systems used by business taxpayers and receives over $400 billion a year in federal tax payments. The system was successfully made compliant and implemented last year.

Non-IT

All areas unrelated to computer systems or software are either Telecommunications or Non-IT systems. Non-IT systems are real or personal property that contain a computer chip used to record or regulate functions. Examples of real property include security systems, alarm systems, heat and air conditioning systems, and utility systems. Examples of personal property include reproduction and other office equipment, vehicles, laboratory equipment, and special production equipment such as the Composite Mail Processing Systems (COMPS) used to process mail at IRS service centers.

The IRS has completed an assessment of its personal property. With the exception of the COMPS equipment that will be replaced with Y2K compliant equipment by November 1999, all of the 5700+ IRS personal property products that could have an impact on IRS operations have been made Y2K compliant.

For real property, the IRS occupies 756 buildings of which 96 have been identified as mission critical. Renovation of 54% of the 96 mission critical buildings is complete. The remaining mission critical buildings are scheduled for completion by July 1999. Contingency Plans for all mission critical buildings will be developed by July 1999.

Of the remaining 660 IRS occupied buildings, which are owned/operated by The General Services Administration (GSA), 41% are Y2K ready. The IRS is working closely with GSA to ensure that the remaining buildings are Y2K compliant on a timely basis.

Budget

For the last two fiscal years, IRS expenditures for the Year 2000 Conversion effort have totaled over $620 million. Expenditures for Fiscal Year 1999 are projected to be $378.5 million. All told, the project life cycle costs of the Year 2000 conversion effort will be approximately $1.3 billion.

IRS' Year 2000 effort also involves replacement of our major tax return processing system and payment processing system. These replacements include our Mainframe Consolidation project and our Integrated Submission and Remittance Processing System.

Mainframe Consolidation

The IRS proposed and received Congressional approval for a program to consolidate its mainframe computers while making them compliant for the Year 2000. This is a major program that involves eliminating 67 mainframe computers in 12 sites and replacing them with 12 new, Y2K compliant mainframes in two computing centers. This program is an important step in moving the IRS to a modern, standardized method of managing its computing resources and is consistent with the Office of Management and Budget (OMB) directives requiring consolidation of mainframe computing. Our current projections indicate that this program will also reduce operating costs by $79 million per year when fully implemented.

This large program consists of 5 projects and each is being carefully managed to ensure our ability to support the filing season, to achieve Year 2000 compliance, and to achieve the objectives of improved management and reduced long-term costs.

As of January, we replaced the non-compliant Communications Replacement System (CRS) and moved the workload from all 10 service centers to the two computing centers. Conversion of CRS was extremely difficult, especially in light of the fact that there is not an effective back-up plan for this system. The new Y2K compliant tax processing mainframes were installed in the two computing centers and workload from three of the 10 service centers was moved. The IRS identified the need for additional emphasis in the areas of standardization, automated tools, and staffing prior to the remaining migrations. In order to complete this work and minimize

risk to the filing season, we held the remaining migrations until after the 1999 Filing Season. Upgrades were made, however, to vendor-supplied software to make the existing, older mainframe computers Y2K compliant. We also replaced over 15,000 obsolete computer terminals as part of the program.

Integrated Submission and Remittance Processing System (ISRP)

The Integrated Submission and Remittance Processing System (ISRP) replaces two legacy systems which could not be made Year 2000 compliant. The Distributed Input System (DIS) and Remittance Processing System (RPS) originally formed the core input system which processes more than 200 million tax returns and accounts for tax revenues of over $1.7 trillion. The new Y2K compliant system is operational for data entry in all 10 of the IRS' service centers. However, we experienced some problems in implementing the Remittance Processing System (RPS) which precipitated our decision to defer the roll out of RPS to four service centers until August 1999. Presently, six service centers have implemented RPS and will perform filing season activities.

Recent events during the week of February 8 helped to lessen the level of concern with ISRP RPS considerably. Major software upgrades were successfully installed in two of the six ISRP RPS centers that alleviate many of the problems and risks associated with the new remittance processing system. Plans are in place to implement these upgrades to the remaining four ISRP RPS centers during the next three weeks. Detailed contingency plans have been prepared by all centers to use the legacy RPS equipment as a backup if the new system has problems during the April peak processing period. All centers will test their plans and equipment by "falling back" to the legacy RPS equipment for several days between now and March 8.

As you can see, the IRS has made significant progress in its Y2K repair efforts over the past several months. This can be attributed to a strong team of IRS employees and contractors and the effective leadership of the CDC Program Office. However, as much as we have accomplished to date, the Year 2000 remains a challenge for the IRS. It is a challenge that forces us to continually adjust our schedule, and to maneuver people and resources to attack the most critical Y2K problems. Failure to manage risks and schedules in this flexible way enormously increases the likelihood of failures and frequently ends up delaying, rather than accelerating, actual progress. We have worked hard to establish a realistic repair schedule that works for the IRS and the specific challenges we face. It is a schedule that gets the job done right the first time, because everyone knows there won't be any second chances. Our teams are at work everyday to meet these deadlines, as well as maintaining our focus on the government-wide deadlines established by OMB. We have come a long way, and we fully acknowledge that there is a great deal of work left to be accomplished this year.

As I discussed, our original schedule was altered on several of our systems due to infrastructure issues. We prioritized our schedule so that systems involved in the filing season are converted and tested first. The remaining systems that are not critical to the filing season will be converted and tested at a later date. I might also add that we are currently using the converted systems to process tax returns. Any problems that we encountered have not impacted taxpayers and were generally fixed within 24 hours of being identified.

I'd now like to explain our most pressing Year 2000 priorities for this year, beginning with filing season activities which are now taking place.

CURRENT PRIORITIES

1999 Filing Season

While the Year 2000 problem is a top priority, providing high-quality service to taxpayers and efficiently collecting tax revenue remains our primary mission. The impact of our Y2K repairs remains a major concern for this filing season and Filing Season 2000, but we are encouraged by the results of the 1999 Filing Season to date. Reports show that as of February 5, 1999 we have processed over 10 million of the 13 million returns received. This is four percent more than last year.

This year, we are proactively reporting errors, Y2K related or not, through a new web page on our Internet site. This page will report errors that impact taxpayers, such as erroneous notices sent due a systems error. It will also include other non-Y2K errors such as incorrect information in printed forms or instructions.

End-to-End Testing

End-to-End Testing will be performed on IRS mission critical systems to ensure that they function together through a series of increasingly complex tests that simulate tax processing activities in a Year 2000 environment. While many tests focus

solely on the individual system, End-to-End Testing will test the entire process that takes a tax return from its receipt to issuance of a notice or refund.

Testing activities are being performed in an isolated test environment so that the IRS can continue its core business activities—processing tax returns. Currently, the second of three major End-to-End Tests is in progress and, to date, testing has been successful. The final End-to-End Test is scheduled to begin in October 1999. However, the fact that we will need to compress our schedule for making changes to filing season software programs makes End-to-End Testing very challenging. All Filing Season 2000 changes need to be made to the software before they can be included in the final End-to-End Test.

Maintaining Focus

Although we have concentrated on converting the systems that have the most direct impact on taxpayers, we have not lost sight of the work that still needs to be done to convert and test some of our smaller systems and complete critical information technology projects.

As prevously mentioned, from April through the end of 1999 most of our efforts will be applied to wrapping up these smaller systems and completing the full-scale End-to-End Testing activities. Simultaneously, we will be completing the roll-out of our Integrated Submissions and Remittance Processing System (ISRP), which will be fully operational by August 1999. Mainframe consolidation efforts will also be taking place as we finish Y2K compliance activities.

Small Business/Practitioner Outreach

In addition to communicating with taxpayers about errors, we are also working with the Small Business Administration (SBA) to inform the small business community about the importance of Year 2000 compliance. We have held a joint press conference and produced a special Y2K article for the SSA/IRS Reporter, which is mailed to 6.5 million businesses throughout the country. In addition, the IRS homepage was updated to encourage small businesses to determine if they are "Y2K OK," and includes a link to the SBA's Y2K homepage which provides a wealth of useful information about the Year 2000. Our efforts will help ensure that small businesses have every opportunity to prepare for the Year 2000.

We also hold regular liaison meetings with practitioner organizations, such as H&R Block, Jackson-Hewitt, and the National Association of Tax Practitioners, which provide a forum in which to discuss the Y2K project. Specifically, the Information Reporting Program Advisory Committee (IRPAC) has addressed the Y2K problem in their semi-annual meetings. IRPAC was established in 1991 as a way to advise the IRS on information reporting issues of concern to the private sector and the Federal Government.

Practitioners are aware that the IRS is operating Year 2000 compliant systems this filing season and they have been asked to help out by identifying problems as they surface. Their efforts will benefit not only the IRS, but also their own organizations since early detection will allow a faster turnaround if corrections or repairs are necessary.

Contingency Planning

The IRS is developing contingency plans that outline the necessary procedures to follow in the event that a Year 2000 problem affects any of the IRS' mission critical tax processing systems. These plans concentrate on those areas that have the greatest impact on tax processing activities in addition to the areas we know to be particularly affected by the Y2K problem. This will allow us to work on aspects that have the greatest risk, while continuing to leverage the majority of our limited resources on Year 2000 conversion activities and testing.

Taxpayer Impact

Mr. Chairman, in addition to our internal technical challenges, there is a question about the impact on taxpayers. We want to be sure that taxpayers who attempt to file in good faith or pay on a timely basis are not harmed because of a Y2K computer problem beyond their control. At the present time, the IRS has discretion to abate penalties for reasonable cause, but has only limited discretion to abate interest. We are currently working with the Treasury Department to develop abatement policies and recommendations to address this issue. We will certainly keep the Committee aware of our progress and advise you of any legislative changes that may be needed.

LONG-TERM BENEFITS

While our primary goal is Year 2000 compliance, the Y2K problem has forced the IRS to address some shortcomings in its current practices. As a result of measures implemented to address the Y2K problem, the IRS will reap several long-term benefits. While I will not take the time to address all of these benefits, I would like to discuss the two which I feel are most important:

Use of Consistent Standards

The Year 2000 problem will allow us to continue to develop and employ consistent standards across the agency. For example, our Y2K work involved extensive testing of Y2K repaired systems, including a series of integrated End-to-End tests. Many of these testing activities will become standard practice at the IRS long after the Year 2000. In addition, as a result of Y2K work, we developed standards for desktop software applications, such as e-mail and word processing programs.

Improved Project Management Practices

The Year 2000 problem is perhaps the greatest project management challenge facing organizations today. Y2K has given the IRS the opportunity to hone its project management skills in preparation for similar large-scale projects, such as modernizing the agency.

CONCLUSION

We are personally monitoring the status of IRS' Year 2000 activities, and are confident that the IRS will be capable of fulfilling its mission in the Year 2000 and beyond. While we recognize that significant risks still exist, we have every confidence that our CDC Program leadership is taking the steps necessary to address them. As we continue to develop our contingency plans and closely monitor our schedule and progress, we will keep the Committee apprised of any Year 2000-related errors we experience, their impact on taxpayers, and our actions to alleviate any added taxpayer burden. We thank you again for the opportunity to discuss the IRS' Y2K efforts and appreciate the continued support of the Committee.

I will be happy to entertain questions.

Year 2000—DASHBOARD REPORT

Project Area	Overall Assessment	Comments
Business Systems Applications	Yellow	• 92% of Mission Critical application systems are Y2K compliant. The remaining systems will be compliant by July 31, 1999. • 75% of Non-Mission Critical application systems are Y2K compliant. The remaining systems will be compliant by July 31, 1999. • A 100% code review is underway and on schedule. 27 million lines of code (LOC) reviewed to date. Error rate—.005%.
Integrated Submission and Remittance Processing System	Yellow	• Return processing segment operational in all 10 service centers. • Remittance processing segment operational in 6 to 10 service centers. • Contingency plans inplace at all sites to mitigate risks.

Year 2000—DASHBOARD REPORT—Continued

Project Area	Overall Assessment	Comments
Infrastructure	Yellow	• Infrastructure supporting 14 of 27 key Tier 2 systems was completed on schedule by 1/31/1999; the remaining systems are scheduled for completion by July 1999 except for 4 systems approved for completion later in 1999. • Contract for an independent review of all COTS product across all tiers has been awarded. Work will begin March 1999 and will be completed September 1999. • All personal computers and laptops to be Y2K compliant by July 1999.
Service Center Mainframe Consolidation	Green	• All segments with Y2K compliance issues, which include security systems and terminal replacements, complete. • Schedule for consolidating remaining segments adjusted to minimize unnecessary change prior to the millenium.
Telecommunications	Green	• Y2K compliant rate for the entire Telecommunications inventory is 99%. • Remaining products/systems are scheduled to be compliant after the filing season.
External Partners	Yellow	• 291 externally exchanged datafiles must be made Y2K compliant. Over 70% of these are currently Y2K compliant. • The balance of the remaining files will be compliant by July 1999. • Additional FMS testing is currently being carried out—scheduled completion date 4/1/1999.
Non-IT	Green	• Of the 67 IRS-controlled mission-critical buildings, 35 are complete, 19 are green (on schedule), and 13 are yellow (5% and 15% behind schedule). • All 5700+ personal property products have been made Y2K compliant with the exception of the Composite Mail Processing System (COMPS). • The IRS is working with GSA to develop reporting of the 29 mission-critical buildings under GSA control.
Budget—FY 1999	Yellow	• Identifying area of potential savings and quantify new costs.
End-to-End Testing	Green	• Testing is on schedule. • Tracking mechanism is in place.
Contingency Management Plant (CMP)	Green	• CMP developed. • Matrix of IS systems to business processes delivered. • All plans comprising the CMP on schedule and due by 5/31/1999.
Location Specific Deployment Plan	Green	• Process in place. • Data is available to all IRS personnel on the Y2K web site.
End Game Planning	Green	• Process underway to coordinate all January 1, 2000 planned activities.

Mr. COLLINS. Thank you, Mr. Commissioner.

Mr. Cosgrave, we will be pleased to receive your testimony.

STATEMENT OF PAUL COSGRAVE, CHIEF INFORMATION OFFICER, INTERNAL REVENUE SERVICE

Mr. COSGRAVE. Thank you, Mr. Chairman. Commissioner Rossotti gave you an overview of both the scope and management of IRS' Y2K program. I will go into a little more depth about the status of our Y2K efforts.

Specifically, I'm going to talk about our software applications and technology infrastructure; our external partners, with whom we exchange information; major systems replacement projects; and finally our end-to-end testing, contingency planning, and additional support planning for January 2000.

First, Commissioner Rossotti discussed the scope of the Y2K effort at the IRS. We have 800,000 individual components that we are converting, testing, and implementing to ensure that they will operate smoothly at the turn of the century. This work is like taking an 800,000-piece jigsaw puzzle apart, looking at each piece individually, doing something, and then putting them back so it all works together. You have to take apart the puzzle and get it all working again.

And I'm pleased to report, all but a handful of those 800,000 pieces will be back together by July of this year. The remaining pieces will be done by September, and they will all be included in our final integration test, which is scheduled for the remainder of this year.

In terms of our applications, at this time 92 percent of IRS' mission-critical applications are Y2K compliant, and 75 percent of our non-mission-critical applications are compliant, with the remainder to be completed by July 1999. Most all of our local-area networks are now Y2K compliant, and all of our PC's and laptops will be Y2K compliant by July 1999.

The entire technology infrastructure that supports these applications is today approximately 56 percent compliant, with the rest to be completed later in 1999. The principal reason for trailing in the infrastructure area is that several vendors of our off-the-shelf business applications did not declare themselves Y2K compliant until late in 1998. So I didn't try to rush implementation and testing of those products. Rather, I decided to wait until after filing season to implement the new programs and validate Y2K compliance of these infrastructure systems.

All the infrastructure and applications with completion dates later in this year will still be part of our final integration tests. We are also conducting an independent review of 100 percent of all of our computer programming code that's over 40 million lines of code. To date, we've reviewed 27 million lines, and that revealed an error rate of only .005 percent. I'll just comment that our error rate approaches a number known as six sigma, which is a standard of quality used by some of the best private-sector companies.

With respect to our external partners, I'd like to give you some sense of our progress. Our external partners include the Social Security Administration, Financial Management Service, a number of banks—NationsBank, BancOne—service providers such as H&R Block, and over 50 and State and local entities, and many others.

IRS is working very closely with our external partners ensuring that their interfacing systems comply with our four-digit year date format and making sure they get the information they need so they can comply with the formats we need. Seventy-two point 5 percent of the files exchanged externally are currently Y2K compliant, and the remainder will be complete by July. We are also assessing the Y2K plans of our most critical partners to ensure they are Y2K ready.

Some of our systems in two particular cases here, are over 20 years old and literally cannot be made compliant. These are some of our most important base systems, the one that processes our basic returns and our payments, and also our mainframe computers that perform our consolidated reporting.

As it relates to processing returns and payments, first our new integrated submissions and processing system has two critical components that have to be made Y2K compliant. The component that processes returns has been completed and is now operational at all 10 service centers and is being used during this filing season. The component that processes payments is currently operational for this filing season in 6 of the 10 service centers, and those six sites are performing their normal activities effectively. The remaining four sites will be converted in August of this year.

The second replacement project is our service center mainframe consolidation project. This project has several objectives, in addition to achieving Y2K compliance, that includes supporting the filing season, positioning the service for modernization, reducing long-term cost, meeting OMB directives, and implementing disaster recovery. All components of this project that had Y2K issues, which include the security systems and the terminal replacements, have now been made Y2K compliant and the workload has been moved from the 10 service centers to two consolidated computing centers.

The schedule for the remaining components, which includes consolidating some collection systems and our printing capabilities, is now complete at three centers. We'll have five centers done by year-end, and will complete all 10 sites in calendar 2000.

Since we have completed all necessary Y2K work, we changed the schedule in order to minimize introducing unnecessary change prior to the actual millennium date.

Finally, our end-to-end tests, which tests how well all these jigsaw pieces fit back together, are on schedule. We completed the first two phases of this testing, and we'll begin the final integrated tests in May.

In addition to end-to-end tests, we're developing contingency plans based on GAO's recommendations. All plans are on schedule and will be complete by May 1999.

In addition to testing and contingency planning, we are also preparing for additional support in January 2000 should hiccups occur in any of these different systems. These plans included activities scheduled for January 1st and 2nd of 2000, prior to the first work day.

So in conclusion, both the Commissioner and I are personally monitoring the status of IRS' year 2000 activities and we are confident we will be able to fulfill our mission in the year 2000.

We recognize that there may be some glitches along the way, but we are prepared to deal with them in an organized manner to minimize any impact on taxpayers.

Thank you for your time.

Chairman ARCHER. Thank you, Mr. Cosgrave.

Our next witness is Mr. Mark Ernst. If you will identify yourself and whom you represent for the record, you may proceed. Welcome.

STATEMENT OF MARK A. ERNST, EXECUTIVE VICE PRESIDENT AND CHIEF OPERATING OFFICER, H&R BLOCK, INC.

Mr. ERNST. Thank you. Mr. Chairman and Members of the Committee. I'm Mark Ernst. I'm executive vice president and chief operating officer of H&R Block. We appreciate the opportunity to discuss the effects that Y2K adjustments by the IRS and IRS' stakeholders will have on taxpayers.

I would like to make just four brief points.

First, H&R Block is the Nation's largest tax preparation firm. With the year 2000 beginning in only 310 days, we and over 15 million of our clients who file one in seven individual tax returns that are received by the IRS (and about 36,000 per Congressional District), have a very big stake in a smooth transition.

Our clients are especially concerned about receiving timely refunds. Seventy percent of taxpayers get refunds, and many families depend on them to pay bills and as a source of annual forced savings.

Second, we know that successful Y2K transition depends not only on the IRS but also on a long chain of external trading partners, including tax professionals like H&R Block. I'm pleased to report that we are on schedule for successfully modifying our systems for year 2000. We've completed and tested 90 percent of 133 Y2K projects in nine mission-critical business functions. The remainder are scheduled for after April 15. While we do not expect any major interruptions of our business, we are preparing contingency plans to address areas of exposure, including trying to anticipate issues which may arise out of the IRS.

Third, we are encouraged by the IRS' progress. The current 1999 tax season, in which many Y2K upgrades are being tested, is functioning fairly well. IRS appears on track, and it has been active in meeting with key partners and stakeholders. So far, so good.

Fourth, for the future we've made a number of suggestions which have been well received by the IRS. They include:

- increasing the openness about the IRS' plans and progress,
- identification of risks to facilitate our and other tax practitioners' contingency planning,
- a continued dialog with a wide group of stakeholders, and
- tests with State revenue departments, the Social Security Administration, and the Financial Management Service before fourth-quarter end-to-end tests.

Mr. Chairman, we appreciate your support and IRS's cooperation. And we look forward to working with the Service and other stakeholders to ensure a seamless transition.

While we can't guarantee that citizens will be any more thrilled about paying taxes in the next millennium, we are working to en-

sure that the process will go smoothly and refunds will be issued promptly. We are happy to respond to questions.

[The prepared statement follows:]

Statement of Mark A. Ernst, Executive Vice President and Chief Operating Officer, H&R Block, Inc.

SUMMARY

• H&R Block handles over 15.6 million individual U.S. tax returns, 1 of 7 received by the IRS (about 36,000 per Congressional district), and markets Kiplinger TaxCut®.

• With Y2K beginning in only 310 days, stakes are high for government units and especially for the 70% of taxpayers who expect timely refunds. Y2K compliance depends not only on the IRS but on a long chain of external trading partners.

• H&R Block is on target to successfully modify its systems and prepare for Y2K. It has completed and tested 90% of 133 Y2K projects in nine mission-critical business functions; the remainder are scheduled after April 15.

• We are encouraged by IRS's progress. The 1999 tax season—in which many Y2K upgrades are being tested—is functioning well. IRS appears on track, and has been proactive in meeting with key partners and stakeholders.

• Our suggestions have been well received, including openness about plans and progress, identification of risks to facilitate contingency planning, continued dialogue with a wide group of stakeholders, and tests with state revenue departments, SSA, and FMS before fourth quarter end-to-end tests.

Mr. Chairman and Members of the Committee: I'm Mark Ernst, Executive Vice President and Chief Operating Officer of H&R Block. Prior to joining the company last September, I was for 12 years affiliated with American Express. We appreciate the opportunity to discuss the effects of Y2K adjustments by the Internal Revenue Service and its stakeholders on taxpayers and beneficiaries of federal programs. With me today are David Jamison, head of our Y2K project office, and Bob Weinberger, our vice president for government relations.

ABOUT H&R BLOCK

H&R Block, founded in 1955 and headquartered in Kansas City, is America's largest tax return preparation company. Over 120,000 individuals take our tax training courses annually. At 8,900 U.S. offices, we handle over 15.6 million individual returns—which is one in seven received by the IRS and about 36,000 per Congressional district. We are leaders in electronic filing, originating over half the practitioner e-filed returns that IRS receives. One of our subsidiaries—Block Financial—develops and markets Kiplinger TaxCut® tax preparation software, which has over 1.5 million users. We also offer our clients mortgages, financial planning, and investment services. We have recently acquired accounting practices in five cities. And we prepare tax returns internationally at over 1,200 offices in Canada, Australia, and the United Kingdom.

HIGH STAKES

The implications of Y2K for taxpayers and the tax system are serious. Calendar year 2000 begins in just 310 days. Almost immediately, America will begin the annual ritual of an intensive and complex 105-day tax season. Over 120 million individual taxpayers, 4.7 million corporations, 640,000 tax-exempt organizations, and millions of payors and employers will file over a billion federal information and tax returns.

The compliance chain needed to make the 2000 tax season successful includes employers and information return providers, software publishers, tax professionals, electronic return trans-mitters and originators, state governments, financial institutions and payroll agents, and nearly 50 federal agencies including the Social Security Administration and the Financial Management Service.

Much depends on that data: IRS bookkeeping, compliance, and enforcement; the operation of thousands of state and local government units; verification of Social Security numbers to validate dependents and credits; the issuance of checks or direct deposits; the offset of refunds for delinquent child support, student loans, and government tax debts; the administration of Social Security and Medicare; and, of course, the availability of $1.8 trillion in revenue that funds federal government benefits and programs that affect all Americans.

Beyond the effect on governments, many of the 70% of individual taxpayers—who today receive an average tax refund of $1,800 each—depend on receiving their refunds promptly. What may be a minor hiccup in the tax system can have significant effects for an individual taxpayer.

BLOCK'S PROGRAM 90% COMPLETE

At H&R Block, we have been working since 1997 to remediate our systems and prepare for Y2K. Our efforts are detailed in an Attachment to my remarks. Of 133 projects within nine mission-critical business functions, over 90% were completed and tested by the end of January; the remainder are scheduled to be finished after the current tax season ends. These efforts relate primarily to company-owned offices. About half of our tax offices are owned by franchisees. We are surveying their progress and offering assistance. We are also monitoring our suppliers and transmitters.

As the IRS notes, results can never be guaranteed, but we believe our own program is on target for successful completion. We are trying to identify any weaknesses of others in the tax chain to work through, or around, any problems. One plus for us is that we prepare our own tax software and so have an infrastructure of programmers and testers. Because we modify our software annually, we have experience in making necessary changes. But while we do not expect major interruption of our business, we are preparing for the possibility in any case.

GOOD IRS PROGRESS

Because of the high stakes, we are encouraged by the progress Commissioner Rossotti, Paul Cosgrave, IRS's Chief Information Officer, John Yost, the Y2K Program Director, and Bob Barr, Assistant Commissioner for Electronic Tax Administration, are making. You have given them needed funds and support to do the job. Each has a solid background in information systems technology and management. They are working to implement best practices.

Significantly, they report *most Y2K changes have been made already with the remainder well on track*. And, despite minor glitches, the current tax season—which is effectively testing many of the upgraded systems—seems to be functioning fairly smoothly. So far, so good.

Our contacts with the IRS have been effective. IRS has been proactive in its outreach and assessment of 13 key external trading partners. IRS's outside consultants, Booz Allen & Hamilton, met separately last winter with us and with our electronic return transmitter—then CompuServe, now MCI-WorldCom—to make sure our Y2K plans were robust. In early 1998, we tested modernized electronic filing formats that reflected Y2K upgrades through the Preparer Acceptance Testing System (PATS). IRS has also addressed stakeholders through the Council for Electronic Revenue Advancement (CERCA) and the Electronic Tax Administration Advisory Committee (ETAAC). IRS end-to-end testing is set for the second half of 1999, and we have eagerly requested to participate.

Suggestions that we have made to IRS have been well received. They include:

- First, we encourage IRS to continue to be open about its plans and progress. Disclosure of trouble spots where IRS believes its systems may be at risk will allow us to develop contingency plans accordingly.
- Second, IRS needs to continue communications with a wide group of stakeholders whose cooperation is essential for a successful 2000 tax filing season. Each is fixing its own computers and software. Active dialogue among stakeholders and with the IRS will help to ensure that the many ways we interact with one another are successful beginning in January, 2000. In our own case as the nation's largest tax preparer, we have invited Messrs. Cosgrave and Yost to a review and planning discussion.
- Third, we suggest that IRS test its systems with state revenue departments, the Financial Management Service, and the Social Security Administration and share the results in advance of end-to-end testing. Each plays an important role in tax administration.

Our suggestions in these areas are not meant to imply that IRS is not adequately planning or sequencing its Y2K operations. It properly needs to keep focus on its own repair efforts. Its cooperation enables us to perform our role in the tax chain and develop contingency plans where risks can't fully be seen.

We look forward to working with the Service and various stakeholders and partners to ensure a smooth transition to a successful 2000 filing season in which returns are filed easily and refunds issued promptly.

I'm happy to respond to questions.

H&R BLOCK Y2K PLANS AND STATUS

In July 1997, H&R Block established a program to inventory, evaluate and mitigate potential Year 2000 related issues. As part of this program, the company identified three key categories of software and systems, including information technology (IT) systems, non-IT systems (systems with internal clocks or imbedded microprocessors) and systems of third parties with which it interacts. Although the assessment phase of the project is essentially complete, our Year 2000 Project Office continually monitors the Y2K environment for new information that may adversely affect us and implements industry best practices to ensure successful operations continue well into the new millennium.

During assessment, we identified nine mission critical business functions, with U.S. tax preparation services topping the list, and 28 non-mission critical business functions. Within each of the business functions, key IT and non-IT systems are being inventoried and assessed for compliance and detailed plans are in place for required system modifications or replacements.

Currently, remediation projects are at different phases of completion. One hundred and thirty-three remediation projects, including both IT and non-IT systems, were identified within the nine mission critical business functions. Of these 133 projects, over 90% completed remediation and testing by January 31, 1999. The remaining projects in testing cannot be fully completed and in production until after the 1999 tax season due to the nature of our business.

We are also in the process of completing a survey and inventory of our tax franchisees. Some readiness issues have been identified and we are assisting our franchisees with their remediation programs to help mitigate their risk. One area in which we are assisting includes an understanding of IRS Y2K status.

The Company has initiated communications and surveyed state, Federal and foreign governments and suppliers and business partners with which it interacts to determine their plans for addressing Year 2000 issues. We are relying on their responses to determine if they will be Year 2000 compliant. Not all have responded. Contingency plans are being modified and developed as appropriate.

One of the Company's mission critical business partners, if not the most mission critical, is the Internal Revenue Service. In its most recent report, dated December 8, 1998, the Office of Management and Budget lists IRS as a "Tier Two Agency"—evidence of progress is visible, but concerns also exist.

The IRS was scheduled to be Year 2000 compliant by January 31, 1999. It plans to do end-to-end testing in a simulated Year 2000 environment with critical business partners and state departments of revenue in the second half of 1999.

We have met with associates from Booz, Allen & Hamilton who represent IRS in its efforts to understand the status of H&R Block's systems and business processes that interface with IRS. We have also audited IRS Program Director John Yost's Y2K update to the Council on Electronic Revenue Advancement (CERCA) membership last October. Eddie Feinstein, H&R Block's Director of Electronic Commerce, has also met with Commissioner Rosotti, CIO Paul Cosgrave, and others in the Y2K project in his role as CERCA Chairman and a member of the Electronic Tax Administration Advisory Committee (ETAAC).

Chairman ARCHER. Thank you, Mr. Ernst.

Our next witness is Mr. William Dennis. If you will identify yourself and whom you represent for the record, you may proceed.

STATEMENT OF WILLIAM J. DENNIS, JR., SENIOR RESEARCH FELLOW, EDUCATION FOUNDATION, NATIONAL FEDERATION OF INDEPENDENT BUSINESS

Mr. DENNIS. Thank you, Mr. Chairman. I'm William Dennis, senior research fellow with the NFIB Education Foundation here in Washington.

Attached to my written statement is a copy of a report that I prepared late last year regarding the preparedness of small business for Y2K as of late October, early November. The report itself was developed from data collected for us by The Gallup Organization,

from a national random sample, not just of NFIB members, but from all small businesses.

We expect to conduct the third survey in this series in April and we will be happy to report to you when the project completed in May.

Since the full report is attached, let me just briefly summarize and discuss implications for issues within the jurisdiction of the Committee. When you think about small business and its preparedness for Y2K, divide the population into thirds. The first third of this 5.7 million small employers is the group that has done something. They have taken steps; they feel that they are prepared; 70 percent have already tested their systems. Unless something very different happens, they think they are prepared.

This group consists disproportionately of larger small firms and more urban small firms. As a result, they cover a greater share of the employment in the small business population than their numbers within it.

The second third falls at the direct opposite end. This is the third that hasn't done anything, and says it is not going to do anything. Their rationale is that they don't think they are going to be affected. But if they are going to be affected, it probably will be cheaper for them to fix any problem after January 1 than to go ahead through the entire process earlier. An optimist would point out that 90 percent of all small firms have had their most critical software updated in the last 2 years and virtually all within the last 5 years. Nonetheless, a substantial number of small firm owners appear not to be ready to do anything further.

The final third can be divided into two equal halves. The first one of these halves is the group that doesn't have computers and says that it doesn't have equipment with any embedded chips in them. This group essentially has no management control over any type of vulnerable equipment. It couldn't take any action within the firm that would affect the Y2K problem one way or another.

The second group, the other sixth, is the group that plans to do something, but hasn't yet done it. Given the history of these surveys, this group probably will follow through. Thus, if we take the plans that they have and extrapolate them forward, we're looking at approximately 3 million small employers who will be prepared. We're looking at about 1 million who essentially are out of the picture and don't really have to be worried. And we're looking at about 1.75 million or slightly less than that who will have taken no action.

Now small business owners basically consider this a small business problem or a business problem. And warn that business is going to have to resolve it themselves. The primary issue for the Federal Government is to make sure its own house is in order. When small business files its taxes, it must be sure that it's taxes been properly credited and so forth.

The second thing the Federal Government can do is lead. It can do more with wheedling, cajoling, and explaining than it already has. And I'd be happy to give you some particulars on that.

Since my time is running short, let me just conclude with one final point. Data problems prohibit us from offering a definitive estimate of the cost that those who have taken action have incurred.

While some are running into extraordinary costs, very high costs, most are running into very minimal costs. In fact, 75 percent have spent less than $5,000 to come into compliance.

So it's not a lot and most of them have annual computer budgets that are larger than that. So at this time, financing is not a major impediment to action.

Thank you very much, Mr. Chairman.

[The prepared statement follows:]

Statement of William J. Dennis, Jr., Senior Research Fellow, Education Foundation, National Federation of Independent Business

Thank you for this opportunity to present testimony on the Y2K preparedness of small business and its implications for matters within the jurisdiction of this Committee.

Attached is a copy of the full report that I wrote in December concerning the preparedness of small business for Y2K as of late October/early November. The report was developed from data collected for the NFIB Education Foundation by The Gallup Organization. The document is the second report in the series, the first published in May and sponsored by the Wells Fargo Bank. The Foundation currently expects to conduct a third survey study in April with results available in May.

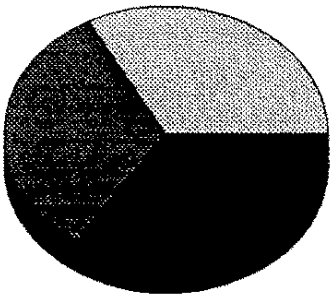
Since the full report is attached, let me summarize the salient points and move to implications. The state of small business preparedness for Y2K can be roughly divided into thirds. The first third of the estimated 5.75 million small employers has taken steps to prevent internal problems that may have been created by the Millennium Bug. This group has generally completed preventive measures (or is the process of completion) and in most instances have tested their systems. Small business owners in this third are ready for January 1, 2000, for all intents and purposes and plan no additional measures. It should be noted that these owners tend to operate larger small businesses and therefore include a disproportionately large share of small business employment. They also are disproportionately located in urban areas.

The second third falls at the other end of the preparedness scale. Its members have taken no action and plan to take none. While it is likely that some will eventually move from the no action category to the action category, my judgment is that most will do precisely what they say they will do—nothing. Their rationale is generally straight-forward: they don't think Y2K is a problem that will directly affect them or will directly affect them enough to worry about. (In this context "directly affects" means an impact that they can control. It does not mean a problem beyond their management authority, e.g., loss of electric power.) Theirs is not an altogether irrational position. A very small business with a relatively new computers and updated software could conceivably spend more checking itself than replacing its system if it went down, and with new equipment the chances of a problem are greatly minimized. An optimist can even point out that almost 90 percent have updated their most critical software in the last two years and the remainder have in the last five.

The difficulty with this rationale, however, and the single greatest argument for small business owners taking preventive measures as soon as possible is that those impacted will all be hit at about the same time. The key to minimizing damage or even surviving will be to get the impacted systems up and running immediately. But small business will be at the end of every line to obtain/purchase help, and those who can find it will pay a premium.

The third must actually be divided into halves. The first half of the group is planning to take action, but has not yet done so (as of the date of the survey). If history provides any insight, this one-sixth of the population will follow-through on its plans. The number in the April survey who planned to take steps was the number in the October/November survey who took steps in that six month interval.

PREPAREDNESS OF SMALL BUSINESS
FOR Y2K AS OF OCTOBER, 1998



The last group, i.e., the second half of the third third, doesn't have equipment susceptible to the Millennium Bug. Owners in this category have no computers or similar devices. They have no embedded chips threatening to close down critical machines. While these ventures may be impacted by events occurring outside their place of business, they can do little within the framework of their enterprise to prevent problems.

It appears that about half of all small employers will have taken action by January 1, 2000, to protect themselves from internally generated Y2K impacts. That constitutes almost three million firms. Yet, over one and two-thirds million will be exposed to difficulties brought on by their own equipment. The final one million do not need to be concerned.

Pressures are being brought to bear within the private sector to improve these numbers. Larger firms often require their suppliers to be Y2K compliant. Some commercial banks are demanding their customers, particularly those who interact electronically, to certify that they have taken preventive measures. Still, only 27 percent of exposed owners claim to have received a communication from a supplier, customer or financial institution asking them to certify their preparedness for Y2K.

Y2K Is a Business Problem

Y2K is essentially a business problem. It originated through a normal business decision-making process which, at the time, seemed quite rational. It was neither instigated nor coerced by government nor will government be the prime vehicle to resolve it.

The most important thing the Federal government can do is put its own house in order. IRS must have its systems prepared to accurately and efficiently process the vast amount of data it receives. If a tax-paying small business owner deposits his taxes on the anointed day, he has every right to expect that he will receive credit for the deposit and that it will be done without persistent snafus. If a tax-paying small business owner needs to inquire about any aspect of his account with IRS, he should be able to receive an accurate and timely response. Those of us on the outside have no means to judge how effectively IRS is addressing its Y2K problem. But little could be more disruptive than to have the tax agency beset by systematic data processing problems.

The second thing the Federal government can do is to adopt a position of the Village Nag. It can use its pulpit to wheedle, cajole and explain. In other words, it can lead. The Federal government can raise Y2K visibility and can warn (in contrast to alarm) people. It can also encourage business to work with one another to identify problems and to resolve them.

None of us really know what will happen next January 1. Some think it will be just another day while others stock their bunkers. But assume for the moment that some machines lock or malfunction. That will not stop business from being trans-

acted nor government from demanding its paperwork. Small employers will be expected to fulfill their legal obligations as if nothing had happened.

But, what will the IRS reaction be if a small employer's computers lock and he can't file his W–3s by the end of January? What will the IRS reaction be if an owner is in the middle of an audit and he can't retrieve critical information? What will its attitude be if a small business owner is the client of a firm which experiences a Y2K malfunction? IRS (and other governmental agencies) should have policies in place to handle such contingencies. An announced policy recognizing and allowing for the existence of adverse Y2K outcomes might have the secondary benefit of serving as an incentive for some to take action when they otherwise might not have.

I easily reconcile the view that Y2K is essentially a business problem with the fear that IRS policy will not appreciate or account for Y2K difficulties (public policy) that may arise among smaller firms. My rationale is the uncertainty of the solutions. To some extent, I am less concerned about the very small firms which have not taken action than larger, firms which have. The reason is that larger firms are on the whole older firms. For example, the median age of a 1–4 employee business is about four to four and one-half years. The median age of a 50–100 employee business is over 10 years. Newer firms will have fewer old systems and affected devices. As a rule, they are also less likely to have sophisticated equipment (though medical facilities are examples to the contrary). In addition, the issue of embedded chip devices remains a major question mark. What equipment contains them? And what equipment contains chips with timing/dating mechanisms? Most think of Y2K in terms of their computers, but what of the other, less obvious systems?

COSTS OF ACTION

Data problems prohibit definitive estimates of Y2K costs. However, most small business owners who have taken action have spent minimal sums to become "Y2K compliant." While there are small firms required to spend $50,000 or more to protect themselves, the common figure is less than $1,000. Over 75 percent who have taken action have spent less than $5,000. (Another nine percent didn't know). That sum clearly falls within their computer budgets. The median annual budget for hardware, software and maintenance is about $4,000 with almost three in four budgeting less than $10,000. As the deadline approaches, costs appear to be rising. The reason isn't clear, though one can speculate that the easiest "fixes" were completed first and the more difficult, more expensive ones are following.

Financing is not a major impediment to action at this time. Only three percent now planning action say that the reason they have not done so to date is a financing problem. Few small business owner respondents mentioned finance in any context. However, for some, the out-of-pocket costs will be significant and ones that they would not normally make. This is not a question of locating debt finance to undertake the preventive measures. That appears readily available. It is a question of paying for them.

INTERNATIONAL PROBLEMS

The Committee has every right to be concerned about the impact of Y2K on international trade given the lesser preparedness in many parts of the world. From the parochial small business perspective, the impact of Y2K does present a serious difficulty. Just three percent of small business owners say that they interact electronically "a lot" with business associates, i.e., suppliers, financial institutions or customers, outside the country. Fifteen (15) say the interact with these people "a little." The rapid growth of e-commerce means these percentages may already have changed since the conduct of the survey upon which this information was developed. Still, it is not a major small business consideration at this time.

CONCLUSION

To repeat, the most important thing that the Federal government can do to help small business with Y2K is be certain that its own house is in order and to exhibit consideration with regard to its administrative requirements for those owners who have encountered an adverse Y2K experience.

I will attempt to answer any questions that you may have.

[The attachment is being retained in the Committee files.]

Chairman ARCHER. Thank you, Mr. Dennis.

Our last witness on this panel is Mr. James White. Would you identify yourself and the group that you are representing, which I think I'm familiar with. You may proceed.

STATEMENT OF JAMES R. WHITE, DIRECTOR, TAX POLICY AND ADMINISTRATION ISSUES, GENERAL GOVERNMENT DIVISION, U.S. GENERAL ACCOUNTING OFFICE

Mr. WHITE. Thank you, Mr. Chairman, and Members of the Committee. My name is James White, I'm the Director of the Tax Issue area at the General Accounting Office. I'm pleased to be here today to discuss the status of IRS' year 2000, or Y2K, effort and the remaining challenges it faces.

My statement makes four points, which are summarized in the full version of my statement on page 2.

First, we are unable to provide an overall picture of the Y2K status of IRS' 133 mission-critical systems. Examples of these systems are Telefile, which allows taxpayers to file simple returns by phone, and various programs that update taxpayer accounts. IRS does not report the status of these mission-critical systems, rather, as Mr. Cosgrave explained, it reports on components, such as application software and hardware. This reflects the way IRS is organized, with one office managing applications, one managing hardware, and so on.

Second, although we cannot report on the status of the mission-critical systems in their entirety, IRS has made significant progress since we testified before the Ways and Means Oversight Subcommittee last May. However, it has not met all of its goals. IRS did meet its January 1999 goal for correcting application software, upgrading telecommunications networks, and implementing the Y2K part of its mainframe computer consolidation.

Despite significant progress, it did not meet its goal for upgrading systems software and hardware, and for fully implementing its new tax return and payment processing system. One consequence of not meeting these goals is that some systems will not be ready for full testing until late in 1999.

Third, in addition to completing the work I just discussed, IRS faces two remaining crucial year 2000 tasks. The first is what is called an end-to-end test of IRS' mission-critical systems. It will test the ability of IRS' upgraded systems to work collectively.

The second critical task is to develop 36 contingency plans to deal with possible failures scenarios. In response to recommendations we made last June, IRS has broadened its contingency planning effort. However, it has delayed the completion date for the plans, leaving less time for testing them, in part because of competing demands on the staff responsible for the plan. IRS has prioritized the due dates for these contingency plans based on risks.

Fourth, IRS will continue to face the challenge of competing demands on its information system staff. Demands that compete with the year 2000 effort include making tax law changes and customer service improvements. To address these competing demands, so far IRS has transferred staff, hired staff, and delayed some activities.

As I said, IRS has made considerable progress in completing its year 2000 work. However, it did not complete all the work it had

planned by January, and in addition has other crucial tasks to complete this year. In the next 5 months, IRS will pass several key milestones, including the April start for end-to-end testing and the May deadline for contingency plans. As each milestone is passed, the IRS and Congress should have additional information about the risks posed by the year 2000 to IRS' mission-critical systems and thus to taxpayers.

Mr. Chairman, that concludes my statement. I'll be happy to answer questions.

[The prepared statement follows:]

Statement of James R. White, Director, Tax Policy and Administration Issues, General Government Division, U.S. General Accounting Office

Mr. Chairman and Members of the Committee: We are pleased to be here today to discuss the status of the Internal Revenue Service's (IRS) Year 2000 efforts [1] and the remaining challenges IRS faces in making its information systems Year 2000 compliant. If IRS' Year 2000 efforts are unsuccessful, the impacts on taxpayers could include millions of erroneous tax notices and delayed or erroneous refunds. IRS had established a goal to complete most of its Year 2000 work by January 31, 1999. IRS established that goal to help ensure that it would (1) have a Year 2000 compliant environment implemented for the 1999 filing season and (2) provide time for working out problems that surfaced in the 1999 filing season and its Year 2000 testing.[2]

Our statement discusses four topics—(1) the extent to which IRS monitors the Year 2000 status of its mission-critical systems in their entirety; (2) whether IRS met the January 31, 1999, completion goal for the areas that it monitors—application software, systems software, hardware, and telecommunications networks; (3) the status of two remaining, critical Year 2000 tasks—conducting Year 2000 testing and completing 36 contingency plans; and (4) the fact that other business initiatives are creating competing demands on staff needed for Year 2000 efforts.

• First, we cannot provide a complete picture of the Year 2000 status of IRS' 133 mission-critical systems because IRS does not report Year 2000 status for these systems in their entirety. Instead, IRS monitors the Year 2000 status of the components of an information system, such as the application software,[3] systems software,[4] and hardware, for each of its three types of computers—mainframes, minicomputers/file servers, and personal computers. IRS officials acknowledge that their monitoring reports do not provide a complete picture on a system-by-system basis. However, these officials believe the costs of doing so outweigh the benefits, particularly given the time remaining to complete IRS' Year 2000 work.

• Second, IRS reports that it met the January 31, 1999, completion goal for some of the areas that it monitors but not for others. IRS reports that it met the January 1999 completion goal for (1) correcting application software, (2) upgrading telecommunications networks, and (3) fully implementing one of its two major system replacement projects. Despite significant progress since our testimony last May,[5] IRS did not meet the goal for (1) upgrading systems software and hardware for its three types of computers and (2) fully implementing the other major system replacement project. As a result of not meeting the goal some changes will not be tested until late in 1999, reducing the time available to make corrections before January 2000. Also, some service center staffs will have no experience before 2000 using the new system to process peak filing season volumes of remittances.

---

[1] IRS' Year 2000 efforts are necessary because IRS' information systems, many of which are over 25 years old, were programmed to read two-digit date fields. Therefore, if unchanged, these systems would interpret 2000 as 1900, seriously jeopardizing tax processing and collection operations. IRS' Year 2000 efforts include (1) fixing existing systems by correcting application software and data and upgrading hardware and systems software, if needed; (2) replacing systems if correcting them is not cost-beneficial or technically feasible; and (3) retiring systems if they will not be corrected by 2000.

[2] The Year 2000 end-to-end test is to ensure that most of IRS' mission-critical systems can operate collectively, with all systems date clocks set forward to simulate the Year 2000.

[3] Application software is the collection of computer programs that allows a user to perform a specific job task.

[4] Systems software is the collection of computer programs that manage the computer's system hardware components (e.g., operating system, central processing unit, or disk drives) that allow the application software to interact with the hardware.

[5] *IRS' Year 2000 Efforts: Status and Risks* (GAO/T–GGD–98–123, May 7, 1998).

• Third, in addition to completing work on upgrading systems software and hardware, IRS faces two remaining, critical Year 2000 tasks. The first task, and one most important for gauging IRS' success in achieving Year 2000 compliance, is an unprecedented, Year 2000 end-to-end test of most of IRS' mission-critical systems. The end-to-end test is to begin in April 1999. The need to conduct this test has created an additional new challenge for IRS—meeting a compressed schedule for developing and implementing tax law changes for the 2000 filing season. The second critical task is to develop 36 contingency plans that IRS has determined are needed to address various failure scenarios for its core business processes. IRS is developing these plans in response to our June 1998 report.[6] IRS has delayed the completion dates so that the first set of plans are to be completed by March 31, 1999, and the second set of plans by May 31, 1999. To the extent that the plans require additional actions, such as those associated with testing or preparatory activities needed to implement the plans, this delay reduces the time available to complete these activities.

• Fourth, as IRS continues its Year 2000 efforts, it will face the challenge of how to address the competing demands on its staff. These competing demands are created by IRS' other major business initiatives, such as implementing tax law changes and completing the non-Year 2000 portions of one of IRS' major system replacement projects. To address these competing demands, in the past several months, IRS has (1) transferred staff from other areas, (2) hired additional staff, and (3) delayed some activities.

Our statement today is based on our past and ongoing Year 2000 work for this Committee's Oversight Subcommittee. As a part of this work, we have interviewed officials from the National Office and reviewed IRS' contingency planning documents and IRS' Year 2000 progress reports for the week ending February 6, 1999. We did not verify the reliability of the data included in the February 6, 1999, reports.

IRS' Reports Do Not Provide A Complete Picture of Mission-Critical Systems' Status

IRS' Year 2000 status reports do not provide a complete picture of the status of IRS' mission-critical systems because IRS does not monitor Year 2000 status for its mission-critical systems in their entirety. Instead, IRS monitors the Year 2000 status of the components of an information system, such as the application software, systems software, and hardware for each of its three types of computers—mainframes, minicomputers/file servers, and personal computers. IRS also monitors its telecommunications networks separately.

As part of IRS' Year 2000 risk mitigation efforts,[7] IRS has hired a contractor to conduct periodic risk assessments. The contractor's December 1998 report recommended exploring the feasibility of tracking status on a system-by-system basis to provide a clear view of IRS' ability to achieve Year 2000 compliance. The report stated that such a system view would permit IRS to, among other things, help assess the need to target resources to achieve Year 2000 compliance. IRS officials said that IRS' approach to monitoring Year 2000 compliance corresponds to how IRS' Information Systems organization is structured to carry out its work. Specifically, IRS officials said that separate organizational units are responsible for application software, systems software and hardware, and telecommunications networks. Therefore, IRS monitors its Year 2000 status by these areas. They do not believe the benefits of monitoring status on a system-by-system basis outweigh the costs, given the amount of time remaining to complete IRS' Year 2000 work.

Reports Indicate That IRS Met The January 1999 Completion Goal For Some Areas But Not For Others

IRS' reports indicate that it met the January 1999 completion goal for some areas but not for others. The reports indicate that IRS met the January 1999 goal for correcting the application software for its existing systems and upgrading telecommunications networks. Since May 1998, when we last testified on this topic, IRS has also made progress in an area that we said was lagging—upgrading systems software and hardware. Despite this progress, however, IRS did not achieve its January 1999

---

[6] *IRS' Year 2000 Efforts: Business Continuity Planning Needed for Potential Year 2000 System Failures* (GAO/GGD–98–138, June 15, 1998).

[7] IRS' Century Date Change Project Office outlined a risk management process that is to (1) identify risks to the successful completion of Year 2000 goals, (2) coordinate the development of risk mitigation strategies, (3) oversee the execution of the strategies, and (4) elevate unmitigated risks to the Commissioner's Executive Steering Committee on the 1999 filing season and Year 2000 efforts.

completion goal for any of its three types of computer hardware. IRS fully implemented the Year 2000 aspects for one of its major system replacement projects. For the other system replacement project, 6 of the 10 service centers were using the full suite of Year 2000 changes.

Reports Indicate that IRS Met Its Goal for Application Software for Existing Systems and Telecommunications Networks

Since we testified in May 1998, IRS has continued to make progress in correcting the application software for its mission-critical systems. As of February 6, 1999, IRS reports indicate that IRS has corrected 88 percent of these applications, thereby exceeding its 85 percent goal.[8] In addition to completing this work, IRS has hired a contractor to review all of the corrected application software to determine whether IRS made any errors. This effort began in August 1998 and is scheduled to continue through May 1999.

In addition, IRS reports indicate that it met its goal for completing work on its telecommunications networks. In May 1998, we said that, according to IRS, telecommunications networks presented the most significant correction challenge and were likely the highest risk for not being completed by January 31, 1999. As of February 6, 1999, with the exception of three areas, IRS reported that it met its goal for these networks.[9]

Reports Indicate That IRS Did Not Meet the Goal for Systems Software and Hardware

IRS' reports indicate that IRS made significant progress in an area that in May 1998 we said was lagging—upgrading systems software and hardware for its three types of computers: mainframes, minicomputers/file servers, and personal computers. Despite this progress, IRS did not meet the January 31, 1999, completion goal for its three types of computers.

For IRS' mainframe computers, IRS officials said IRS fell short in meeting its goal because of delays in receiving the Year 2000 upgrades for one of its system replacement projects. IRS officials said those upgrades are to be received and implemented by March 1, 1999.

For minicomputers/file servers, IRS reports indicate that as of February 6, 1999, IRS' Information Systems organization had completed 60 percent of the work for upgrading systems software and hardware—a significant increase from 13 percent that was done in May 1998, when we last testified on the IRS' Year 2000 status.[10] According to IRS, systems software and hardware for 13 of the 27 mission-critical systems that use minicomputers/file server were not upgraded by January 31, 1999. The systems software and hardware for 7 of the 13 systems are not scheduled to be Year 2000 compliant until after March 1999. As a result of the delay, some changes are not to be tested until October 1999, when the second part of the Year 2000 end-to-end test is to begin. This delay reduces the time available to make any needed corrections before January 1, 2000.

For personal computers, IRS officials said they plan to replace about 35,000 personal computers and the associated systems software between February 1999 and July 1999 to achieve Year 2000 compliance. As a part of this replacement effort, IRS plans to reduce the number of commercial software and hardware products in its inventory from about 4,000 to 60 core standard products. According to IRS officials, thus far, IRS has completed testing on 5 of the 60 core products. IRS plans to complete the testing for the remaining 55 products by April 1999. IRS' goal is to eliminate all nonstandard products by July 1999.

Full Implementation of Year 2000 Changes Achieved for One of the Two Replacement Projects; Less Than Full Implementation Achieved for the Other

For one of IRS' two major system replacement projects, IRS implemented the Year 2000 changes at all 10 service centers by January 31, 1999; for the other system replacement project, 6 of the 10 service centers were using the full suite of Year 2000 changes for the system by January 31, 1999. IRS' two major system replace-

---

[8] In assessing progress, IRS determined that it needed to complete 85 percent of its application software work by January 31, 1999. The work for the remaining 15 percent includes the steps needed to certify that IRS has achieved Year 2000 compliance. IRS has deferred correcting about 2 percent of its application software until July 1999 and January 2000.

[9] The three areas are (1) voice mail for some of IRS' field locations; (2) telephone routing for IRS' automated collection system; and (3) telecommunications networks for at least 8,000 terminals. Work on these three areas is to be completed by July 31, 1999.

[10] IRS' goal for systems software and hardware was to complete 80 percent of the work by January 31, 1999.

ment projects are Service Center Mainframe Consolidation (SCMC) and the Integrated Submission and Remittance Processing (ISRP) System. SCMC is to consolidate the mainframe computer tax processing activities from the 10 service centers to 2 computing centers—thereby reducing the total number of tax processing mainframe computers from 67 to 12. Specifically, SCMC is to (1) replace and/or upgrade mainframe hardware, systems software, and telecommunications networks; (2) replace about 16,000 terminals that support frontline customer service and compliance activities; and (3) replace the system that provides security functions for on-line taxpayer account databases with a new system known as the Security and Communications System (SACS). Replacement of the terminals and the implementation of SACS are critical to IRS' achieving Year 2000 compliance. The other replacement project is ISRP. ISRP is a single, integrated system that is to perform the functions of two systems that are not Year 2000 compliant—the Distributed Input System that IRS uses to process tax returns and the Remittance Processing System that IRS uses to process tax payments.

SCMC

IRS completed the Year 2000 critical portions of SCMC by January 31, 1999. Specifically, in early October 1998, IRS completed its implementation of the 16,000 terminals that are needed for frontline customer service and compliance activities. Also, as of January 31, 1999, all 10 service centers were using SACS.

Originally, IRS had planned to have the other aspects of SCMC besides SACS—that is, the tax processing activities of the 10 service centers—moved to the 2 computing centers by December 1998. As of January 31, 1999, the tax processing activities for three service centers had been moved to the computing centers. IRS is determining the number of additional service centers that are to be moved in 1999. SCMC officials have developed several different schedule options for moving the tax processing activities of the remaining seven service centers. At the time we prepared this statement, IRS officials had not yet selected a schedule option.

According to IRS officials, the tax processing activities of all 10 service centers do not need to be moved before 2000 because the existing mainframes in each of the 10 service centers have been made Year 2000 compliant. Thus, in all likelihood, at the start of the 2000 filing season, some service centers will be processing their data locally, whereas others will have their data processed at the computing centers. IRS' Year 2000 end-to-end test is designed to include both processing scenarios.

ISRP

Both functions of ISRP—tax return processing and remittance processing—were to be implemented in November 1998. However, as a result of problems that occurred during the pilot test of ISRP and the contingency option IRS implemented for the 1999 filing season to address those problems, 4 of the 10 service centers are not to begin using the remittance processing portion of ISRP until August 1999.

For the 1999 filing season, the contingency option for ISRP is to retain enough of the old tax processing and remittance processing equipment in the service centers so that IRS could revert to the old systems if ISRP experiences problems. However, four of the service centers did not have enough floor space to accommodate both the old tax processing and remittance processing systems and the ISRP equipment. As a result, these four service centers are to continue using the old remittance processing equipment during the 1999 filing season and convert to ISRP in August 1999. These four service centers were among the top five remittance processing centers during the peak of the 1998 filing season. We recognize that this contingency option may have been the only feasible one for IRS. As we reported in December 1998, these four service centers are to receive their equipment late in 1999. As a result, their staffs will have no experience with the new equipment before the 2000 filing season in processing the large volume of remittances that occur in the peak of the filing season.[11]

TWO REMAINING CRITICAL YEAR 2000 ACTIVITIES STILL REMAIN; ONE OF WHICH IS BEHIND SCHEDULE

In addition to fixing its existing systems, IRS still needs to complete two critical activities for its Year 2000 efforts, and one of these activities is behind schedule. The two critical activities are the completion of (1) an unprecedented Year 2000 end-to-end test of 97 of IRS' 133 mission-critical systems and (2) 36 contingency plans for IRS' core business processes.

---

[11] *Tax Administration: IRS' 1998 Tax Filing Season* (GAO/GGD–99–21, Dec. 31, 1998).

Unprecedented End-to-End Test is to be Begin in April 1999

Using thousands of test cases, IRS' Year 2000 end-to-end test is to assess the ability of IRS' mission-critical systems to function collectively in a Year 2000 compliant environment. These cases are intended to replicate the many different kinds of transactions that IRS' information systems process on any given day to help assess whether IRS' systems can perform all date computations using data and systems date clocks with January 1, 2000, or later. The test will involve 97 of IRS' 133 mission-critical systems.[12] Most of IRS' mission-critical system application software has been tested individually; however, the ability of the application software to operate collectively, using Year 2000 compliant systems software and hardware, with all systems date clocks set forward to simulate the Year 2000, has not been fully tested.

In July 1998, IRS began the preliminary activities associated with conducting the end-to-end test. These activities included, but were not limited to, establishing a dedicated test environment to replicate IRS' tax processing environment, developing test plans and procedures, and doing some preliminary testing of some systems with the systems date clock set forward to 2000. Currently, IRS is developing baseline data from the 1999 filing season that will be ultimately used for the Year 2000 end-to-end test. The end-to-end test is to have two parts. The first part is scheduled to begin in April and end in July 1999. The second part is to begin in October and end in December 1999. The April test is to include the application software that is currently being used for the 1999 filing season. The October test is to include the application software changes that are needed for the tax law changes that are to be implemented for the 2000 filing season.

The need to conduct this test has in turn created an additional challenge in completing the work necessary for the 2000 filing season. As shown in table 1, to accommodate the Year 2000 end-to-end test, IRS revised its traditional milestones for implementing tax law changes for the 2000 filing season, thereby compressing the amount of time available to develop and test these changes. Under this compressed schedule, instead of having until January 2000, IRS must program and test all tax law changes that are to take effect in the 2000 filing season before September 30, 1999.

Table 1.—Key Activities Associated With Implementing Tax Law Changes, Traditional Milestones, and Revised Milestones as a result of Year 2000 Test Schedule

Key activity	Traditional milestone	Revised milestone as a result of Year 2000 testing requirements
Business requirements developed ..	Summer to January	Summer of 1998 to January 1999
Business requirements transmitted to Information Systems organization.	February to June	February 1999
Development of application software.	March to October	March to Mid-June, 1999
Systems acceptance testing[a]	Late August to mid-January.	Mid-June to September, 1999
Final phase of the Year 2000 end-to-end test.	N/A[b]	October to December, 1999
Implementation	January	January 2000

[a] IRS' systems acceptance testing assesses whether an application meets the specified user requirements.
[b] Not applicable.
Source: IRS data.

Under the compressed schedule, business requirements are to be delivered to IRS' Information Systems organization by February 28, 1999; the Information Systems organization is scheduled to complete the application software changes by June 15, 1999; and testing of these application software changes is be completed by September 30, 1999.

Staggered Milestones Developed for Completing IRS' Contingency Plans

In 1999, IRS is to complete the development of 36 contingency plans that IRS determined are needed to address various Year 2000 failure scenarios for its core busi-

[12] According to IRS' Product Assurance officials, 97 systems represent the maximum number of systems Product Assurance could effectively manage. Testing for the remaining systems is to be done by those organizations that have responsibility for maintaining them.

ness processes. IRS' initial goal was to have these plans completed by December 1998; however, IRS' revised goal is to complete 18 submissions processing contingency plans, 2 customer service contingency plans, and 3 key support services [13] plans by no later than March 31, 1999. One key support services contingency plan and 12 compliance contingency plans are to be completed by May 31, 1999.

In June 1998, we reported that IRS' Year 2000 contingency planning efforts fell short of meeting the guidelines included in our Year 2000 Business Continuity and Contingency planning guide.[14] Accordingly, we recommended that the Commissioner of Internal Revenue take a series of steps to broaden IRS' contingency planning effort to help ensure that IRS adequately assesses the vulnerabilities of its core business processes to potential Year 2000 induced system failures. Specifically, we recommended that the Commissioner take the following steps: (1) solicit the input of business functional areas to identify core business processes and identify those processes that must continue in the event of a Year 2000 failure; (2) map IRS' mission-critical systems to those core business processes; (3) determine the impact of information systems failures on each core business process; (4) assess existing contingency plans for their applicability to potential Year 2000 failures; and (5) develop and test contingency plans for core business processes if existing plans are not appropriate.

Since we issued our report, IRS has been taking actions to address our recommendations. IRS has solicited the input of its business officials and established working groups to identify failure scenarios and to develop the contingency plans. The working groups determined IRS should develop 36 contingency plans that cover various aspects of its core business areas of submissions processing, customer service, compliance, and key support services. One factor influencing the staggered schedule for completing contingency plans was that the staff assigned to develop plans have competing responsibilities, such as the development of business requirements to implement tax law changes as well as other business improvement initiatives. Under the staggered schedule, with the exception of the key support services area, earlier completion milestones were established for those aspects of three other core business areas that, according to IRS officials, were likely to experience a Year 2000 before the other areas. To the extent that the plans require additional actions, such as those associated with testing or preparatory activities, these delays reduce the time available to complete these activities.

According to IRS officials, the completion milestones of March and May 1999 reflect when the technical work for the plans is to be completed. Once that work is completed, the plans are to be approved by the official responsible for the core business process and tested. According to IRS officials, a contractor is still developing the testing approach. As a result, these officials could not provide us with the completion milestones and staff requirements for testing the contingency plans.

Other Business Initiatives Are Creating Competing Demands On Certain Staff Needed For Year 2000 Efforts

In addition to Year 2000 efforts, IRS has other ongoing business initiatives that are placing competing demands on its information systems and business staff. The Commissioner's Executive Steering Committee (ESC) and IRS' risk mitigation efforts have provided a forum for addressing these issues.

Concurrent with its Year 2000 efforts, IRS is continuing to make changes to its information systems to accommodate changes resulting from various business initiatives. These initiatives include the SCMC project that we discussed previously, implementation of the IRS Restructuring and Reform Act provisions, and of various taxpayer service initiatives.[15] While we do not question the importance of these initiatives, as we have said before, the need to make a significant number of tax law changes for the 2000 filing season introduces an additional risk, albeit one that we could not quantify, to IRS' Year 2000 effort.[16]

---

[13] Key support services include internal business processes, such as maintaining buildings and executing budget functions and payroll activities.

[14] *IRS' Year 2000 Efforts: Business Continuity Planning Needed for Potential Year 2000 System Failures* (GAO/GGD–98–138, June 15, 1998).

[15] The Commissioner of Internal Revenue established the Taxpayer Treatment and Service Improvement Program in November 1997 to plan, coordinate, and manage hundreds of commitments for improvements in service to taxpayers that have emanated from various sources. These sources include the National Performance Review, Senate Finance Committee hearings, and the IRS Restructuring and Reform Act.

[16] *Internal Revenue Service: Impact of the IRS Restructuring and Reform Act on Year 2000 Efforts* (GAO/GGD–98–158R, Aug. 4, 1998).

In November 1997, the Commissioner established the ESC Steering Committee (ESC) to identify risks to the 1999 filing season and the entire Year 2000 effort and to take actions to mitigate those risks. In addition, IRS hired a contractor to conduct periodic risk assessments. The contractor's most recent report was issued in December 1998.

Recent ESC documents, the contractor's December 1998 risk assessment report, and our interviews with SCMC officials, have identified the following examples of competing demands on staff in IRS' Information Systems organization and business organizations:

• Documents prepared for the September 1998 ESC meeting stated that IRS' Information Systems organization that is responsible for systems software issues was "overextended" because of Year 2000 demands, SCMC, and support for the Year 2000 end-to-end test.

• The contractor's December 1998 risk assessment report indicated that some of IRS' core business area staff face competing demands from the need to (1) identify business requirements for the 2000 filing season and (2) complete Year 2000 contingency plans. As we said previously, IRS' goal is to have business requirements completed by the end of February.

• According to the minutes from the January 1999 ESC meeting, IRS' Internal Audit has also raised a concern about the availability of sufficient staff to support the Year 2000 end-to-end test given the other Year 2000 demands. According to IRS officials, Internal Audit has not released a formal report on this matter.

• IRS' draft paper on the SCMC schedule options states that one of the risks for each of the schedule options is the resource drain on IRS staff and contractors from the filing season, the Year 2000 end-to-end test, and critical staff being used to train any new SCMC staff. The draft option paper notes that the extent of the drain varies somewhat depending on how many service centers are to have their tax processing activities moved to the computing centers in 1999.

Over the last several months, IRS has taken various actions to address these competing demands. For example:

• To address the "overextension" of the Information Systems organization that is responsible for systems software, the Chief of that organization said that he obtained contractor support and transferred staff from other areas. He said the additional staff, coupled with the delays in moving the tax processing activities of the service centers to the computing centers, helped alleviate this overextension.

• To address the competing demands on the business staff to develop Year 2000 contingency plans and finalize business requirements for the 2000 filing season, IRS officials decided to stagger the completion milestones for contingency plans.

• To help prioritize the work within the Information Systems organization IRS officials told us they have established another executive steering committee. In addition, the minutes from the January 1999 ESC meeting said that the Commissioner has asked the cognizant staff to identify the source of each of the 2000 filing season requirements—(i.e., IRS Restructuring and Reform Act, Taxpayer Service Improvement Initiative, etc.). This identification is the first step for providing the additional information that would be useful for establishing priorities for IRS' Information Systems staff.

CONCLUDING OBSERVATIONS

Since our testimony in May 1998, IRS has made considerable progress in completing its Year 2000 work. However, IRS did not complete all the work that it had planned to do by January 1999. This unfinished work and upcoming critical tasks are to be completed in the remainder of 1999. At the same time IRS is addressing its Year 2000 challenge, it is undertaking other important business initiatives, such as preparing for the 2000 filing season and implementing SCMC. These various initiatives place competing demands on IRS' business and Information Systems staff. To date, IRS has taken actions to address these competing demands, including delaying the completion milestones for some Year 2000 activities.

In the next 5 months, IRS will pass several key milestones. As IRS passes each one, it will have more information on the status of its Year 2000 effort and the amount of remaining work. This information should help IRS and Congress assess the level of risk to IRS' core business processes in 2000. For example:

• By the end of February 1999, the business organizations are to submit their requirements to IRS' Information Systems organization for the 2000 filing season. In the event that business requirements for the 2000 filing season are not submitted on time, IRS increases the risk that some tax law changes may not be thoroughly tested before they are implemented.

• From April to July 1999, IRS is to conduct its Year 2000 end-to-end test. The results of this test will be an indicator of the extent to which, for the work completed thus far, IRS has been successful in making its systems Year 2000 compliant. The results of this test should also provide information on how many Information Systems staff will be needed for correcting any problems that are identified.

• By the end May 1999, IRS is to complete its contingency plans. These plans should provide information on any additional steps needed to implement the plans.

We plan to continue to monitor IRS' progress in meeting these key milestones.

Mr. Chairman, this concludes my prepared statement. I welcome any questions that you may have.

Chairman ARCHER. Mr. White, thank you. And thank you for also giving us a little time back. We appreciate it.

Mr. WHITE. You're welcome.

Chairman ARCHER. Mr. Commissioner and Mr. Cosgrave, this country owes both of you a deep debt of gratitude for coming to its aid at a time of great need. I know there are many other things that you could do with your lives very productively in our society, and I for one congratulate you and compliment you on being where you are and the kind of job, the professional job, that you are committed to do and which you are undertaking with a very, very complicated, far-flung, difficult operation to manage.

I suppose your computer system is about the largest in the world, is it not?

Mr. ROSSOTTI. Well, it's one of the largest. Yes. Depends on how you measure it.

Chairman ARCHER. So this is not a small problem; this Y2K is not a small problem for you. Are you satisfied at this point that when we go into next year that the IRS will be able to perform its essential services in a timely manner?

Mr. ROSSOTTI. First of all, let me just thank you for your opening comment, Mr. Chairman. I really appreciate that very much.

The answer to your question, yes. I am confident that we will be able to perform our central mission. I do want to qualify that with the fact, as we said repeatedly, that I think we will be able to sufficiently test broadly to be sure that we will meet, be able to continue to function our central mission. But we won't be able to test every possible combination of everything.

That's why there still will remain the possibility, the risk, of particular problems that may occur. And that's why we are organizing what we call our end-game strategy, not our end-to-end tests, but our end-game strategy, which means that we will be prepared to respond to things that are unexpected, that come up, so that we can get them out of the way quickly.

Chairman ARCHER. My question assumes that you will have contingency plans in the event that there is some snag in your computer operation so that your services can still performed in a timely manner. Is that a fair statement?

Mr. ROSSOTTI. I'll let Mr. Cosgrave mention some of the contingency plans, but I do want to not mislead, Mr. Chairman and others. The contingency planning that we're doing is aimed at being able to respond if there's a temporary outage in a particular area, for example. There really is no contingency plan, broadly speaking, that if our computer systems were not functioning in a predomi-

nantly successful way that we could really, really execute an entire filing season. So, I mean there are contingency plans that are very important to do, but they are not contingency plans that, say if the whole IRS computer network were not functioning, that we could still do a tax season.

I don't think we need a contingency plan for that. First of all, there really isn't a contingency plan for that. But I believe we have more than adequate confidence that we are not going to have a global failure of that kind. But having said that, let me just ask Paul here to talk about some of the contingency planning that we are doing.

Mr. COSGRAVE. Thank you, Mr. Commissioner.

Let me, first, just acknowledge GAO's assistance here. They reported back in June of last year that the IRS was behind in their contingency planning. We took that recommendation to heart—in fact, adopted an approach that they laid out to us that had already been used effectively at the Social Security Administration as the way to go about this problem. In fact, we, are executing the exact model that they have identified. This involves addressing this problem from the business perspective. We have each of our businessowners actively involved in building contingency plans. First of all, they are identifying which contingency plans are needed based on the critical business processes that we need those plans for. They did that work and that's complete. We have identified the need for 37 plans. Twenty-four of those 37 plans will, in fact, be completed by March, and the remaining 13 will be done by May. So by May of this year, we will have contingency plans in place for all of our critical business applications.

Chairman ARCHER. Are you confident that all refund checks will go out in a timely fashion next year?

Mr. ROSSOTTI. Well, I think that gets to the point. We are confident that we will be able to process refund checks. They will be able to go out in a timely manner. But when you say all refund checks, I have to say I can't be confident of that because there could be particular situations for particular taxpayers because of some particular path that they go through that we haven't tested, where there could be, as we call it, a glitch.

I don't predict that. I certainly don't want that to happen, but we also don't want to offer false confidence that there won't be any problems. This is why we are preparing not only contingency plans, as Paul mentioned, but also quick response situations, so that if we find a particular problem, as we do in every filing season, actually, we'll be able to respond to it quickly and hopefully minimize any taxpayer impact to the bare minimum.

Chairman ARCHER. Do all refund checks go out today in a timely manner.

Mr. ROSSOTTI. Actually, most do. [Laughter.]

But there are some that don't.

Chairman ARCHER. Even without the Y2K problem, you can't make that a blanket statement?

Mr. ROSSOTTI. That's actually an excellent observation. That's very, very true. Every filing season there are problems.

Chairman ARCHER. My last question is, is there anything further that the Congress can do to help you to do your job?

Mr. ROSSOTTI. Well, let me just say that in my year or so here, I have been very pleased with the response we have gotten from the Congress. We have gotten just about everything we've requested from the Congress. At this moment, with respect to the IRS Y2K problem, I don't think there is. I did mention in my testimony, that one of the things we are studying in our role as tax administrator, is to make sure that we are prepared in case there are taxpayers who have, problems in filing or paying timely because of a situation that might develop totally beyond their control. For example, with their bank.

We haven't completed this study yet, but this is something we are going to be working on with the Treasury. We want to make sure that we are prepared and able to deal with those situations to avoid any harm to the taxpayers. We may need to consult with the Committee over the course of this year, over the next few months even, as we study that issue to make sure that we have the requisite authority to deal with that.

We will continue to consult with you on this issue throughout the year. As of this moment, I think we have what we need.

Chairman ARCHER. OK. Thank you very much. If you need anything else, we invite you to let us know immediately so we can go to work in working with you.

Ms. Thurman.

Mrs. THURMAN. Thank you, Mr. Chairman. We appreciate all of you being here today. If for no other reason, these hearings are good to keep the public aware that this is an issue still ongoing, probably to give some more confidence that we are in better shape than what some have anticipated so that we don't have runs on banks and we don't have some of the things that we are all very concerned about.

But, Mr. Dennis, I really need to ask you some questions because, and I'm sorry I was not here for your testimony when you were actually saying it, but I do have the testimony that you have written before. And I need some clarification on the last page because it says there that financing is not a major impediment to action at this time. Only 3 percent now planning action say that the reason that they have not done so to date is the financing problem. Few small business owners-respondents mentioned finance. I guess this is in the form of your survey. However, for some, the out-of-pocket costs will be significant, and ones they would not normally make. This is not a question of locating debt-finance to undertake the preventive measures, that appears readily available. It is a question of paying for them.

You've lost me somewhere in here. One minute it doesn't seem it's about cost, and then the next minute it seems to be about cost. So I need some clarification on that, particularly because you know that I've introduced a piece of legislation to try to do an accelerated depreciation for businesses specifically for the purposes of kind of grabbing the attention of small businesses that they really need to get into this Y2K compliance issue.

So if you could give me some direction, I would be very appreciative.

Mr. DENNIS. Surely. Thank you.

Most small businesses who have taken action already tell us that they are spending relatively small amounts of money. When I say most, 75 percent have spent less than $5,000. There are exceptions, those spending large sums, over $50,000. It's a very small percentage thus far, one, 2 percent at most.

My reference to financing not being a major problem is tied to the survey. We provided respondents with reasons for not going ahead. Financing was one of them. I think it was 3 percent who indicated that that was a problem impeding them from going forward. So yes, there are extreme cases where it is going to be difficult. There's no if, ands, or buts about it. But for the most part, it is not an issue. Owners have told us that that is not an issue.

When it comes to debt capital, the Small Business Administration's, SBA's 7(a) program, is a back up. Not only that, in the 20-some years that I have been working at NFIB, the present is probably the most favorable conditions for small-business borrowing I've seen. So that's not an issue either.

Mrs. THURMAN. However, they are familiar with the Code that does allow them that accelerated depreciation so they might be a little bit more familiar with this, might be more comfortable in using some kind of tax issue.

But let me just make this comment too because I think this is really important, and I'm real concerned after reading this. I don't know if you were here this morning when I read from an article about what businesses were doing, and they are doing something called "windowing" and "encapsulation," which may not be the wherewithal of the fix that some of them are going to put themselves in believing that they are going to spend this extra dollar or they are going to roll their computer back. And then all of a sudden it quits anyway. Do we know what's happening with small businesses in that way? I'm going to talk about it when I'm home, but I think we have to capture their attention on this because I'm really concerned.

Mr. DENNIS. I couldn't agree with you more in the sense that many simply don't believe it, simply don't believe this is going to affect them and don't think it's a problem. So I couldn't agree with you any more. I think there's a number of things that could be done just on awareness issues. One of the things that's really been disappointing is the use of industry-specific trade associations to get this message out, even more so for embedded-chip-type equipment that's particular to certain industries than for computers in general.

I think that vehicle could be used to a much greater extent than has been done in the past. Any type of awareness activity I think is something good to do because there are many owners out there who just don't believe it, don't believe it will affect them, and feel that it's not worth the effort to do anything.

Chairman ARCHER. The gentlelady's time has expired. Mr. Weller.

Mr. WELLER. Thank you, Mr. Chairman. Before I ask my questions, I also want to salute the Commissioner of the IRS for the commitment you've shown to implement IRS reform. The first IRS reform began in this Committee room under the leadership of our Chairman and the Ways and Means Committee. And the follow

through, I definitely want to salute you on your commitment to following through on IRS reform, making IRS responsive to the taxpayer, rather than the other way around. So thank you for that.

I'm going to keep the focus of my questioning also on small business, Mr. Dennis. In your knowledge and you pointed out in your response to Ms. Thurman's questions, that some small business owners don't believe anything is going to happen so they are not going to worry about it. What do you feel is really the remaining big risk for small business in being Y2K compliant, and particularly as it relates to taxes and tax collection.

Mr. DENNIS. I think the greatest risk, quite frankly, is getting people to do something. That's the first major one. The second one, I would suggest, probably is a little bit different than you may think. I worry a great deal about embedded chips and what it's going to do to some firms. Now you say, how does that affect taxes? Well, it affects taxes because they are going to have to put all their resources and energy into correcting any Y2K problem, whatever that problem is. If their equipment goes down, the key to their survival is going to be how quickly they can be up and running. That is the absolute critical thing. So it's possible that some dates can slip and that kind of thing.

I was very encouraged when Mr. Rossotti indicated that IRS was developing some sort of internal policy which might address that problem. Indeed I mentioned that in my written testimony. I would like to see a policy made public to really encourage people to take action. The IRS policy would really encourage a lot of people to say "Well, gee, if there is some kind of consideration and if I have done something to address the potential problem, that might be a very strong incentive to prepare."

Mr. WELLER. Who is, you know, you had mentioned that perhaps the trade organizations and business groups could be better utilized to get information out. Who is everyone depending on for information today? Where are small business owners getting their information if it's not coming from their professional or trade organization?

Mr. DENNIS. That's a very good question, and I don't know that I have a good answer for you. We hear anecdotally, but that was not one of the questions I asked on the survey. Anecdotally, we believe that they are getting a lot of information from the net. They are getting some from general business magazines, including their trade association-type magazine. It's kind of a catch-as-catch-can. One of the problems is that there seems to be a lack of simplistic—no, I don't want to use the word simplistic—relatively easy, step-by-step approaches to how you specifically handle problems discovered. Some Internet addresses, for example, provide very complicated solutions.

Mr. WELLER. Is there one, you know, if you were able to do one thing to do a better job of getting information out there to help small business owners deal with Y2K compliance, what would that initiative be?

Mr. DENNIS. Having Mr. Koskinen or someone grab trade association execs by the back of the neck and say, this has got to be done.

Mr. WELLER. And so those trade organizations in the audience make a note of that, be thinking how they can communicate to their members.

And last, I realize the light's yellow here, but are there any particular tax incentives that may help small business better comply and afford the cost to comply, realizing that small business, and many of them are mom and pop shops, limited on resources and staff?

Mr. DENNIS. Tax incentives are always nice. But in terms of getting more people to do things to resolve their potential Y2K problems, I haven't seen any evidence they would. Obviously there will be a few, but not an overwhelming number.

Mr. WELLER. All right. Thank you.

Chairman ARCHER. Mr. Foley.

Mr. FOLEY. Thank you, Mr. Chairman.

Mr. Rossotti, in your written testimony, you touched briefly on the end-to-end testing. Can you explain the rigor of your end-to-end test, and also give us a little greater detail on that and when it may be complete.

Mr. ROSSOTTI. I think I'll ask Mr. Cosgrave, if it's OK, to respond to that. He's directly in charge.

Mr. COSGRAVE. The end-to-end test is a totally integrated test, where we are taking most of all our systems and putting them together in a totally integrated environment, that includes almost 95 different systems linked together. We're doing this in three different phases. The first two have already been completed. And the 1st part of the third phase will start in April and will run into July of this year. From my experience, and I believe the Commissioner has the same experience having done a lot of systems testing in other businesses, this is as complex, as complete, and as large a test as we have ever seen anyone undertake. It's running well to date, and we anticipate having those mission-critical systems tested and-to-end beginning in April.

Mr. FOLEY. There's also discussion on—oh, did you want to——

Mr. ROSSOTTI. I was just going to add one thing. One of the key things about this that is different from the other testing that we do, is that we take a special computer and we actually set the clock forward so we make believe it's already January 1, 2000. That's the one thing that we can't do in our normal testing, because we can't change the actual computer clocks or we'll make everything run awry. This actually involves taking a separate set of computers and operating them with the clock set forward.

Mr. FOLEY. You also touch on, you mentioned it briefly in response to the chairman on contingency planning. It seems to me that the most critical part of it is to have a backup plan in case. What is that plan for processing returns, to assure customer assistance, and, of course, compliance in general.

Mr. ROSSOTTI. Well, again, I'll let Mr. Cosgrave give you some detailed examples of our 37 contingency plans. But I again need to stress that there really is no contingency plan that, given a computer failure, broadly speaking, that will allow us to continue to do the business of the IRS. We are just too dependent on these computers, and there isn't any really practical backup plan you could have on a broad scale. So our strategy is to use our end-to-end tests

to make sure we don't have a broad failure, recognizing there could be limited failures.

Our contingency plans are basically designed to cope with those kinds of localized or specific failures. That's why there are 37 of them. Mr. Cosgrave can give some examples of what these are.

Mr. COSGRAVE. I'll give one or two examples. In fact, I happen to have brought one of those plans with me today. This is the FTD, Federal Tax Deposit, contingency plan. It gets very specific. For example, on January 3, if something is not operating the way it should, who will be there to provide backup support? What exactly are the approaches we would take as a workaround to the problem? It's got phone numbers; it's got every conceivable thing we would need in an emergency situation.

The major systems that I described earlier that we're implementing, where we are actually replacing the system and hence have the most risk, would be our submissions processing and our remittance processing systems. In those cases, we are actually, in the case of remittance processing, keeping the old system around. Even thought it won't be Y2K compliant, we know we can trick the system to fake out the date factor, and we'll use that as a fallback. But again, those systems are 20 years old, and frankly we are glad to have the opportunity to replace them and get some new technology in there. But they will be there in the backup mode, should we need them.

Mr. FOLEY. In the transition period, is there any security breach problems we may encounter through the electronic filing method? Is there any way for somebody to penetrate the computer system to alter data?

Mr. COSGRAVE. That's an interesting question. With the new integrated submissions-remittance processing system, we did detect in our final test one potential security breach. And so we actually de-installed a few components that would have allowed that breach. We have operated until just recently, when we were able to get a fix for that, with some of the functionality turned off. Now that we have fixed that problem, we are back in production with the system at full capacity.

Mr. FOLEY. Thank you, Mr. Chairman.

Chairman ARCHER. Ms. Thurman would like to make a short inquiry, and I believe that will conclude this panel.

Mrs. THURMAN. Chairman Rossotti, what I'd like to ask is, if you could get me some information of how many of our small businesses are using section 179? That might give us a better idea of whether tax incentives, depreciables, the kinds of things that we would look in looking at ways we might help.

Mr. ROSSOTTI. Unfortunately, the IRS does not have reliable data documenting whether businesses located in empowerment/enterprise zones are using the additional expensing allowance for depreciable business property as allowed for in section 179 of the Internal Revenue Code. Use of this provision is very infrequent. The General Accounting Office noted this finding in their June 1998 report, Community Development—Information on the Use of Empowerment Zone and Enterprise Community Tax Incentives. The report states "IRS officials reported that none of the information on expensing and depreciation that businesses or individuals file on

Form 4562 (Depreciation and Amortization) is computerized and entered into a master file." In addition, further review of sample data for tax year 1996 indicated that of 124 returns with expensing deductions large enough to indicate that they might be eligible for the additional EZ expensing allowance, almost none were. The Department of Treasury found similar results for tax year 1995.

As the IRS transitions to four operating units designed to serve unique groups of taxpayers, the need for more specialized data about customer segments will increase. While the Small Business/Self Employed Operating Division may not collect specific information in the future about section 179, they will have an opportunity to collect more specialized data about their customers, small businesses and self-employed taxpayers. This will allow IRS to better understand the needs of these taxpayers and share that information with Treasury and Congress.

Chairman ARCHER. The Committee will stand in recess for the vote on the floor. We'll go vote and come back as quickly as possible and reconvene.

Glad to see our next panel is already assembled at the witness table. And Mr. Magaw, we're going to start off with you if you are ready. And if you will identify yourself and whom you represent, for the record, you may proceed.

Our general ground rules are that we'd like for you to keep your verbal testimony to within 5 minutes, and the lights will come on. And your entire printed statement, without objection, will be inserted in the record.

Mr. Magaw.

STATEMENT OF JOHN W. MAGAW, DIRECTOR, BUREAU OF ALCOHOL, TOBACCO, AND FIREARMS

Mr. MAGAW. Thank you, Mr. Chairman. My name is John W. Magaw and I'm the Director of the Bureau of Alcohol, Tobacco, and Firearms. Members of this Committee, I am pleased to appear here today concerning an extremely important issue, that of Y2K compliance. Accompanying me today, is Mr. Pat Schambach, and he's like you, Mr. Chairman, I think like you are right now, wearing two or three hats.

At ATF, he is the assistant director for science and technology. He's also our chief of information. And also he is our senior executive for year 2000 compliance, and works on it virtually every day. And he's sitting to my left and will make a few comments in a moment.

Most people know ATF for our roles as regulators and enforcers of criminal laws relating to alcohol, tobacco and firearms. But it is not as well known that ATF is a major revenue collector. In Fiscal Year 1998, ATF collected a total of $12.4 billion, this includes $6.5 billion in alcohol taxes, $5.6 billion in tobacco taxes, and $300 million in firearms and ammunition taxes. We estimate that the multiple tobacco tax increase that is scheduled to begin in January of 2000 will expand the annual revenue by the year 2002 to more than $15 billion.

We fully appreciate that the continuity of revenue collection is critical to the Nation's well-being. Our budget for Fiscal Year 1999 is $608 million, and I am pleased to note that for the fourth con-

secutive year, ATF has received the highest possible rating on the annual general audit of our finances and internal controls. This audit was conducted by Price-Waterhouse-Coopers and the Treasury Inspector General's Office.

It is our intent to maintain a sound revenue management and regulatory system that continues to reduce taxpayer burden, improve service, collect the revenue due, and prevent illegal diversion. We continue to accomplish these objectives in large part through the partnership with the industry, taxpayers and through technological innovations. Our National Revenue Center, in Cincinnati, Ohio, had applied these two principles in improving the consistency of our tax administration in preparing for Y2K.

Mr. Schambach will detail more specifically the measures that we are taking, not only in the area of revenue collection, but also in all of the matters that impact our ability to serve the public of this Nation.

Thank you, sir.

[The prepared statement follows:]

Statement of John W. Magaw, Director, Bureau of Alcohol, Tobacco and Firearms

Thank you, Mr. Chairman, Congressman Rangel, and Members of the Committee. Accompanying me today is Mr. Pat Schambach who wears three hats here at ATF—Assistant Director for Science and Technology, Chief Information Officer, and Year 2000 Senior Executive.

With your permission, I will briefly provide an overview of the mission of the Bureau of Alcohol, Tobacco and Firearms before deferring the balance of my time to Mr. Schambach who will address ATF's significant Y2K conversion efforts.

ATF's three strategic goals are to reduce violent crime, protect the public, and collect the revenue. We administer and enforce the Federal laws and regulations relating to alcohol, tobacco, firearms, and explosives. Although perhaps not readily apparent, the commodities regulated by ATF share a common bond—each has legal consumer uses, the potential for serious abuse, and significant revenue implications.

In Fiscal Year 1998, ATF collected a total of 12.4 billion dollars—including $6.5 billion from the alcohol industry/ and $5.6 billion from commerce in tobacco. We estimate that tax increases effective January 1, 2000 on tobacco products will provide $2.5–$3 billion per year in additional revenue by 2002 as we implement the Taxpayer Relief Act of 1997. These collections are made with a budget of approximately $600 million. All funds are transferred to the Treasury or other Federal agencies for further distribution in accordance with various laws and regulations.

Permit me to note that for the fourth consecutive year, ATF has received the highest possible rating on the annual General audit of our finances and internal controls. This audit was conducted by Price Waterhouse Coopers and the Treasury Inspector General.

It is our intent to maintain a sound revenue management and regulatory system that continues to reduce taxpayer burden, improve service, collect the revenue due, and prevent illegal diversion.

We continue to accomplish these objectives, in large part, through partnership with industry members, States, and other Federal agencies—and through technological innovation. Our National Revenue Center has applied these two principles in improving the consistency of our tax administration, and providing timely trend analyses and industry statistics.

ATF has used the integration of partnership and innovation to identify and overcome the potential vulnerabilities that the Year 2000 portends. We fully appreciate that the continuity of revenue collection is critical to the Nation's well-being.

Mr. Schambach will detail the measures we are taking not only in the area of revenue collection but also in all matters that impact our ability to serve the public.

STATEMENT OF PATRICK SCHAMBACH, ASSISTANT DIRECTOR, SCIENCE AND TECHNOLOGY, CHIEF INFORMATION OFFICER, AND YEAR 2000 SENIOR EXECUTIVE, BUREAU OF ALCOHOL, TOBACCO, AND FIREARMS

Mr. SCHAMBACH. Thank you, Mr. Director. Mr. Chairman, we first established our program—sorry

Chairman ARCHER. Mr. Schambach, if you will give your full name and the entity that you represent, you may proceed.

Mr. SCHAMBACH. Thank you, sir. I'm Patrick R. Schambach, Assistant Director of the Bureau of Alcohol, Tobacco, and Firearms. Mr. Chairman, we first established our program in ATF to address the Y2K challenge in 1996. As you have heard from many other witnesses, we soon discovered the Y2K challenge has tentacles into every corner of our organization and extends beyond the boundaries of our organization into relationships with other entities.

Our primary efforts can be categorized into the following major areas, information technology systems, non-information technology systems, business continuity and contingency planning, crisis management and outreach. Over 30 full-time-equivalent positions, both ATF employees and consultants, support these efforts in our program management office. Additionally, representatives from all core business areas of our bureau actively participate in each of these efforts.

In 1997, an integrated project team was established. This team, chaired by me, was established to provide an open forum for communicating Y2K status throughout our organization and for raising and resolving Y2K business issues.

I'd like to focus my remarks in two distinct parts, those activities aimed at internal ATF preparations, followed by external preparations aimed at preserving the smooth flow of revenue that ATF is charged to collect from the alcohol, tobacco and firearms industries.

The chart on the easel to your left, which I will explain in a few minutes, indicates the volume of dollars collected from each of these regulated industries in Fiscal Year 1998. In our internal preparations we have identified 156 information technology systems in operation within ATF. Of these, 24 are mission-critical, and all 24 have completed assessment. Nineteen are now year 2000 compliant, and 5 systems remain to be replaced. And efforts are under way to replace these five systems during Fiscal Year 1999.

Through a major technology upgrade using a new acquisition method in the Federal Government, called Seat Management, last year we provided Y2K-compliant personal computers to all ATF employees. We are certifying all other computer hardware to provide the best assurance possible that our processes will continue to function properly. Concurrently we are updating our contingency plans that have been developed for each mission-critical system so that we have realistic and actionable alternatives should we experience unexpected failure.

We have also identified 129 non-information-technology systems within ATF, to include building security systems, laboratory equipment, and other devices that contain computer chips and computer logic. Of these, 85 are mission-critical. Eighty of these systems

have been assessed, and 32 are Y2K compliant. Renovation plans are in place to repair, replace or retire the remaining systems determined to be non-compliant.

We are also updating our contingency plans that have been developed for non-IT mission-critical systems.

While it's our goal to avoid any unexpected surprises to ensure our vital processes remain intact, or can be resumed most expeditiously, we are developing business continuity plans relative to our core processes. That is, we want to have plans in place should any infrastructure or facility failure occur that is totally out of our control.

Concurrently, we have started planning efforts for an ATF crisis management operation to be in effect for the century date change holiday period. The primary purpose of this initiative is to have in place a centralized team that will have the authority and expertise to receive reports of suspected Y2K failures, analyze them, and make appropriate business decisions. I expect to have this team in place and operational in late 1999, working through the New Year's holiday weekend, and collecting input from more than 220 locations throughout the country.

Now a few words about our external preparations. As you can see from the chart, ATF is responsible for collecting over $12 billion annually in Federal excise and other taxes. That amounts to approximately $500 million collected every 2 weeks, with the first payment in the new year is due January 14. Even a minor delay in that flow of funds can be costly both to the government and to the American taxpayer.

Let me take a minute to walk you through the chart, beginning on the right side. A small amount of our revenue, approximately $2 million, comes from the tax to transfer certain controlled weapons, such as machine guns that have been controlled by law since 1935. Excise taxes are collected from manufacturers of guns and ammunition to the tune of $165 million last year. Special occupational taxes are imposed on those involved in the distribution chain of alcohol, tobacco, and firearms products, which amounted last year to $106 million.

And, finally, firearms and explosives dealers paid license fees to the tune of $4 million.

That brings us to the larger of Federal excise taxes on alcohol, on the top half of the pie chart, showing by industry, beer producers paying over $3 billion, distilled spirits producers just under $3 billion, and wine producers, almost half a billion dollars.

Tobacco producers also pay excise taxes of over $5 billion. In this last category, as the Director mentioned, with the tax increases already passed by Congress, revenue from tobacco will increase our overall collections to approximately $15 billion.

Now, to protect the smooth flow of this revenue, ATF initiated a proactive outreach program in the summer of 1998. We began by visiting several of our largest taxpayers, primarily large producers in the beverage alcohol industry to discuss mutual Y2K concerns and preparations. I've also addressed an industry-wide Y2K task force of alcoholic-beverage-industry representatives. As recently as last week, we hosted major alcohol and tobacco industry members

at our headquarters and via teleconference in a meeting to continue these important conversations.

Our outreach efforts are aimed at assisting industry members with contingency plans for tax calculations and payment processes in order to prevent any disruption to the flow of Federal excise tax revenue. I've been invited to address a major industry conference next month to explain our expectations for industry.

And complementary to these conversations, we are creating a Y2K Internet site that will be designed to streamline communication with our industry partners and taxpayers.

In concert with these efforts, similar to comments of Commissioner Rossotti in the earlier panel, we are looking at internal policies that would enable ATF to mitigate or waive penalties for late payments due to Y2K disruptions which are out of the control of our taxpayers.

Finally, in addition to our efforts with our industry partners, we are also working with other Federal agencies, such as our sister bureau, the Financial Management Service, the Federal Reserve and its financial institutions to ensure that there will be no disruptions to the revenue flow.

In closing, we are confident that ATF has a viable Y2K program that is linked to the success of our core business areas, and we will continue to work diligently to assure the continuation of our mission. We have enjoyed our longstanding partnership with industry, and we look forward to building on that relationship as we deal collectively with year 2000 issues.

Thank you, Mr. Chairman.

[The prepared statement follows:]

Statement of Patrick Schambach, Assistant Director, Science and Technology, Chief Information Officer, and Year 2000 Senior Executive, Bureau of Alcohol, Tobacco, and Firearms

INTRODUCTION

I am Patrick Schambach, Assistant Director of Science and Technology at the Bureau of Alcohol, Tobacco and Firearms. Additionally, I am the Bureau's Chief Information Officer (CIO) and Year 2000 Senior Executive. I appreciate the opportunity to acquaint you with the status of ATF's year 2000 program, our renovation efforts and our remaining challenges that will ensure the continuation of vital services provided through ATF programs.

BACKGROUND

ATF established a program in 1996 to address the Y2K challenge. As with many organizations, the initial focus of our program was to educate our people and assure our Information Technology systems were compliant with the century date change. As our awareness and knowledge increased it quickly became evident that the scope and focus of our program had to change to meet those challenges. What began as a modest Information Technology (IT) effort, consisting of 67 legacy application systems, now encompasses over 150 application systems Bureau-wide and a myriad of hardware, commercial software, and other specialty equipment and infrastructure areas that affect ATF's core business activities. As you have heard from many other witnesses, the Y2k challenge has tentacles into every corner of our organization, and extends beyond the boundaries of our organization into our relationships with many other entities.

Y2K Program Structure

Our Year 2000 efforts can be categorized into the following major areas:

Information Technology Systems, Non-Information Technology Systems, Business Continuity and Contingency Planning, Crisis Management, and Outreach. Over 30 full-time equivalent positions, both ATF employees and consultants, support these

efforts. Additionally, representatives from other Bureau core business areas outside of the IT organization actively participate in each of these major efforts. In 1997 an Integrated Project Team was established. This team, chaired by me, was established to provide an open forum for communicating Y2K status throughout our organization and for raising and resolving Y2K related business issues.

Current Status

I'd like to focus my remaining remarks in two distinct parts—those activities aimed at internal ATF preparations for the century date change—followed by external preparations aimed at preserving the smooth flow of revenue that ATF is charged to collect from the alcohol, tobacco and firearms industries.

Internal Preparations

Information Technology Systems: We have identified 156 Information Technology systems in operation within ATF. Of these, 24 are mission critical. All 24 have completed assessment: 19 are Year 2000 compliant and 5 systems remain to be replaced. System development efforts are underway to construct Y2K-compliant replacements for these 5 systems in FY '99. Additionally, we are certifying our hardware platforms to provide the best assurance possible that our client-server computers and personal computers will function properly. Concurrently, we are updating our contingency plans that have been developed for each of our mission critical systems, so that we have realistic and actionable alternatives should we experience an unexpected failure.

Non-Information Technology Systems: We have identified 129 Non-Information Technology Systems within ATF. Of these, 85 are mission critical. Eighty of these systems have been assessed, and 32 are Year 2000-compliant. Renovation plans are in place to repair, replace or retire the remaining systems determined to be noncompliant. In addition, several facility and security assessments at key ATF locations throughout the country are underway. As with the IT effort, we are updating our contingency plans that have been developed for each of our Non-IT mission critical systems.

Business Continuity/Contingency Planning and Crisis Management: While it is our goal to avoid any "unexpected surprises," to insure our vital business processes remain intact or can be resumed in the most expeditious manner, we are developing business continuity plans relative to our core business processes. Concurrently, I have started planning efforts for an ATF Crisis Management operation. The primary purpose of this initiative is to activate a centralized team during the century datechange period. This team will have the authority and expertise to receive reports of suspected Y2k failures, and to analyze, resolve and make appropriate business decisions to effectively address unplanned outages anywhere within ATF operations. I expect to have this team in place and operational in late 1999, working through the New Year's holiday weekend, and collecting input from more than 220 ATF locations throughout the country.

External Preparations

As you can see from the chart presented here in the hearing room, ATF is responsible for collecting over $12 billion annually in federal excise and other taxes. On this chart ATF revenues are broken down by industry-type to give you an idea of our tax-paying "customer" base.

Outreach: With the intent of protecting the smooth flow of this revenue, ATF initiated a proactive outreach program in the Summer of 1998. My counterpart, Mr. William Earle, the Bureau's Chief Financial Officer and I began by visiting several of our largest taxpayers, primarily large producers in the beverage alcohol industry, to discuss Y2k concerns and preparations. I have also addressed an industry-wide Y2K Task Force of alcoholic beverage industry representatives. As recently as last week, we hosted alcohol, tobacco, and firearms industry members at our headquarters -and via teleconference -to continue these important conversations.

Our outreach efforts are aimed at assisting industry members with contingency plans for tax calculations and payment processes in order to prevent any disruption to the smooth flow of federal excise tax revenue. I have been invited to address a major industry conference next month to explain our expectations for industry in preparing for the century date change. Complimentary to these conversations, we are creating a Y2K Internet site that will be designed to streamline communication with our industry partners and taxpayers. It is our intent to provide pertinent ATF Y2K information that will be useful to our industry partners and will provide them a direct link to address concerns.

In concert with these efforts, we are looking at internal policies that would enable ATF to mitigate or waive penalties for late revenue payments due to Y2K disrup-

tions which are out of the control of the taxpayer. Finally, in addition to our efforts with our industry partners, we are also working with other Federal agencies and financial institutions to ensure that there will be no disruption to the revenue flow process.

CLOSING

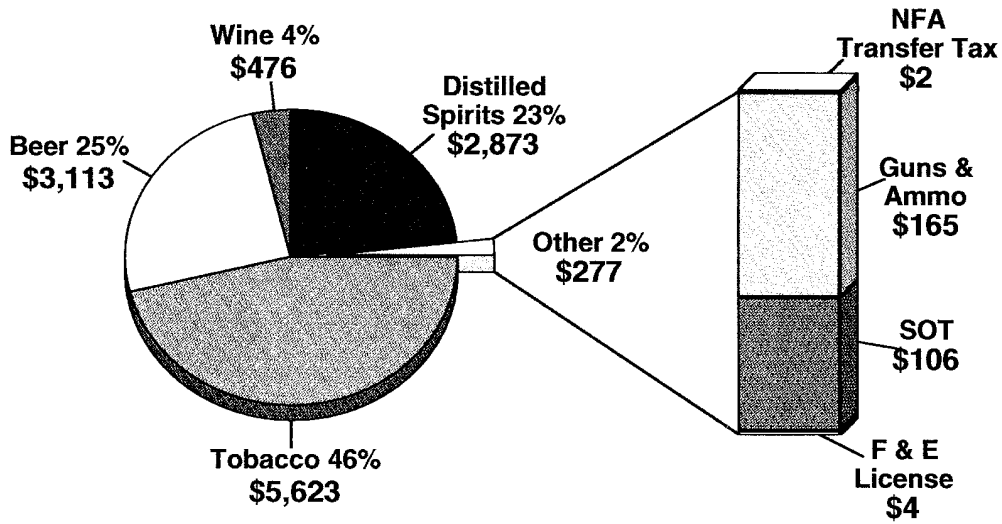
In closing, we are confident that ATF has a viable Y2K program that is linked to the success of our core business areas. We will continue to work diligently to ensure the continuation of our mission. We have enjoyed our long-standing partnership with industry and we look forward to building on that relationship as we deal collectively with year 2000 issues.

Thank you again for the opportunity to appear before you today. I would be happy to answer any questions you may have.

BUREAU OF ALCOHOL, TOBACCO AND FIREARMS

Revenue for FY-98

Amounts in Millions $



Total Collections = $ 12.4 Billion

[Sources: FMD MGT & NRC Tax Table RPT 1/99]

Chairman ARCHER. Thank you, Mr. Schambach.

Mr. Hall, if you'll identify yourself, you may proceed.

STATEMENT OF S.W. HALL, JR., ASSISTANT COMMISSIONER AND CHIEF INFORMATION OFFICER, U.S. CUSTOMS SERVICE

Mr. HALL. Mr. Chairman, my name is S.W. Hall, Jr. I currently serve as the Assistant Commissioner for Information and Technology, and Chief Information Officer at the U.S. Customs Service.

Mr. Chairman and members, I would like to thank you for the opportunity to report on the progress of the year 2000 program at U.S. Customs. I'd like to make some brief remarks and then submit my statement for the record.

Ensuring that the U.S. Customs automated systems are Y2K compliant is critical to the smooth flow of trade imports and exports, the movement of passengers in and out of the country, timely revenue collection, and effective enforcement of national laws.

My message today is that Customs is well on its way to ensuring that these vital systems are ready for the new millennium. At this point in time I am happy to report that we have reviewed 25 million lines of code in our mission-critical systems, and have returned those to production. We are in the midst of a major independent verification and validation effort, where we are using automated tools to rescreen that software to make sure that things have not been overlooked.

We are doing an independent functional review of our processes to make sure we had indeed followed our internal testing protocols. We are planning to put an emergency response center capability in place beginning this summer which will allow us to support our trade partners as well as any unforeseen national infrastructure issues that might arise affecting the operational viability of our systems.

We are in the process of completing the replacement or upgrading of approximately 20,000 personal computers nationwide to make sure that they are Y2K compliant. We are in the process of replacing and upgrading approximately 300 telephone systems and almost 200 voice mail systems to likewise ensure that they remain operationally viable. And, we are completing a comprehensive set of business continuity of operations plans that ensure that each major operating location has contingency procedures in place to deal with either local or national conditions that might arise.

We have had some independent review of our approach to the Y2K remediation effort. We've received a favorable audit from the General Accounting Office and the Treasury Department's Inspector General, which found that our management approach to this major challenge is disciplined and effective. We have had an independent review done by the Gartner Group, an independent consulting group that specializes in auditing and analyzing IT, information technology, issues. And they declared our program to be among the best in class.

We have also had the management of this effort recognized by government Executive magazine as one of the top 20 management success stories this past year in the Federal Government, and our

Y2K program manager was recognized by government Computer News as an example of a very successful government information technology manager.

With this in mind, I'd like to conclude by assuring you that we believe that the Customs Y2K program is on track and demonstrates when provided the necessary support and resources, that we can attack a large system challenge successfully and get done what needs to be done.

This concludes my remarks, and I'd be happy to answer any questions that you might have.

[The prepared statement follows:]

Statement of S.W. Hall, Jr., Assistant Commissioner and Chief Information Officer, U.S. Customs Service

THE YEAR 2000 PROGRAM AT CUSTOMS—"CURRENT STATUS AND REMAINING CHALLENGES"

On May 7, 1998, the Assistant Commissioner, Office of Finance and Chief Financial Officer for the U.S. Customs Service, testified before this Committee's Subcommittee on Oversight. During her testimony, she provided the Committee with an overview of the Customs Year 2000 Program and the status of the Program at that time. Today, I wish to provide the Committee with a brief update on the current status of the Year 2000 Program at Customs, a summary of the accomplishments which the Program has realized to-date, and a description of the ongoing tasks which the agency intends to complete prior to the advent of Fiscal Year 2000.

OVERVIEW

On a yearly basis, Customs mission critical computer systems process over $850 billion worth of imported merchandise and account for the collection of more than $21 billion in revenue. Annually, information concerning over 450 million people who enter the United States from foreign lands are processed by Customs law enforcement and targeting systems. Other systems process export information, provide administrative and payroll support to the Customs Service, and support trade, carrier and other commercial organizations.

Crucial to the fulfillment of the Customs Mission, Customs computer systems are also vital to the operational success of other federal government agencies with whom Customs shares electronic information: The U.S. Census Bureau, the U.S. Fish and Wildlife Service, the U.S. Food and Drug Administration, The U.S. Department of Justice, the U.S. Department of Agriculture, and Customs' sister bureaus within the Department of the Treasury are representative of the government agencies with whom Customs systems interface and share information.

Customs overarching objective in addressing the Year 2000 Problem was to ensure that its mainframe mission critical computer systems continue to deliver timely, reliable, and accurate information, without interruption, into the new millennium. To achieve this goal, the Customs Year 2000 Program reviewed approximately 25 million lines of computer code and successfully renovated, tested for Year 2000 compliance, and migrated into the Customs Production environment 100 % of its mainframe mission critical assets. This monumental feat was accomplished within budget, in accordance with General Accounting Office guidelines, and in advance of deadline dates imposed by the Department of the Treasury and the Office of Management and Budget.

With Customs mainframe mission critical systems Year 2000 compliant and fully functional, assuming the public data and telephone infrastructure is also Year 2000 compliant, Customs can continue to operate in an efficient , effective, and dependable manner. If these systems were not Year 2000 compliant however, the results to Customs operations would be devastating. Millions of passengers and billions of dollars worth of merchandise arriving into the U.S. would have to be processed manually, thus creating delays and contributing to a loss of revenue. The integrity of U.S. borders would be jeopardized, and efforts to apprehend criminals and interdict narcotics would be severely crippled.

YEAR 2000 PROGRAM ACCOMPLISHMENTS

Guided by the Year 2000 Executive Council and through the proper management, allocation, and mobilization of necessary resources, the award-winning Customs Year 2000 Program has successfully met the Year 2000 Program milestones established by GAO, OMB and Treasury. In fact, the combined audit team from GAO and the Inspector General's Office within Treasury found that "Customs Has Established Effective Year 2000 Program Controls." In addition to the timely renovation, validation, and implementation of Customs mission critical mainframe computer systems, Customs has also:

- Validated and tested its mainframe mission critical hardware, including network and communication interfacing equipment.
- Renovated, validated, and tested the computerized user developed programs which interface with Customs mainframe computer systems, tables and files.
- Validated and tested the computer software used in conjunction with its mainframe and personal computers. These software packages, including operating systems, capacity planning tools, security packages, word processors and spreadsheets, were tested in Customs own systems environment.
- Identified, tested, and evaluated over 5,000 non-information technology (non-IT) assets for Year 2000 compliance including facilities systems, portable radios, lab equipment, building security systems, and other such products having date-related functions. Sixty non-IT products assessed as non-compliant will be renovated or replaced prior to May 1999.
- Completed, and submitted to Treasury, business continuity of operations, technical compliance assurance and business quality assurance plans. These plans were developed as a contingency against potential Year 2000 induced failures. These plans have been used by Treasury as a model for use by its other bureaus. A simulated test of these procedures, at the Customs Port in Houston, Texas, was postponed due to local trade community opposition.
- Conducted awareness conferences throughout the country, addressing Year 2000 issues of concern to field level Custom offices.
- Completed the development of recommendations for a Year 2000 Emergency Response Center (ERC). The purpose of the ERC is to protect our private and public sector trading partners as well as our field support from Year 2000-induced IT failures. Although Customs is confident in the thoroughness and quality of its Year 2000 remediation process, there are external risks over which the agency has no control (e.g., non-compliant data exchanges from our trading partners, civil infrastructure failures). We are taking this proactive step to provide further assurance that service to the field offices and to our public is unaffected. Our objective is to have the ERC operational starting August 1, 1999.

REMAINING CHALLENGES

While the Customs Year 2000 Program is on-schedule and has continued to meet all prescribed deadline dates for completion of its many processes, there is still much work to be accomplished in the months ahead. Briefly, the Customs Year 2000 Program will be undertaking the following tasks:

- Though Customs mainframe mission critical systems have been successfully tested and are functioning properly, to further ensure the functionality of the systems, we are re-testing and will continue to re-test all systems via simulated post-2000 environments.
- Customs is continuing a series of tests with organizations with whom we interface. These external interface tests, which began in January 1998, will continue through June 1999. The tests will assist these interfacing organizations in ensuring that their systems will work with Customs into the Year 2000 and beyond.
- Customs is either checking, upgrading, or replacing nearly 19,000 personal computers to be Year 2000 compliant. This task is nearly 60% completed. It is anticipated that all systems, including their software, will either be replaced or upgraded by June 1999.
- Customs is currently replacing 300 telephone systems and 156 voice mail systems. Year 2000 related upgrades are being performed on 34 voice mail systems. It is anticipated that this task will be completed by June 1999.
- Customs recently completed Business Continuity Of Operation Plans and quality assurance plans for its major business processes. The Information Technology Continuity Of Operations Plans, in support of Customs business functions, are in process and will be completed by June 1999.
- Customs is conducting an Independent Verification and Validation (IV&V) Program. Upon the completion of the IV&V Program, Customs will have reasonable assurance that all of Customs systems are Year 2000 compliant and that the processes

used in the conduct of the Year 2000 Program followed appropriate GAO, OMB, and Treasury guidelines. The IV&V Program includes the use of an automated tool which double checks potential date problems which may have been overlooked in the original testing of renovated computer programs. The IV&V Program will continue through June 1999.

• Customs is in the process of developing formalized plans and an implementation schedule for the Year 2000 ERC. The plans are based on the recommendations developed in December 1998.

• Customs anticipates completion of the renovation, testing, and replacement of its non-compliant non-IT assets by May 1999.

• Through January 31, 1999, Customs expended approximately $85 million on the Year 2000 Program. We currently expect to complete all Year 2000 remediation efforts under the original project estimate of $120 million.

LONG-TERM BENEFITS OF THE YEAR 2000 PROJECT APPROACH

Customs implemented its Year 2000 Program with an eye to the future. The plans, processes, and procedures put into place to support the Year 2000 effort were developed so that Agency operations could continue to benefit from this value-added approach well after the year 2000 has passed. These long-term benefits, most of which are based on the agency's "lessons learned and best practices," include:

• The completion of a comprehensive inventory of applications and user procedures which cross-reference system files, tables, and systems users, both within and outside of Customs.

• The development of a coordinated approach, and repeatable processes, to project management and tracking, through a Project Program Office. The success of the Customs approach has been recognized with an award of excellence by Government Executive Magazine.

• The upgrade and standardization of various equipment and systems at both Headquarters offices and field locations. This approach will create a more cost-effective asset base and more consistent training methodologies, and will facilitate enhanced communications between organizational entities within the agency.

• The creation of a separate computer system testing environment which will be beneficial for other projects as they enter the acceptance testing phase of the systems development life cycle.

• The development of contingency strategies, plans, and procedures which will become a permanent part of Customs business process environment, and which will be invoked in the event of Year 2000 or other induced systems failures.

• The development of an awareness of the importance of Audit Trail Models and the maintenance of system "artifacts." Following their audit of the structure and processes of the Year 2000 Program, GAO and Treasury Inspector General informed Customs that: "Customs Has Established Effective Year 2000 Program Controls."

• The development of an Independent Verification and Validation (IV&V) Program. Through the Year 2000 Program, Customs developed an IV&V process. Customs will be continuing the IV&V Program as part of its ongoing quality assurance program which will be incorporated into all OIT projects.

This concludes my remarks before the Committee. We would now be pleased to entertain any questions you may have about our Year 2000 Program and our project approach.

Chairman ARCHER. Thank you, Mr. Hall.

Admiral Naccara, welcome. If you'll identify yourself, you may proceed.

STATEMENT OF REAR ADMIRAL GEORGE N. NACCARA, DIRECTOR, INFORMATION AND TECHNOLOGY, U.S. COAST GUARD

Admiral NACCARA. Thank you, sir. I'm George Naccara, the Coast Guard's Chief Information Officer. I have responsibility for the Coast Guard's Year 2000 project, and thank you very much, Mr. Chairman, for the opportunity to testify before you and your Committee today.

The Coast Guard is certainly aware of the potential for disruption posed by the so-called Millennium Bug both in Coast Guard readiness as well in cooperation with and in support of other agencies. We are working diligently to ensure that our own information technology systems are prepared for the millennium. Our motto is Semper Paratus, Always Ready, and therefore we must similarly ensure that our hardware with which we deliver our marine safety, environmental protection, search and rescue, and maritime law enforcement services to the public is also ready.

On that score, I am pleased to report that we are making excellent progress, and we expect our boats, ships, planes, and command and control systems will be ready and operating January 1, 2000, and the many other dates on which there may be Y2K events.

In addition, our managers and technical staffs are repairing the administrative and support systems that underpin our operations. And we expect them to be repaired and working when the new millennium dawns.

The Coast Guard will leave no stone unturned to prepare its technology for the millennium, but will also be ready to continue responding to the call even if a piece of technology lets us down.

We have directed our unit commanders and our Headquarters program managers to prepare contingency plans for all systems that are important to the functioning of their units, hence the term "mission-critical systems" for us. We recognize that even if all Coast Guard systems and equipment are prepared for the year 2000 rollover, there is a potential for failures across the country in public infrastructure, among our suppliers and business partners, and in the industry we regulate. To prepare properly for external disruptions that may impact the Coast Guard, we are evaluating the range of possible Y2K impacts upon the Coast Guard for all regions, and developing business continuity contingency plans to address all potential problems.

Now I want to address the Coast Guard's interface with and support of the Customs Service and the Bureau of Alcohol, Tobacco, and Firearms, and the impact of Y2K in maintaining those relationships.

The primary interaction between the Coast Guard and the Customs Service and Bureau of Alcohol, Tobacco, and Firearms is the sharing of law enforcement information. We have no direct data system contacts with either Customs or ATF. We are, however, users of the Treasury Enforcement Communications System. And any Y2K problem in that system would affect us. It is our understanding from Customs that it is Y2K compliant.

The Coast Guard, through its Law Enforcement Information System, provides information on vessel sightings and boardings to the Joint Maritime Information Element, JMIE, a classified multiagency database of maritime intelligence information from the Coast Guard, Navy, Customs Service, Drug Enforcement Administration, and FBI. The LEIS and JMIE databases reside at the Coast Guard Operations Systems Center in Martinsburg, West Virginia. They both have undergone Y2K testing and renovation, and will be compliant with the OMB-mandated schedule well before the year 2000.

Therefore, law enforcement agencies accessing this JMIE system will received the same information as before with no anticipated interruption in service.

Similarly, the Coast Guard has investigated to ensure it will be able to receive law enforcement information from other agencies. We have determined that the Coast Guard connection to the Anti-Drug Network will continue to function correctly. Also we receive information from the National Crime Information Center through LEIS. That connection has been tested by the Coast Guard and is also Y2K compliant.

The Coast Guard participates directly with the Customs Service primarily in counterdrug operations. This includes Coast Guard aviation, cutter, and boat support, as well as in conducting joint dockside boardings. The primary Y2K concern for these operations is in communication capability. The Coast Guard communicates with Customs via UHF and VHF radios. We have obtained manufacturer verification that most of our radios are Y2K compliant. Those that are not will be replaced well before January 1, 2000.

One special initiative between the Coast Guard and Customs, though still on a small scale, is still worthy of note. Based on a Memorandum of Understanding between our agencies, a small number of Coast Guard container inspectors in the port of Savannah began to access Customs. Automated Manifest System, tracking all incoming merchandise for tariff and legal reasons. Coast Guard access is for targeting of hazardous material containers for inspection. The arrangement has been very successful. And we plan to expand to four additional offices in the near future. The system is totally Y2K ready.

The Coast Guard has very limited and only sporadic direct working relationships with ATF. We have no data interfaces or any common computer systems or applications.

Thank you very much, Mr. Chairman.

[The prepared statement follows:]

Statement of Rear Admiral George N. Naccara, Director, Information and Technology

Good afternoon, Mr. Chairman and distinguished Members of the Committee. I am Rear Admiral George Naccara, the Coast Guard's Chief Information Officer. I have responsibility for the Coast Guard's Year 2000 (Y2K) project. I want to thank you for the opportunity to testify before you today.

The Coast Guard is certainly aware of the potential for disruption posed by the so-called millennium bug, both in Coast Guard readiness as well as in cooperation with, and support of, other agencies. We are working diligently to ensure our own information technology systems are prepared for the millennium. Our motto is "Semper Paratus"—Always Ready—and therefore, we must similarly ensure that our hardware with which we deliver our marine safety, environmental protection, search and rescue, and maritime law enforcement services to the public is also ready.

On that score I am pleased to report that we are making excellent progress, and we expect our boats, ships, planes, and command and control systems will be ready and operating on January 1, 2000, and the other dates on which there may be Y2K events. In addition, our managers and technical staffs are repairing the administrative and support systems that underpin our operations, and we expect them to be repaired and working when the new millennium dawns.

The Coast Guard will leave no stone unturned to prepare its technology for the millennium, but will also be ready to continue responding to the call even if a piece of technology lets us down. We have directed our unit commanders and headquarters program managers to prepare contingency plans for all systems that are important to the functioning of their units, hence the term "mission critical" system.

However, we recognize that even if Coast Guard systems and equipment are prepared for the year 2000 rollover, there is the potential for failures across the country, in public infrastructure, among our suppliers and business partners, and in the industry we regulate. To prepare properly for external disruptions that may impact the Coast Guard, we are evaluating the range of possible Y2K impacts upon the Coast Guard for all regions and developing Business Continuity Contingency Plans to address potential problems.

I want to address the Coast Guard's interface with, and support of, the Customs Service and the Bureau of Alcohol, Tobacco, and Firearms, and the impact of Y2K on maintaining those relationships.

The primary interaction between the Coast Guard and the Customs Service and Bureau of Alcohol, Tobacco, and Firearms (ATF) is in the sharing of law enforcement information. We have no direct data system contacts with either Customs or ATF. We are, however, users of the Treasury Enforcement Communications Systems (TECS) and any TECS Y2K problem would affect us. It is our understanding that TECS is Y2K compliant.

The Coast Guard, through its Law Enforcement Information System, version II (LEIS II), provides information on vessel sightings and boardings to the Joint Maritime Information Element (JMIE). JMIE is a classified multi-agency database of maritime intelligence information from the Coast Guard, Navy, Customs, Drug Enforcement Administration and Federal Bureau of Investigation. The LEIS II and JMIE databases reside at the Coast Guard Operations System Center in Martinsburg, WV. They both have undergone Y2K testing and renovation and will be Y2K compliant in accordance with the Office of Management and Budget-mandated schedule well before the year 2000. Therefore, law enforcement agencies accessing JMIE will receive the same information as before with no anticipated interruption in services.

Similarly, the Coast Guard has investigated to ensure it will be able to receive law enforcement information from other agencies. We have determined that the Coast Guard connection to the Anti-Drug Network (ADNET) will continue to function correctly. Also, we receive information from the National Crime Information Center (NCIC) through LEIS II. That connection has been tested by the Coast Guard and is Y2K compliant.

The Coast Guard participates directly with the Customs Service primarily in counterdrug operations. This includes Coast Guard aviation, cutter, and boat support, as well as in conducting joint dockside boardings. The primary Y2K concern for these operations is in communications capability. The Coast Guard communicates with Customs via UHF and VHF-FM radios. We have obtained manufacturer verification that most of our radios are already Y2K compliant. Those that are not compliant will be replaced by January 1, 2000. One special initiative between the Coast Guard and Customs, though still on a small scale, is also worthy of note. Based upon a Memorandum of Understanding between the Coast Guard and Customs, a small number of Coast Guard container inspectors at our Captain of the Port (COTP) office in Savannah began in 1992 to access Customs' Automated Manifest System (AMS), which tracks all incoming merchandise for tariff and legal reasons. Coast Guard access is for targeting of hazardous material containers for inspection. The arrangement has been very successful at the Savannah site, and a program to expand to four additional COTP offices has been funded and is now coming on-line. The system is Y2K ready. As a result, we do not anticipate any Y2K threat to Coast Guard and Customs joint operations.

The Coast Guard has very limited and only sporadic direct working relations with ATF. We have no data interfaces or any common computer systems or applications.

I will be happy to answer any questions you might have.

Chairman ARCHER. Thank you, Admiral.

Mr. Clawson, if you will identify yourself for the record, you may proceed.

STATEMENT OF JAMES B. CLAWSON, SECRETARIAT, JOINT INDUSTRY GROUP

Mr. CLAWSON. Thank you, Mr. Chairman, Members of the Committee. I am Jim Clawson, I'm chief executive officer of JBC Inter-

national and for purposes of this hearing, secretariat to the Joint Industry Group. The Joint Industry Group is a member-driven collection of over 140 companies and associations and firms representing about $350 billion in international trade. We concern ourselves with the Customs issues worldwide.

Our purpose in being here, and we appreciate this opportunity, is to talk about the Y2K compliance of the U.S. Customs Service. We've known about this programming glitch in the private sector with Customs for many years. In fact, in the late 1980's and early 1990's, our view was that how we were going to fix it was to pass the Customs Modernization Act, which provided for a totally new automated system that we thought would be in place by now. And it was our belief that all of those elements that we are looking at now with the Y2K would be taken care of.

Boy we sure missed that action and misjudged that because here we are in 1999 without a new system, but we are here to tell you that customs by diverting resources that it was going to use in developing the new system has been able to look at all of the data lines, and we're here to say to this Committee and we are very pleased that the Customs Service has done a good job under very difficult conditions in renovating its legacy systems and getting the Y2K compliance and renovation done.

My written testimony describes in more detail that renovation, but that's not all of the story. As we've heard here today a great deal of those systems are so interdependent with what the other folks are doing that there is still some concern with us. We are concerned about the private sector's compliance of their renovation of the Y2K programs as well as other agencies in the U.S. Government. The Customs Service performs multiple functions for many agencies as well as internationally.

You heard this morning about some other countries that may not be Y2K compliant. I don't say this lightly. In my capacity with JBC International, we have done a survey of 100 other countries and their Customs compliance with the Y2K issues. U.S. Customs is a world leader. Let me say that it doesn't look good in the rest of these other countries. There are some real concerns about the kind of information that might be coming internationally, and the kinds of disruptions that that might cause to the U.S. Customs, even though it can deal with it properly.

Also, we are concerned about the information with regard to transportation, telecommunications, the transportation companies, particularly in ocean freight. Many of them are foreign-owned, they are not operating under U.S. requirements—there are just a whole bunch of these outstanding issues that are out there that we don't have control over.

So that's of concern to the private sector in these mission-critical elements in the supply chain management and getting just-in-time inventories. And we have become so dependent today on that supply-chain for our economy to continue.

Now for those issues, what can we do? Some of the countries can still do manual clearance. You have heard IRS say today that it cannot go back to manual processing. Our belief is that the U.S. Customs Service is not able to go back to a manual system either. You may have seen some newspaper articles about Customs trying

to do some tests in one of the ports in case of any kind of contingency planning to go back to manual systems. The private sector was very unhappy about that. It didn't want to do it. It's a real problem for us in terms of what happens if a system fails. On this point, it isn't the Y2K that is a real problem for us, it is the antiquated legacy system that we have been trying to replace with ACE.

What we are facing is that there has not been sufficient funding. This Committee was kind enough to authorize another $50 million in legislation that just passed, but we've got to get some money appropriated for them to do the work on getting this system upgraded and in place to perform the services that the private sector is paying for. In fact, there is a merchandise processing fee the private sector—this is not like taxpayers money—pays that raises almost $1 billion a year. This, for the privilege of having their goods cleared. We think that those moneys are there to keep these systems up to date. What we're looking for is the ability to, as payers of this user fee, is the ability to have the services provided and benefit from those services.

We're comfortable that some of the work that is being done on Y2K is going to take place, but we're very uncomfortable about the fact that the system itself may collapse. And it may not even be in place by the end of the year to see if Y2K works.

And with that, I would like to encourage this Committee in its other capacities to look at that part of the issue. We are happy to work with you in any way we can.

I'm here to answer any questions you may have.

[The prepared statement follows:]

Statement of James B. Clawson, Secretariat, Joint Industry Group

INTRODUCTION

My name is James B. Clawson and among many other responsibilities I serve as the Secretariat to the Joint Industry Group (JIG). JIG is a member-driven coalition of over one hundred-forty Fortune 500 companies, brokers, importers, exporters, trade associations, and law firms actively involved in international trade. We both examine and reflect the concerns of the business community relative to current and proposed international trade-related policies, actions, legislation, and regulations and undertake to improve them through dialogue with the Executive Branch and Congress. JIG membership represents more than $350 billion in trade.

The Year 2000 problem goes back to the early days of computer programming, when memory capacity was nowhere near what it is today. In an effort to efficiently use a limited amount of memory, programmers used two-digits to represent years instead of four-digits. As a result, computers using software so programmed cannot distinguish between the year 1900 and 2000.

YEAR 2000 BACKGROUND

Although some economists and analysts are attempting to assess the possible impact of the Y2K problem as it is called, no one really knows how extensive the effects will be. Obviously, all computer hardware and software will have to be checked and re-programmed to deal with the Y2K problem. Compounding the problem, however, is the amount of non-Y2K compliant hardware and software embedded in anything from consumer electronics to medical devices.

The U.S. is currently one of very few countries worldwide that is monitoring the progress of government agencies on a regular basis. We commend Congress, the Administration, and government agencies for taking this problem seriously.

CUSTOMS YEAR 2000 PROGRESS

JIG has enjoyed a cooperative relationship with the U.S. Customs Service for several years. Our coalition has closely followed their progress in achieving Y2K compliance for all of its mission critical systems. We appreciate the enormous effort and resources that the Customs Service has allocated to renovating all of its computer systems; particularly those involved in the processing of trade transactions. The trade community is dependent on the functionality of Customs automated systems and must be assured that the interaction will continue as normal at the dawning of the new millennium.

Customs has performed several internal tests of their computer systems, including tests with other government agencies, software providers, and one financial institution. On January 22, 1999, the Customs Service opened testing to the private sector so that the interface between the trade community and Customs can be evaluated for compliance. Customs supplies test data, while industry participants are responsible for advancing their system clocks to test compliance.

Although industry appreciated Customs' invitation, the private sector is hesitant to allocate the time and equipment to conduct the test because Customs is offering no incentive to participate. One way to induce industry participation is for Customs to provide a Year 2000 statement of compliance to software providers that sell products that directly interface with Customs. Once the software provider has been tested and evaluated as compliant with Customs systems, Customs can permit the company to use the compliance statement on marketing documents and company websites. Such a statement will provide assurances to those companies using the software that its systems, working with the Customs' system, will experience no glitches because of Year 2000 problems. Similar to the statement of compliance, Customs could offer the use of a mark or similar certification after software providers or other companies have successfully completed the testing.

Because Customs has not provided a mechanism for guaranteeing that after the testing is complete that the participant's systems will continue to effectively interface with Customs in the Year 2000, companies are not willing to allocate the time or resources. An incentive program would not only benefit export-import software providers, but also their customers and companies using proprietary internal software to interface with Customs.

After meeting with several Customs officials to discuss their progress, we are satisfied that the Customs Service has prepared its computer systems to continue operations uninterrupted after January 1, 2000. We question, though, the preparedness of the users of Customs automated systems—companies, brokers, and other government agencies. Shutdowns caused by non-Y2K compliant systems will affect the entire import processing system and will lead to timely and costly delays in the clearance of goods at our nation's ports and border crossings.

Clearance of imports by other government agencies through the U.S. Customs system is critical. Up to 40 percent of entries can require approval from the Food and Drug Administration. The Department of Agriculture inspection agencies work closely with U.S. Customs in the ports. The Bureau of Alcohol, Tobacco and Firearms, the Department of Transportation and many more must be consulted to approve imports and exports. From a review of these agencies' progress in becoming Y2K compliant, the fact that U.S. Customs has completed and tested its systems may be irrelevant to the private sector if these other agencies cannot clear the goods.

We strongly urge the government to keep the pressure on all departments and agencies to complete renovation and test their mission critical systems. We also request that the government find ways to encourage the private sector to jointly conduct tests with the respective government agencies to ensure that their computer systems can handle the rollover to the year 2000.

CUSTOMS AUTOMATED SYSTEMS

Our perception of the government's Y2K readiness, particularly the Customs Service, may be irrelevant. Customs Assistant Commissioner for Information Technology, Woody Hall, stated it best in a February 18, 1999, Wall Street Journal article when he said, "The joke around here is that a lot of good it's going to do you to be Y2K-compliant if the system crashes around you." The current system, the Automated Commercial System (ACS), is nearly 15 years old and is showing its age. After several brownouts in the past year, Customs is more determined than ever that a new system must be created. Although the new system, the Automated Commercial Environment (ACE) is already in development stages, ACS must be kept operational as new ACE applications are brought online. With only $8 million available in FY 1999, keeping ACS functional is an enormous obstacle for Customs. The

effects of patchwork repairs on ACS that Customs has resorted to because of lack of funding are spilling over to industry as brownouts, slow-downs, and other reductions in "user service." These problems will inevitably slow or even halt trade if ACS and its replacements are not properly funded.

Failure to replace the aging components of ACS with comparable elements from ACE prior to ACS's eventual collapse will shut down the import process and thereby harm all U.S. importers and manufacturers, particularly those who rely on just-in-time delivery systems. Importers will be forced, if it is even available, to file import entry information through a time consuming paper process rather than through quick and efficient electronic means. The loss of revenue to the government will be staggering and the costs that consumers will eventually pay will rise.

Customs has made significant efforts to develop a comprehensive ACE Business Plan, which has been revised as industry and government needs have changed. The system is intended to be modular, in that components of ACE can be adapted as new technology or new needs arise. Customs has stated that they intend to work with outside contractors to build the system because the private sector has the most innovative technologies and systems development expertise. Customs has made valiant efforts to include the trade community in ACE design through the Trade Support Network (TSN) conferences. Customs is sensitive to its customer requirements but more needs to be done by both the private sector and Customs to ensure the new systems will be open, interoperable, and capable of meeting the challenges of the new millenium.

Unfortunately, ACE planning and implementation is stalled. The White House has shown absolutely no support for Customs automation. Industry is insulted by the Administration's proposal for a new "user fee" that importers will pay for the "privilege" of using Customs automated processing systems. Of the monies proposed to be collected, the Administration has set aside only $163 million and $150 million of that cannot be spent on automation until 2001.

This approach is unacceptable. First, the trade community is already paying for Customs automation through taxes, duties, and the merchandise-processing "user" fee imposed a number of years ago to pay for the commercial clearance of goods (which at the time was 90 percent automated). Since 1994, the merchandise-processing user fee accounts for an average of $800 million annually. This fee should have been used to keep the automated system updated and current for its users.

Secondly, at the proposed spending rate for the proposed new fee of $150 million per year, ACE (at a total cost of about $1.2 billion) will take approximately 8 years to develop. An 8-year development cycle for any automated system is unheard of. By the time ACE is fully implemented, the technology will be obsolete. So, under this proposal the private sector traders who represent the bulk of this nation's economy will be paying over $1 billion in new "user fees" for something it has already paid for and that may be outdated when it arrives. We deserve better than this from our government.

In addition to the lack of support from the Administration, the General Accounting Office (GAO) has consistently criticized Customs efforts. GAO disdainfully points out that Customs has not completed a sufficient ACE design plan from start to finish. Although many points in the most recent GAO reports are legitimate concerns shared by the private sector, some GAO comments do not consider the technology or development process involved in these unique Customs automated systems. We know of no other system in government where the private sector and government exchange millions of electronic communications 24 hours a day filing multiple tax returns resulting in more than $23 billion in revenue to the U.S. Government.

Realizing that it is impossible to anticipate advances in technology, Customs has developed a framework for the functionality that the system should perform. The technical aspects of the initial releases of ACE should be fairly well documented, but it is shortsighted to plan for the technical design of future modules now. It is also essential that GAO acknowledge that Customs personnel will not be "building" ACE. Customs' responsibilities are to work with the private sector to define the requirements and specifications for the system, leaving the technical design to outside contractors.

Industry applauds Customs for developing a plan that includes a detailed description of the ACS to ACE migration strategy. The plan explains that portions of ACS must remain operational during ACE development. As components of ACS are redesigned into ACE modules, only those portions of ACS will be turned off. This method of implementation seeks to ensure minimal disruptions in trade during development and implementation. In order for the conversion to be successful, Customs must have the money to keep ACS operational during ACE development.

Although the Year 2000 problem does not directly affect the International Trade Data System (ITDS) proposed by the Treasury Department, JIG would like to ex-

press our continued support of the overall concept. ITDS is a project that has demonstrated that hundreds of government agencies can coordinate their automation policies and systems to create a "front-end" interface that the government will use to distribute international trade data collected from industry. JIG is concerned, though, that too much emphasis is focused on ITDS development at the expense of ACE. As the "functional" part of the government's automated processing system, it is more important to develop ACE now rather than designing a data interface system. If no "functional" module operates, the development of the "front-end" interface is irrelevant.

CONCLUSION

JIG requests the Ways and Means Committee to authorize the estimated $1.2 billion to Customs for ACE and ITDS development. This will keep the Customs' Y2K renovation elements operational. A 4-year ACE and ITDS development cycle is essential. During these times when we are discussing budget surpluses, we do not understand the reasoning that money is not available and a new tax is needed. Automation is an essential function of the Customs Service mission for processing trade-related documentation. The existing budget should reflect this responsibility by making automation funding part of the $800 million user fee revenue amount a baseline component for the Customs Service.

While the Year 2000 is a critical issue, the JIG believes that Customs' progress in this area is insignificant if the automated systems that they have renovated are not operational. Without sufficient monetary resources, Customs and industry will be lucky if ACS is still functioning by January 1, 2000.

On behalf of the JIG, I thank you for this opportunity to provide our comments.

Chairman ARCHER. Thank you, Mr. Clawson.

Mr. Schindel, if you will identify yourself you may proceed.

STATEMENT OF DENNIS S. SCHINDEL, ASSISTANT INSPECTOR GENERAL FOR AUDIT, OFFICE OF INSPECTOR GENERAL, U.S. DEPARTMENT OF TREASURY

Mr. SCHINDEL. Mr. Chairman, Members of the Committee, my name is Dennis Schindel, I'm the Assistant Inspector General for Audit for the Treasury Inspector General.

This morning I testified on the results of our oversight of the Department of Treasury's Y2K efforts, and more specifically, FMS. I would now like to briefly summarize the results of our work at ATF.

I want to start off by mentioning that ATF was a bureau that we chose to pilot-test our Y2K audit approach. Not only was ATF very responsive to our findings and recommendations, but they were extremely open and cooperative with us from the very beginning of our audit work. This helped our learning process and enabled us to share what we learned from ATF with other bureaus.

I also want to point out, that at the time we performed our work, ATF too was still learning and adjusting their approaches to the best way to manage the Y2K conversion effort.

It's been 4 months since we issued our draft report to ATF, and even longer since we first brought our findings to their attention. ATF has taken corrective action on the issues we identified during our audit, and their management of the process and their progress is greatly improved.

In our audit, we evaluated ATF's Y2K conversion effort in the areas of project management, system conversion and certification, and contingency plans for business continuity. As with FMS, our

focus was on the broader issue of how well ATF was managing and controlling their Y2K conversion effort. We found that ATF had top management commitment, a good infrastructure, skilled resources, and reasonable guidance in place to address its Y2K conversion task.

However, some aspects of managing the effort and coordinating among the various components within ATF needed to be strengthened. Also, while ATF was generally following GAO's Y2K guidance, improvements were needed in some key parts of the Y2K conversion process.

For example, we identified the need for better coordination and communication between the Y2K project office and the software development staff to accommodate the respective needs of all the affected groups within ATF. Originally, we found that while the two groups were dependent on each other for Y2K certification, they had not coordinated testing, migration and certification dates with each other.

As a result, the Y2K project office was unable to identify systems that were ready for certification since the two schedules had differences in key system dates. After we discussed this issue with ATF, they expedited the reconciliation of their testing schedules from these cross-functional areas with Y2K responsibility.

We also found that while ATF had identified its data exchange partners, they had not developed plans to coordinate the testing of their interfaces with these data exchange partners.

ATF's Y2K project management office has now been assigned responsibility to ensure data exchange testing procedures are incorporated into the compliance testing process.

In our report to ATF, we included nine specific recommendations designed to help ATF strengthen their Y2K conversion effort. We recently met with ATF to determine what progress they have made since our field work. Although they have made significant progress in all areas and have implemented most of our recommendations, ATF still has a good deal of work ahead of them. They have three mission-critical systems that are not expected to be implemented until May, July and August of this year. Testing still needs to be performed with critical data exchange partners, and business continuity plans must be prepared and tested for each core business function. ATF is aware of the tight timeframe for the remaining tasks, and they have a good infrastructure in place that should enable them to effectively address this increased risk.

As I mentioned earlier in my testimony this morning, we plan to do additional work at ATF. We will first focus on the results of independent verification and validation, and then contingency planning. With three mission-critical systems that will not be implemented until after March 1999, it will be imperative that ATF have comprehensive contingency plans in place that subsequent testing in late 1999 identifies any serious Y2K non-compliance.

This concludes my remarks, and I would be happy to answer any questions.

Chairman ARCHER. Thank you, Mr. Schindel. Mr. Hite, if you will identify yourself for the record, you may proceed.

STATEMENT OF RANDOLPH C. HITE, ASSOCIATE DIRECTOR, GOVERNMENTWIDE AND DEFENSE INFORMATION SYSTEMS, ACCOUNTING AND INFORMATION MANAGEMENT DIVISION, U.S. GENERAL ACCOUNTING OFFICE

Mr. HITE. Thank you, Mr. Chairman. My name is Randy Hite, I'm an Associate Director in GAO's Accounting and Information Management Division. My statement today is based on our ongoing review of Customs' Y2k program management. That review is being done at the request of this Committee's Subcommittee on oversight and Subcommittee on trade. Very shortly we will issue our report on our review, detailing our findings. Today, I can sum those up in two simple words, cautious optimism.

I'm optimistic because of the good progress that Customs has made to date. Mr. Hall described the status of the Y2K efforts. I won't repeat that. He did a fair job of describing that in an accurate manner. I'm also optimistic because Customs has implemented effective controls for managing its program. As you know, GAO issued a series of three documents describing a set of effective management controls for managing a Y2K program. We compared Customs' structures and processes against these guides and found that they were fully implementing all of the tenets that were specified in those guides. So for these reasons, Mr. Chairman, I'm optimistic.

My optimism is somewhat tempered because Customs' work on Y2K is not yet done. And challenging work remains. Hence the reason for cautious in my two-word summary. For example, important steps remain to be completed, such as end-to-end testing, and finalizing testing of continuity of operations contingency plans.

Now, given that Customs must interact with thousands of business partners, and in implementing its mission, it relies on a decentralized organization involving over 300 ports of entry, this is no trivial task. Also, to perform its missions, Customs depends on many external systems that are out of its control, such as public infrastructure systems, transportation, telecommunication, and power. Customs also depends on systems owned and operated by its business partners and other government agencies.

For these collective reasons, I am cautiously optimistic.

Before concluding my statement, I would also like to comment briefly on how Y2K is both an IT management problem and an IT management opportunity, and to acknowledge Customs' stated intention to learn from its Y2K experience and to apply these lessons learned to its management of IT in general. Over the last 5 years we have reported on a number of agencies in terms of IT management weaknesses, particularly those agencies that have very large modernization programs.

We've made a series of recommendations for correcting these weaknesses, and I might add that Customs is one of the agencies where this has been the case. However, for its Y2K program, Customs chose to break from existing IT management practices, and instead, institute structured and disciplined processes for managing IT, modeled after GAO's year 2000 guides. The result is a program that's on target.

In Y2K, Customs' leadership has stated its intention to implement the same kind of management rigor and discipline to all of its IT efforts. But I realize an intention to implement is a long way

from having actually implemented. It's a positive first step. And I would submit that other Federal agencies would be well-served by following Customs lead and also taking this first step.

Mr. Chairman, this concludes my statement. I'll be happy to answer any questions you may have.

[The prepared statement follows:]

Statement of Randolph C. Hite, Associate Director, Governmentwide and Defense Information Systems, Accounting and Information Management Division, U.S. General Accounting Office

Mr. Chairman and Members of the Committee: Thank you for inviting me to participate in today's hearing on the challenges faced by the Customs Service in responding to the century date problem. If this problem is not addressed in time, key automated systems affecting trillions of dollars in trade between the United States and other countries could malfunction, resulting in delayed trade processing, lost trade revenue, and increased illegal activities, such as narcotics smuggling, money laundering, and commercial fraud. Fortunately, Customs has made good progress to date addressing its Year 2000 problem, thanks in large part to the effective Year 2000 program management structures and processes that it has in place for doing so. Nevertheless, Customs faces certain Year 2000 challenges, such as completing end-to-end testing, before it will be ready to cross into the new millenium. My testimony today will address these three areas—progress to date, program management effectiveness, and future challenges. Additionally, I will comment on how Customs can benefit from its Year 2000 experience in strengthening its management of information technology.

This testimony is based on our ongoing review of the effectiveness of Customs' Year 2000 management and reporting controls. We are performing this review at the request of this Committee's Oversight Subcommittee and its Trade Subcommittee. In short, we have reviewed Customs' Year 2000 management and reporting structures and processes, including those relating to testing, contingency planning, risk management, and quality assurance, and we have compared these to GAO's Year 2000 Guidance [1] to determine whether key internal controls are in place and functioning as intended. We have also traced the reported status of selected system components back to supporting systems documentation to verify the reported information's accuracy. We conducted our work in collaboration with the Treasury Inspector General and in accordance with generally accepted government auditing standards between July 1998 and January 1999.

CUSTOMS' RELIES EXTENSIVELY ON AUTOMATED SYSTEMS

Addressing the Year 2000 problem in time is critical for the Customs Service because it relies extensively on information technology to help enforce trade laws and collect and account for duties, taxes, and fees on imports.[2] As the following illustrates, Customs has five mission-critical systems that run over 20 million lines of application code and are used by thousands of users within Customs, other government agencies, and the trade community.

- The Automated Commercial System (ACS) tracks, controls, and processes all commercial goods imported into the United States. Over 97 percent of the data filed for imported cargo entries are sent through ACS and more than 15,000 trade and other government agency users have access to this system.
- Customs' Treasury Enforcement Communications System (TECS) interfaces with the FBI's National Crime Information Center and a number of other law enforcement systems and is the major automation component of the Interagency Border Inspection System, which serves as a clearinghouse for law enforcement data. Some 27,000 users, including Customs; Immigration and Naturalization Service; Internal Revenue Service; Bureau of Alcohol, Tobacco, and Firearms; and the State Department rely on TECS.
- The Seized Asset and Case Tracking System (SEACATS) processes and tracks activity associated with seizures for the initial law enforcement interest in the property to its final disposition. This system is used by more than 16,000 Customs em-

---

[1] *Year 2000 Computing Crisis: An Assessment Guide* (GAO/AIMD–10.1.14, issued as an exposure draft in February 1997, issued final in September 1997); *Year 2000 Computing Crisis: Business Continuity and Contingency Planning* (GAO/AIMD–10.1.19, issued as an exposure draft in March 1998, issued final in August 1998); and *Year 2000 Computing Crisis: A Testing Guide* (GAO/AIMD–10.1.21, issued as an exposure draft in June 1998, issued final in November 1998).

[2] During 1997, Customs collected $22.1 billion in revenue at more that 300 ports of entry.

ployees, and it interfaces with the Justice Department and Internal Revenue Service systems.

• Customs' Automated Export System (AES) collects export-related data from exporters and carriers and is used to help target export violators. More than 28,000 users nationwide rely on this system.

• ADMIN is Customs' primary administrative system supporting financial and human resource functions. It is comprised of 40 separate systems that interface with each other and with ACS, AES, and TECS.

In addition to fixing and testing its systems, Customs must assess and remediate a wide range of telecommunications equipment and non-information technology (non-IT) assets installed in over 900 facilities. This non-IT equipment includes check-writers; scanners; optical readers; security systems such as badge readers, x-ray systems, cameras, secured doors and safes; fire alarms; heating and air conditioning systems; planes; and automobiles.

CUSTOMS IS MAKING GOOD PROGRESS IN ADDRESSING ITS YEAR 2000 PROBLEM

As of January 1999, Customs reported that it had met milestones recommended by the Office of Management and Budget (OMB) for renovating and validating most of its mission-critical systems.[3] Specifically, it reported that it had completed renovation, validation and systems acceptance testing[4] of all five of its mission-critical systems. Moreover, it plans to complete end-to-end testing[5] for these systems and associated telecommunications systems by March 1999.

Customs has also renovated most of its telecommunications equipment. Specifically, as of January 1999, Customs reported that it had assessed all of its national data center-related telecommunications systems and renovated, validated, and implemented 92 percent of the inventory requiring Year 2000 work. It had also assessed telecommunications equipment in its field offices and completed 68 percent of needed renovations. Additionally, Customs had completed about half of the work needed on headquarters and field office voice communications equipment, including telephone and voice mail systems.

Customs reported that it has assessed about 82 percent of its mission-critical non-information technology products. It reported that 95 percent of the products assessed is compliant, 4 percent requires renovation or replacement and one percent is to be retired. It expects to complete this work by May 1999.

To help ensure that the information it reports on Year 2000 progress is reliable, Customs has implemented reporting controls. For example, quality review teams review the information reported for (1) consistency (by comparing it to previously reported information), (2) completeness (by comparing it to reporting standards), and (3) accuracy (by validating it through observation, inquiry, or review of supporting documentation). Our review of quality review team results, as well as our independent review of the reliability of the information reported in selected system components, disclosed no discrepancies between what was being reported and what supporting system documentation showed actual progress to be.

EFFECTIVE MANAGEMENT STRUCTURE AND PROCESSES ARE KEY TO CUSTOMS' SUCCESS

GAO's Year 2000 Guides provide a framework for effective Year 2000 program management. Collectively, they define a comprehensive set of program management controls for planning, directing, monitoring, and reporting on Year 2000 efforts.

Customs' program management structures and processes are entirely consistent with GAO guidance, and Customs' good progress to date is largely attributable to this program management capability. Along these lines, Customs has done the following.

• Established a Year 2000 Program Office and designated a Year 2000 Program Manager in May 1997 and charged the office with authority over and responsibility for agencywide Year 2000 efforts, including such functional areas as Year 2000 con-

---

[3] OMB requires that agencies complete renovation of their mission-critical systems by September 1998, validation by January 1999, and implementation by March 1999.

[4] The purpose of system acceptance testing is to verify that the complete system (i.e., the full complement of application software running on the target hardware and systems software infrastructure) satisfies specified requirements (functional, performance, and security) and is acceptable to end users.

[5] 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, interoperate as intended in an operational environment, either actual or simulated.

tracting, budgeting and planning, technical support to project teams, quality assurance, auditing and reporting.

• Engaged its senior executives in the Year 2000 effort by charging the agency's Executive Council[6] with approving and overseeing the implementation of the Year 2000 strategy and resolving such issues as institutional Year 2000 priorities.

• Developed a Year 2000 Strategic Plan and Year 2000 Operational Program Management Plan in June 1998, which (1) identified organizational roles and responsibilities, (2) established schedules for completing each program phase and described the tasks to be completed under each phase, (3) established reporting requirements to track progress in the various phases, (4) defined performance measures, and (5) estimated and allocated resources for the tasks and system activities within these phases.

• Issued policies, guidelines, and procedures for managing and implementing the Year 2000 program, including guidance on quality assurance, configuration management, and testing, as well as business continuity and contingency planning.

To ensure that the plans, policies, and guidelines are being implemented, the Year 2000 program manager is (1) holding weekly status meetings with the Year 2000 Program Office staff and the project teams, (2) tracking, prioritizing, and managing the risks associated with the IT and non-IT system conversion efforts, (3) overseeing and managing budget-related issues, and (4) conducting internal audit reviews to monitor and assess the implementation of established Year 2000 procedures. The Program Office is also tracking progress against plans and identifying issues that may impact its strategy using a central database it developed.

Structured and disciplined processes have also been implemented for the testing phase of Customs' Year 2000 effort. This is important since Customs' key mission-critical systems run hundreds of interdependent applications, and must interface with thousands of external systems. In particular, Customs designated a Year 2000 test manager for mission-critical IT systems and assigned this manager authority and responsibility for key testing activities, such as defining exit criteria, designing and planning the tests, and executing the tests. It also established in its Year 2000 Application Testing Strategy and Plan an agencywide definition of Year 2000 compliance; engaged an independent verification and validation (IV&V) agent to ensure that process standards have been followed and that software products perform as intended; provided for ensuring that vendor-supported IT and non-IT products have been tested and that they are Year 2000 compliant; and established a Year 2000 test environment. These controls and processes have enabled Customs to meet milestones recommended by OMB for renovating and validating mission-critical systems and to allow time to conduct end-to-end tests.

Finally, Customs has implemented sound management processes for developing business continuity and contingency plans that help Customs to mitigate the risks associated with unexpected internal and uncontrollable external failures. Specifically, Customs established a business continuity work group; developed a high-level business continuity planning strategy; developed a master schedule and milestones; implemented a risk management process and established a reporting system; and implemented quality assurance reviews. It then performed a business impact analysis to determine the effect that failures of mission-critical information systems have on the viability and effectiveness of agency core business processes. By defining disruption scenarios and assessing business, legal, and regulatory risks for major business processes, this analysis provided Customs the information needed to develop contingency plans for continuity of operations. Customs is now in the processes of testing its contingency plans and it plans to complete contingency plan testing, including plans for non-IT systems, by June 1999.

IMPORTANT CHALLENGES STILL FACE CUSTOMS IN MONTHS TO COME

Notwithstanding either Customs' good progress to date or the effectiveness of its program management controls, Customs still has very important and challenging tasks to complete to effectively reduce its chances of serious business disruptions. In particular, Customs still needs to conduct end-to-end testing of the systems that support important trade missions. These tests will be particularly challenging since Customs has hundreds of business partners and their respective systems. Additionally, Customs still needs to complete its contingency plans for ensuring continuity of its core business areas in the event of Year 2000-induced system failures. For Customs, this is especially challenging because it involves 42 distinct lines of business that cut across Customs' organization units, and it involves over 300 organiza-

[6]The Council is co-chaired by the Chief Information Officer and the Chief Financial Officer and includes the Year 2000 project managers as members.

tional units that are located throughout the United States, each with its own unique and localized Year 2000 readiness issues.

Moreover, Customs, like most organizations, faces serious risks outside of its control. For example, Customs' depends on public infrastructure systems, such as those that provide power, water, transportation, and voice and data telecommunications. Given the number of Customs ports of entry throughout the United States, even localized disruptions in infrastructure-related services could seriously impact Customs business operations. As Customs works to develop, test and complete its contingency plans, it must ensure that these localized event scenarios are adequately addressed.

CUSTOMS RECOGNIZES THAT MANAGEMENT IMPROVEMENTS MADE TO ADDRESS THE YEAR 2000 PROBLEM CAN PROVIDE FUTURE BENEFITS

For federal agencies, the lessons to be learned from the Year 2000 problem are significant. Longstanding organizational weaknesses in managing information technology contributed to both the size of the federal government's Year 2000 problem, and agencies' ensuing difficulties in addressing it. That is, agencies' unsuccessful attempts to modernize their information systems over the last 5 years have forced them to continue to maintain and rely on antiquated, poorly documented, non-compliant systems. The result was large inventories of non-compliant systems that the agencies had to quickly repair, replace, or retire in order to be century date ready. The Internal Revenue Service, with its well-chronicled history of modernization difficulties and its mammoth Year 2000 problem, vividly illustrates this point.

Additionally, to address the Year 2000 problem, agencies chose to employ the same weak information technology management structures and processes that have contributed to their system modernization problems. Our reports and testimonies over the last 5 years have highlighted these weaknesses in major modernization programs.[7] These weaknesses include the lack of CIO authority over agencies' IT resources, the absence of complete and enforced systems architectures, the lack of mature software development and acquisition processes, and the failure to make informed IT investment decisions. Because of these weaknesses, we have designated certain modernization efforts, such as the Federal Aviation Administration's air traffic control modernization and the Internal Revenue Service's tax systems modernization, as high-risk federal programs.[8]

Customs did not adopt a "business-as-usual" approach to solving the Year 2000 problem. Using GAO's Year 2000 guidance, Customs defined and implemented effective management structures and processes, as this testimony has described. The result is a Year 2000 program that is on schedule and has plans and management controls in place for completing remaining tasks. As important, Customs' Commissioner has also committed to leveraging the agency's Year 2000 experience by extending the level of project management discipline and rigor being employed on Year 2000 to other information technology programs and projects. By doing so, Customs could greatly strengthen its information technology management capabilities.

In conclusion Mr. Chairman, we are cautiously optimistic about Customs' Year 2000 program. We are optimistic because of Customs' progress to date and its effective program management controls. We are cautious because important tasks remain, and because Customs, like all organizations, depends on others in order to fulfill its mission responsibilities.

This concludes my statement. I would be glad to respond to any questions that you or other Members of the Committee may have at this time.

Chairman ARCHER. Thank you, Mr. Hite.

---

[7] *Tax System Modernization: Management and Technical Weaknesses Must Be Corrected If Modernization Is to Succeed* (GAO/AIMD–95–156, July 26, 1995); *Tax Systems Modernization: Actions Underway but IRS Has Not Yet Corrected Management and Technical Weaknesses* (GAO/AIMD–96–106, June 7, 1996); and *Tax Systems Modernization: Blueprint Is a Good Start but Not Yet Sufficiently Complete to Build or Acquire Systems* (GAO/AIMD/GGD–98–54, February 24, 1998); *Air Traffic Control: Immature Software Acquisition Processes Increase FAA System Acquisition Risks* (GAO/AIMD–97–47, March 21, 1997); *Air Traffic Control: Complete and Enforced Architecture Needed for FAA Systems Modernization* (GAO/AIMD–97–30, February 3, 1997); and *Air Traffic Control: Improved Cost Information Needed to Make Billion Dollar Modernization Investment Decisions* (GAO/AIMD–97–20, January 22, 1997).

[8] *High-Risk Series: An Update* (GAO/HR–99–1, January 1999); *High-Risk Series: Information Management and Technology* (GAO/HR–97–9, February 1997); and *High-Risk Series: An Overview* (GAO/HR–95–1, February 1995).

Are there any questions for this panel? If not. Mr. Foley?

Mr. FOLEY. Just a second, if I could, Mr. Chairman, thanks very much. Relative to Customs then, the question Mr. Clawson raised, I believe, is Customs reached out to the trade industry to make certain that its data to trading partners will be able to transact business through their related systems in the year 2000?

Mr. HALL. Yes, sir. We began testing last spring, when we made ourselves available to trading partners. We did some limited testing during the spring and summer. We just announced a 5-month window, beginning this month, where we will make time available to anyone who is ready and prepared to come test, end-to-end, their systems with ours. That testing has begun. At this point, while it's a relatively small number of organizations, something on the order of 25 or so, they represent the folks who provide software to about half of our trading partners.

We will continue to do this testing through the spring and, of course, we will make ourselves available. Actually we are planning to support testing past the change of the millennium. We think this is a very helpful way to ensure that the many types of organizations that use our systems and provide information to it, have an opportunity to make sure that their applications work as well as ours.

Mr. FOLEY. What have you done specifically to ensure the safety, if you will, of the information you currently have regarding drug interdiction, drug traffickers, others in the system that you have been monitoring? To protect that information in the event there's a computer problem.

Mr. HALL. We have emergency backup facilities at the Newington Data Center itself in terms of generators and battery banks so that we could withstand a temporary loss of power. We do traditional tape backups of data so that we can rebuild databases if we were to have hardware failures. Does that get to the point?

Mr. FOLEY. Just making certain we have something to go back to, if the computer resets itself and eliminates data. Just making certain that somewhere there's an ability to recapture that important information that you may have in process.

Mr. HALL. Yes, sir. Those are the two major strategies. One is to make sure we can maintain power if there is an infrastructure failure, and the other is to back up the data bases.

Mr. FOLEY. Thank you, Mr. Chairman.

Chairman ARCHER. Before excusing you, the Chair has just two quick questions that apply to every one of you except Mr. Clawson, I believe. Is each of you confident that the entity that you represent will be able to perform its essential functions and services on January 1st of next year?

I assume by a silence that each of you is saying yes, we are confident. And let the record show that.

The second short question is, are there any additional resources that the Congress need to give you to complete your remediation problem? I don't mean now, updating the entire Customs situation Mr. Clawson talked about. [Laughter.]

I'm talking about the Y2K problem. OK?

Admiral Naccara.

Admiral NACCARA. Thank you. I think it would be beneficial if there were continuing opportunities for supplementals as the year progressed. We continue to find surprises in different systems.

Chairman ARCHER. If there are immediate needs, we would like to be notified so that we can accommodate those in a responsible way.

Thank you, gentlemen. Appreciate your input.

Our next witness is Nancy-Ann DeParle, Administrator of HCFA. We're happy to have with us today, Ms. DeParle, and I see you brought with you Dr. Christoph, and welcome to you also. And if you'll officially identify yourself for the record, you may proceed?

STATEMENT OF NANCY-ANN MIN DEPARLE, ADMINISTRATOR, HEALTH CARE FINANCING ADMINISTRATION

Ms. DEPARLE. Thank you, Mr. Chairman, and distinguished Members of the Committee. Thank you for inviting me here to discuss the progress of the Health Care Financing Administration in addressing the Year 2000 computer challenge. As you said, Mr. Chairman, I have with me Dr. Gary Christoph, who I brought in as HCFA's chief information officer last year and who has been leading our information technology efforts. And he is no stranger to this Committee because he spent a good deal of time here with your staff over the year.

Mr. Chairman, HCFA still has a great deal of work to do, but we're making good progress and we'll be ready well before January 1, 2000. As you know, we're responsible for financing health care for Medicare beneficiaries. We can assure that our claims processing and payment systems work and that doctors and hospital bills will get paid. Continuity of care, however, depends on much more. Doctors, hospitals, and other providers must ensure that they are also ready. We are therefore engaging in an unprecedented outreach effort to help our partners meet their responsibility, and we appreciate the help of Members of this Committee in doing that.

We have aggressively attacked our part of this problem. We must continue to re-test systems and refine contingency plans. However, we've come a long way in the year since I became administrator. To get to this point we've had to make some tough decisions, including delaying some provisions of the Balanced Budget Act. We reached a significant milestone in December when we reported that all 25 of our internal mission-critical systems are now compliant. These are the systems that are under our direct control. At the same time, we also required the systems operated by the private insurance companies that we contract with to pay claims to be renovated and to complete three levels of testing by December 31, 1998. All 78 of the external mission-critical claims processing systems have been renovated now and 54 of them have been self-certified as compliant.

Let me stress that self-certification does not mean that our work is finished. It does mean that the software has been renovated and that it has been tested and that systems are able to process and play claims with future dates. We allowed contractors to self-certify based on just those things that they directly control. We required the contractors to tell us in detail about any qualifications, and we

investigated those qualifications ourselves. For the 54 contractors whose certifications we accepted, we're confident that the remaining problems are minor and do not significantly compromise the claims processing function.

We've established a war room to track progress on all fronts in our Baltimore headquarters. We have special teams on site all over the country monitoring contractors as they deal with their remaining work. And we're developing comprehensive business continuity and contingency plans in case any unforeseen problems arise.

We've asked our independent verification and validation contractor to be tough in judging our progress. They tell me that they are confident that our Y2K efforts will lead to success by January 1, 2000. Their latest report says that 17 contractor systems require only minimal effort to resolve remaining issues. Another 39 require moderate effort. And they agree with our assessment that about 54 of our 78 external contractor systems have adequately self-certified.

The GAO and our independent verification and validation contractor have identified essential work that remains for all our systems to be millennium ready. We agree with GAO that one of the most critical tasks is testing our many data exchanges to ensure that all of our interdependent systems function properly together. We also must continue end to end testing from the point of claim submission to the point of sending a payment instruction to a bank and printing a notice to a beneficiary.

Because testing is so important, we're going beyond current industry practice. Providers should be able to test whether a Y2K compliant claim can be accepted by our claims processing contractors. We're now instructing our contractors to begin testing with those providers throughout the country who want to submit future date claims. This will help build provider confidence. If they want to test their claims against our system, they can do so.

In addition, we plan to freeze all of our systems this summer and then to re-test and re-certify this fall in a fully production-ready integrated environment. For that final wave of testing, everything must work properly with no if's, and's or but's. And we also must finish and refine our contingency plans which we are doing in accordance with the GAO's advice.

Mr. Chairman, we have much more to do and we fully expect that there may be bumps in the road. But I want to assure you that we're committed to doing everything we need to do to get this job done. And I also want to say that all of this would have been much harder without Congress's support. And I want to thank you for that, as well as for GAO's diligent and continuous efforts with us.

Dr. Christoph and I will be happy to answer your questions.

[The prepared statement follows:]

Statement of Hon. Nancy-Ann Min DeParle, Administrator, Health Care Financing Administration

Chairman Archer, Congressman Rangel, distinguished committee members, thank you for inviting me here today to discuss my highest priority—the Year 2000 computer challenge. I am happy to report today that, despite serious concerns about the Health Care Financing Administration's (HCFA) ability to meet this challenge, we are making remarkable progress. In fact, I am confident that HCFA's own Year 2000 systems issues will be resolved well before January 1, 2000.

Our foremost concern has been and continues to be that our more than 70 million Medicare, Medicaid and Children's Health Insurance Program (CHIP) beneficiaries continue to receive the health care services they need. That is why we are not only addressing the Year 2000 issues in those systems over which we have responsibility, but are also engaging in an unprecedented outreach effort to raise awareness and provide information to those other parts of the health care system where we have little authority and control.

HCFA is responsible for the financing of health care for our beneficiaries. We can assure that HCFA's claims processing and payment systems will work, that doctors and hospital bills will get paid. Continuity of care, however, depends on far more than payment systems. It depends upon doctors, hospitals and other service providers ensuring that their equipment will work and their offices will remain open. It depends upon pharmaceutical and medical supply chains, which rely heavily on information technology, continuing to operate normally. And all of this, of course, requires the continued functioning of basic utility and telecommunication services.

We have aggressively attacked our part of the problem. While our job is not yet done, and we will continue to work hard for the next year on testing and retesting our systems, as well as developing our contingency plans, we have already accomplished a great deal.

• All 25 of our internal mission-critical systems are now certified as Year 2000 compliant, three months ahead of the government-wide deadline of March 31, 1999.

• All 78 of our external mission-critical claim processing systems that our claims processing contractors use to pay bills are renovated. Of these, 54 have been self-certified as compliant. Our independent verification and validation (IV&V) expert contractor has rated 17 systems as highly compliant and will require only a minimal effort to resolve any remaining issues; another 39 systems will require a moderate level of effort. Our IV&V contractor has assured us that these systems will be compliant on time and that there is no evidence to suggest they will not. We will continue to have our own experts and staff on-site, monitoring and assisting contractors with remaining Year 2000 work, and we will recertify all mission-critical systems before October 1999.

• And 27 of our 55 non-mission critical internal systems are certified as compliant.

We readily acknowledge that we got a late start with our Year 2000 problem, and that this has caused considerable concern and criticism. We recognize the importance of our programs to our beneficiaries and have thus set very aggressive goals and put together a vigorous Year 2000 program, with extensive testing and independent review. We have asked our IV&V contractor to set rigorous performance measures and be hard in their judgment of our contractors' progress.

For the remainder of 1999, we will continue to renovate, test, and retest our systems. We are ahead of schedule on our internal mission-critical systems, and we are well on our way to meeting the Federal government's March 31, 1999 deadline for our external systems. We will certainly be ready well before January 1, 2000.

I must be clear, however, about what HCFA can and cannot do. HCFA pays bills. Providers provide service and send claims to our claims processing contractors once services are delivered. We are responsible for all our own systems, our claims processing contractors' systems, and data exchange interfaces between all of these systems and the systems of States, providers, banks, phone companies, and other partners. We do not have the authority, ability, or resources to step in and fix systems for others, such as States or providers. And that leads to a rather substantial concern for which we need the assistance of Congress and others to address.

CONCERN FOR STATES AND PROVIDERS

It is not enough for HCFA alone to be ready for the Year 2000. Health care provider computers and systems must be Year 2000 compliant in order for providers to be able to generate and submit bills to us. State computers and systems also must be Year 2000 compliant for Medicaid and CHIP to continue uninterrupted payment for beneficiary service. Many States and providers will meet the Year 2000 challenge on time. However, monitoring by us and the General Accounting Office (GAO) indicates that some States and providers could well fail. This is the first time any of us have had to deal with such a problem, and we at HCFA are eager to share the lessons we have learned along the way. We are providing assistance to the extent that we are able. But that likely will not be enough. This matter is of urgent concern, and literally grows in importance with each passing day.

Our own progress in meeting the Year 2000 challenge is due in large part to the outstanding effort and commitment of staff throughout HCFA and at our Medicare contractors. We have been greatly aided by wise counsel from the GAO, and espe-

cially by the expert IV&V contractors we hired, based on the GAO's recommendations, to ensure that our Year 2000 work is done correctly. And, importantly, we could not have come so far so quickly without the timely support and funding that Congress has provided.

HCFA'S YEAR 2000 EFFORTS

There is no question that we have faced an uphill battle in achieving Year 2000 compliance. A number of key steps are getting us where we need to be. They include:

- *Building a "War Room"* in our Baltimore headquarters dedicated solely to tracking Year 2000 efforts on a daily basis not only within our own agency, but also with our partners across the country. I can now find out what is happening on any of our essential Year 2000 projects at a moment's notice. That is something I couldn't do last year.
- *Establishing contractor oversight teams* specifically responsible for closely monitoring and managing Year 2000 work for all contractors involved in processing Medicare claims. These teams include staff who are now on-site to oversee and aid contractors who most need assistance in meeting the March 31, 1999 deadline. They also provide timely information on contractors' status to the War Room.
- *Negotiating amendments* to contracts with more than 60 claims processing contractors. This established, for the first time, clear requirements that contractors must meet to make their information systems Year 2000 compliant.
- *Hiring AverStar, Inc.,* formerly Intermetrics, Inc., an IV&V contractor to provide assurance that our Year 2000 work is done right. They have helped us refine our renovation processes, measure our progress, as well as audit our testing plans and processes.
- *Hiring Seta Corporation,* another contractor providing independent testing of especially critical systems, to further ensure that the Year 2000 work on these systems has been done correctly. This independent testing goes beyond that described by GAO.
- *Helping States* by hiring another IV&V contractor, TRW, to visit every state and validate their Year 2000 progress. TRW is giving us direct information regarding the status of States' Year 2000 renovation efforts, particularly for critical Medicaid enrollment and claims processing systems. We also are sharing with the States whatever information and insights we can provide.
- *Helping providers* learn what they must do to prepare for the new millennium through an unprecedented and broad provider outreach campaign. It includes mailings, publications, an Internet site, a speakers' bureau, a number of seminars and conferences, and a wide range of other efforts.

SCOPE OF HCFA'S YEAR 2000 WORKLOAD

The Year 2000 especially affects the programs HCFA administers because of our extensive reliance on multiple computer systems. More than 150 different systems are used by HCFA in administering the Medicare program. About 100 of these systems are considered "mission-critical." These systems are both internal and external and are responsible for establishing beneficiary eligibility and making payments to providers, plans, and States. Medicare is the most automated health care payer in the country. We process nearly one billion claims annually, most electronically.

In fact, 97 percent of inpatient hospital and other Medicare Part A claims, and 81 percent of physician and other Medicare Part B claims are submitted electronically to the Medicare claims processing contractors. All claims undergo substantial electronic processing at the contractors and many claims are processed to payment with no manual intervention whatsoever. This high level of electronic billing has allowed us to achieve significant operating efficiency and cost savings. However, this reliance on automated systems also has made the Year 2000 computer fix a major challenge. Critical dates in computerized claims processing include the date a beneficiary became eligible, the date a patient was admitted or discharged from a hospital, the date a wheelchair rental began, or the date an enrollee entered a managed care plan.

Renovating all these systems has been complicated. Each system used by our programs and our 60-plus claims processing contractors, as well as interfaces with State Medicaid programs, banking institutions and some 1.3 million providers has to be thoroughly reviewed and renovated by those responsible for each particular system. We are requiring that systems be tested individually, as well as with the exchanges they perform with other partners.

To fix the Medicare systems alone, we have had to renovate some 49 million lines of internal and external systems code to find date-sensitive processes. We have had

to repair all of our Medicare-specific software so it will work with new versions of vendor-supplied software. We have had to update the operating systems that drive the hardware we use with millennium compliant versions. We also have had to test and upgrade deficient operational hardware, including our telecommunications equipment and software. And we must assure that all data exchanges with thousands of our partners will function properly.

PROVIDERS' PROGRESS

Providers must ready their own systems for the Year 2000 in a timely manner if the health care system is to meet the millennium challenge completely and successfully. One of the first steps, and perhaps the easiest, is changing the formats of claims to allow for 8-digit date fields. Our electronic media claims monitoring indicates that over 98 percent of Part B claims submitters (either physicians/suppliers or their billing agents) are submitting the 8-digit date fields. Fifty-eight percent of Part A submitters (hospitals and other institutions or their billing agents) that submit claims electronically are also using the 8-digit fields.

It is essential that all providers address the Year 2000 issue. Thus, we recently announced that we would require all submitters to start using the 8-digit date formats by April 5, 1999. Claims received on or after that date without the new formats will not be accepted. That does not mean that providers need to be fully compliant by April 5, but it does mean that we want to be assured that they have begun working on their systems by, at least, having taken this first step.

As mentioned earlier, we will be ready to process claims, but providers need to be able to submit correct claims. And, we are concerned that providers address other Year 2000 issues as well, not just their billing system issues. Providers must take appropriate Year 2000 remediation steps with other systems, such as clinical systems, and their biomedical devices to ensure continued high quality patient care.

PROTECTING BENEFICIARIES

I must stress our concern must always be focused first and foremost on protecting the beneficiaries and their continued access to care. Providers who fail to fix their own systems, and thus are unable to bill us for services, are strictly prohibited from billing beneficiaries. Beneficiaries are legally protected from liability for bills that Medicare would ordinarily pay, even if the provider is not Year 2000 compliant. To safeguard beneficiaries in the new millennium, we will provide them with a phone number to call to report any inappropriate billings they receive from providers or any difficulties they encounter in accessing care. Our beneficiaries are counting on us. Their health care needs will continue regardless of what day it is.

PROVIDER OUTREACH

Due to the critical need for providers to become Year 2000 compliant, we have launched a broad outreach campaign. Last month, in an unprecedented step, we mailed a letter to all 1.3 million providers serving our beneficiaries explaining the gravity of the Year 2000 problem and providing a checklist for what must be done to achieve compliance.

Our provider outreach campaign features a special Year 2000 Internet site, www.hcfa.gov/Y2K, which includes some of the basic steps that can be taken by a Medicare provider or supplier, such as:

- Preparing an inventory of hardware and software programs and identifying everything that is mission-critical to their business operations.
- Assessing the Year 2000 readiness of their inventory as well as options for upgrading or replacing systems, if necessary.
- Updating or replacing systems important to business operations, if necessary.
- Testing existing and newly purchased systems and software and their interfaces.
- Developing business continuity plans for unexpected problems.

The Internet site also includes links to other essential sites for providers, such as the Food and Drug Administration's Internet site on medical device compliance.

We have developed a speakers' bureau with staff trained to make presentations and answer questions on Year 2000 issues all around the country. We are leading the Health Care Sector of the President's Council on Year 2000 Conversion, which includes working closely with provider trade associations and public sector health partners to raise awareness of the millennium issue and encourage all providers to become compliant. And our claims processing contractors are offering providers Year 2000 compliant electronic billing software for free or at minimal cost.

I was pleased that some provider associations have recently announced their intention to assess the Year 2000 readiness of their membership and to step up educational efforts on the critical nature of this problem. This is an essential undertaking. Quite simply, Year 2000 compliance cannot be a one-way street. Providers also must meet this challenge head on, or risk not being able to receive prompt payment from Medicare, Medicaid, or virtually any other insurer.

We welcome Congress' help in making providers aware of the Year 2000 and energizing them to address their part of the problem. I invite you to help us identify opportunities to get the Year 2000 message across and encourage you to stress the importance of this issue when you meet with providers. As I mentioned previously, we have established a special Year 2000 speakers' bureau with staff around the country prepared to speak and offer guidance. You may want to have them join you when you meet with providers, and let others know that they are available.

STATES' PROGRESS

Our concern for States is as great as our concern for providers. For both, we do not have the authority, ability, or resources to step in and fix their systems for them. Our ten regional offices are monitoring the status of each State's remediation effort. We also have an expert IV&V contractor, TRW, to assist us in conducting on-site visits in every State to provide advice and validate assessments so that we can maintain an accurate picture of each State's progress. We have already done on-site visits in 13 States and the District of Columbia and expect to visit the remaining States by the end of April. The preliminary reports confirm earlier work by the GAO which strongly suggests that some States may not be ready on time.

We have asked all Medicaid and CHIP Directors to:

- report the status of their Year 2000 compliance efforts;
- document contingency plans for systems that may not be compliant;
- and provide updates to HCFA's regional offices on States' progress.

It is each State's responsibility to take the steps it believes are appropriate to meet the needs of its Medicaid and CHIP beneficiaries. Our primary role is to assess, as best we can, each State's progress and to provide guidance. While we do not have the authority, ability, or resources to fix State systems, we can and do want to help. Besides furnishing the services of TRW, we have developed technical assistance documents, and we have held regional meetings and workshops for States on how to develop contingency plans. We know that States and Congress share our goal of protecting all our beneficiaries throughout the millennium transition.

CONTINGENCY PLANNING

Although we fully intend to have our own systems ready long before January 1, 2000, we know we must be prepared in case any unanticipated problems arise. We are undertaking an extensive effort to develop contingency plans for all our mission-critical business processes. Our top priorities in developing these plans are to:

- process claims so as to be able to pay providers promptly;
- prevent payment errors and potential fraud and abuse;
- ensure quality of care; and
- enroll beneficiaries.

Contingency planning is an Agency-wide effort with active participation of all of our most senior executives. We are closely following the GAO's advice on contingency planning which they outlined in their August 1998 guidance, Year 2000 Business Continuity and Contingency Planning and in their September 1998 report, Medicare Computer Systems—Year 2000 Challenges Put Benefits and Services in Jeopardy .

We recently completed the second phase of the contingency planning process by reviewing 280 Medicare business processes, performing risk and impact analyses, and identifying the potential impact of mission-critical failures. We are now in the third phase wherein we will explicate and document our contingency plans and implementation modes, define events that will trigger use of the plans, as well as establish and train implementation teams should the need arise to execute the plans.

We expect to complete this third phase of contingency planning in March 1999. By the end of June 1999, our draft contingency plans will be validated, reviewed, and finalized. We anticipate completing our agency-wide plan by July 1999, three months ahead of the date recently recommended by GAO.

BUDGETARY NEEDS

The Year 2000 problem is not static. We are obligated to perform rigorous testing because of the extent of our reliance on information systems. Efforts to solve one

element of the problem often uncover other problems. This makes it challenging to determine our budgetary requirements. As you know, we previously have had to request additional funding and redirect existing funding to meet these changing demands.

In fiscal year 1998, we received $107.1 million in funding for millennium activities. This funding included a $15 million appropriation; an additional $30 million that was transferred from other agency projects; $20 million in redesignated funds originally appropriated for systems transitions; and $42.1 million made available by the Department of Health and Human Services (HHS) through the Secretary's one percent transfer authority. Through very careful financial management and a keen recognition of the importance of the Year 2000 effort, we actually obligated approximately $148 million in fiscal year 1998 on Year 2000 activities: $130 million on external systems and $18 million on internal systems.

Thanks to your support in the fiscal year 1999 appropriations process we are making significant progress toward obtaining the funding needed to support all of our Year 2000 efforts. We received $82.5 million in our appropriation for this year. The Office of Management and Budget (OMB), with Congressional concurrence, transferred an additional $205.1 million from the Year 2000 emergency fund. This funding provides a total of $287.6 million to support our Year 2000 efforts in fiscal year 1999. We plan to use FY 1999 as well as FY 2000 funding to increase our contingency planning efforts by developing, testing and rehearsing contingency plans.

The President's Budget request for FY 2000 includes an additional $150 million for our Year 2000 effort. In addition to funding our contingency planning efforts, a large portion of this funding will support outreach, continuing external systems remediation, and increases in billing and communications activities at our contractors. Increased public awareness of the Year 2000 and concern about potential problems, coupled with possible disruptions in claims processing, may increase the number and cost of paper and duplicate claims, the level of inquiries from beneficiaries and providers, as well as related printing and postage costs. This funding will help us and our contractors meet these anticipated challenges.

It is important to note that because our systems are highly automated and the majority of our processes are completed electronically, we are performing far more rigorous Year 2000 testing than many businesses. Many businesses are not testing their systems for future dates and they will not know with certainty if their systems will operate in the Year 2000. HCFA will. Our testing regimen is far more rigorous than the industry standard, with multiple layers of testing, including regression testing, testing in a simulated Year 2000 environment, and testing our entire systems in an actual Year 2000 environment.

In addition to the extensive tests performed by those who actually maintain the system, we also are requiring independent testing of our most critical systems and additional oversight by an IV&V contractor. This coming year we expect to perform extensive validation and recertification of these critical systems to ensure that changes made during 1999 do not affect our Year 2000 renovations. Although this additional testing and validation significantly increases the time required for and the cost of certifying the Medicare systems, we know that we simply cannot afford to fail and are doing everything within our power to ensure that we do not.

Our systems are not only complex in their own right, they also require extensive data exchanges with more than one million partners, such as providers, banks, and vendors. We must guarantee that all of our renovated systems work with all of these partners. And so we must conduct data exchange tests with the provider community to ensure that we can exchange the transactions required for electronic commerce.

CONCLUSION

We have made remarkable progress in our Year 2000 compliance effort and have taken critical steps to ensure that all of our systems will be ready for the new millennium. There is still a great deal of work to be done, but we now feel that we are making significant progress. We will continue in 1999 to work, test and retest our systems. But I must reiterate our concern with the progress of some States and providers in meeting their own Year 2000 challenges. We are committed to providing all the assistance we can, but in some cases that may not be enough. We all share a common goal of guaranteeing that our systems and programs function in the new millennium. I thank you for your attention to this essential issue, and I am happy to answer any questions you may have.

Chairman ARCHER. Well, Ms. DeParle, the Chair is imminently aware of the difficulty of the job that you have. The IRS is very, very tough and in a way bigger, but I don't think there's anything that is more difficult to manage than what you have to do. And we as the Congress want to cooperate with you in every way that we can.

I'm going to ask you the same questions that I've asked the other witnesses. They're both very brief. Are you confident that when January the 1st rolls around that HCFA will be able to perform its essential functions and services?

Ms. DEPARLE. Yes, sir, I am.

Chairman ARCHER. All right. So you think you'll be able to handle the Y2K problem?

Ms. DEPARLE. Yes, sir, I do.

Chairman ARCHER. All right. And that reimbursements to providers will occur in a timely fashion?

Ms. DEPARLE. Yes.

Chairman ARCHER. And has the Congress given you adequate resources in order to remediate any Y2K problems?

Ms. DEPARLE. Yes, you have. And I want to say again I appreciate the work that the Congress has done toward that end.

Chairman ARCHER. OK. Thank you very much. Are there any other questions of Ms. DeParle? Yes, Mrs. Johnson?

Mrs. JOHNSON of Connecticut. Thank you, Mr. Chairman. The GAO will testify that your progress has been overstated because you relied too much on self-certifications and that the independent contractor that you hired has found that most of the contractor self-certifications will need major to moderate level of effort to resolve. In other words, that the certifications were overstated and there's still work to be done, anywhere from major to moderate. You implied that work is proceeding. At what pace is it proceeding and when do you think you will start the end-to-end testing?

Ms. DEPARLE. We're already doing end to end testing in some cases, and we'll be in the thick of it throughout the spring and we'll finish some time this summer.

Mrs. JOHNSON of Connecticut. You'll finish end to end testing some time this summer?

Ms. DEPARLE. Yes, but then we'll probably do another round of it because, as you know, one of the challenges that we face is that there are changes continually made to the way we pay claims and to systems that have to do with implementation, for example, of changes in the law. As I mentioned, and, as you know, we've had to delay some of those changes because they were too complicated and would have gotten in the way of the work.

Mrs. JOHNSON of Connecticut. Right.

Ms. DEPARLE. But, for example, the system that maintains the names and eligibility of Medicare beneficiaries is called the common working file. And we'll be updating that throughout the year. So it won't be until the fall that we freeze all of that work and do final end to end testing.

Mrs. JOHNSON of Connecticut. Great. In discussing this with the Social Security Administration, when they did their first round of

end-to-end testing, they discovered some problems. And that's why you do it, you find out. And the second round they found less. But where are you in that process?

Ms. DEPARLE. I'm going to ask Dr. Christoph?

Mrs. JOHNSON of Connecticut. How many problems did you find the first time through? How long did it take to correct those problems? And what was the situation with the second round of testing?

Mr. CHRISTOPH. Well, actually we've done a complete round of testing with the majority of contractors, I would say about 70 of them, as part of our certification process. We've gone through three levels of testing, the last round of which was integrated or end-to-end testing. And we've already gone through that round. All of the problems that they've found have been fixed or will be fixed by the end of March. So we've gone through one full cycle at this point. And then the second round will occur starting July 1 and we've allowed 4 months for this.

Mrs. JOHNSON of Connecticut. And on your contingency plans, particularly in terms of payments, have you given any thought to the possibility of providing the equivalent of MIP payments to hospitals so that before the turn of the year they have a lump-sum payment which then they can rectify after the term of the year in case the system doesn't work. To large recipients of Medicare payments, inability to pay would be an absolute disaster. Is that kind of pre-payment plan, which we have used in Medicare over many years very satisfactorily, is that any part of your contingency planning and can hospitals through that mechanism rely, A, on payment and, B, on timely updates?

Ms. DEPARLE. Well, first of all, as I've discussed with you, Mrs. Johnson, we want providers to all be ready. And that is a big part of our effort right now. And I appreciate the help that you've provided up in Connecticut, with a State which is already, in fact, ahead of most of them in terms of its providers being ready. We are looking at a number of different possible contingency scenarios. The one you described is one of them. But I want to stress that we think the most important thing is for all providers to try to get ready. We don't want to provide right now some sort of a fix that might incentivize some providers to think, "Well, I don't have to get ready for this. I won't make the investment." But we are looking at all those kinds of contingencies and would be happy to discuss those with the Committee.

Mrs. JOHNSON of Connecticut. Thank you. Thank you, Administrator DeParle.

Chairman ARCHER. Mr. Houghton, do you have any questions?

Mr. HOUGHTON. No.

Chairman ARCHER. Mr. Foley.

Mr. FOLEY. In following up on Mrs. Johnson's questions, one thing came to mind because you're going to be integrating a new system clearly with a lot of providers trying to log on and communicate with your organization. Have you considered minimizing the changes to the system, the technical side, but to the codings and the reimbursements in the period with which you are then transitioning?

Ms. DEPARLE. Not only have we considered it, but, as I mentioned, we had to make some tough decisions last year. We have been in the process of implementing the 300-plus provisions of the Balanced Budget Act and because of the scenario you described, which is that it is difficult to make these kind of changes and to make sure they're going to work at the same time you're changing coding and changing other things to implement new payment methodologies prescribed by law. The independent verification and validation contractor recommended to me that we stop implementing some of the provisions of the Balanced Budget Act. And so we had to do that in order to minimize the kinds of changes that you're talking about because you're exactly right, they can pose problems if you're trying to make renovations and testing a system.

Mr. FOLEY. Because it seems one of the greatest complaints I get from providers is the fact that they're constantly being inundated with changes in the system. That's a fundamental problem to begin with. But then you lump in there compliance requirements for the Y2K, and so you've compounded what could be a disastrous consequence. And I think Mrs. Johnson mentioned and alluded to if the payments are then withheld, then the providers themselves can't meet their own obligations. And we see something spiraling terribly out of control.

Ms. DEPARLE. Well, the good news actually that I have to report is that as of January, the majority of claims submitters now are submitting compliant eight-digit date claims, which means that they at least are capable of submitting the claims with the four digits for the year, which is what they need to do. When I last talked to the Committee, it didn't look as good. Right now, for part A claims submitters, such as hospitals, 58 percent of them are already submitting claims in the proper format. And for Part B claims submitters, such as doctors, it's more than 98 percent. So we regard that as good news of their progress. But you're exactly right that it's difficult for them to make all these other changes at the same time they're trying to get their systems ready.

Mr. FOLEY. What do you see as the major risks remaining right now going into that final stage?

Ms. DEPARLE. I think the one that I just alluded to, which is that some providers may not make the changes they need to make. And we are working, as you know, we've sent out a letter to all 1.3 million Medicare providers, which is I think unprecedented. We don't deal directly with the providers. But we did it this time, in January, because we wanted to make sure that they were aware of the problem and knew what they needed to do to fix it. We're also allowing them to do testing of their claims in a future date environment if they want to. But one thing that the Members of Congress can do is to help us to get the word out; and we've offered to send speakers to your districts or do whatever we can to make sure that providers get ready.

Mr. FOLEY. Final follow-up. The question you mentioned about the delaying implementation of the requirements of the Balanced Budget Act, the good news is you're saying we're going to be compliant and probably ready to meet our expectations. The bad news is we'll probably overshoot the budget?

Ms. DEPARLE. Well, actually it turns out that most of the provisions that we're delaying aren't provisions that had significant savings or if they were, they're being delayed by a few months. And then, of course, the Committee last year dealt with one of them, which I appreciate, which was the home health problem, which we would have lost savings if we had not been able to implement that. And the Committee dealt with that last year.

Mr. FOLEY. Thank you, Mr. Chairman.

Chairman ARCHER. Mr. Tanner.

Mr. TANNER. Thank you very much, Mr. Chairman. I'm glad to see Ms. DeParle here. She is from Tennessee. And we've been friends for a long time. You alluded to the progress that has been made over the last 12 months. And could you expand on that because last year I know that there was some concern about where we might be now. And did I hear correctly 58 percent of the hospitals are now using——

Ms. DEPARLE. Yes, that's right. Our most recently available statistics show that 58 percent of Part A claims submitters, such as hospitals, are submitting claims in the 8-digit date compliant format. Now that doesn't mean that all their billing systems have been fixed, but it means they know how to submit a Medicare compliant claim, which I think is a good sign of progress.

Mr. TANNER. Your agency probably much more than any other Federal agency depends on data from States. How are we doing there with the interface that will have to take place on all of that data exchange?

Ms. DEPARLE. Well, last I guess late summer or early fall, we were concerned about the data we were getting from States about their Y2K readiness. As most members know, and I know you know, the Federal Government pays for half of their costs for running their systems. And we would pay for them to have independent verification and validation folks to come in and look at their systems. But most of them weren't doing that. So we decided last fall to hire an IV & V contractor to go out to the States and look at them. And we've now completed I think 14 site visits. Tennessee is not one of them yet. They're scheduled for a future month. By the end of April, we'll have been into every State and the District of Columbia.

And we're looking at two things, one is what's called the MMIS, which is the Medicaid Management Information System. That is the way they pay claims in the States. The other is the eligibility system. And in general what we're finding is consistent with what the GAO found when they looked at self-reported data in November, which is that most States' eligibility systems are in pretty good shape. There is a more mixed story on the side of the claims payment system. And there are a few States that appear to behind schedule. There are others that appear to be making good progress. And we are now engaging with those States to make sure that their Medicaid directors and their Governors and State officials are aware of the problem.

Mr. TANNER. Is there anything we can do to help in that regard, that the Congress could do?

Ms. DEPARLE. Well, at the appropriate time. We have sent out the information to each of the States and we've asked them to give

us back any of their comments. At the appropriate time, I would like to share with you where the States are because I think members need to know that.

Mr. TANNER. Yes and maybe we could help if necessary.

Ms. DEPARLE. Thank you.

Mr. TANNER. Thank you. Mr. Chairman, I yield back.

Chairman ARCHER. Are there any other further questions? Ms. DeParle, thank you very much. Dr. Christoph, thank you for being with us. We appreciate your input.

Ms. DEPARLE. Thank you, Mr. Chairman.

Chairman ARCHER. Our next panel is Mr. Fred Brown, Mr. Donald Palmisano, I'm sorry, Dr. Donald Palmisano, Curtis Lord, Diane Archer, and Joel Willemssen.

I've never met Ms. Archer but I wonder if we might be distantly related because my family originally settled at Fordham Manor when they came over from England in the New York area. And maybe we'll research that somewhere down the line.

Mr. Brown, I would like for you to be our first witness if you will. And if you will identify yourself for the record, you may proceed?

STATEMENT OF FRED BROWN, VICE CHAIRMAN, BJC HEALTH SYSTEMS, ST. LOUIS, MISSOURI, AND CHAIRMAN, BOARD OF TRUSTEES, AMERICAN HOSPITAL ASSOCIATION

Mr. BROWN. Thank you, Mr. Chairman.

Chairman ARCHER. And I think you probably heard the general ground rules, try to keep your verbal testimony within 5 minutes and your entire written statement will be printed in the record without objection. You may proceed.

Mr. BROWN. Realizing this is the last panel of a long day.

I am Fred Brown, vice chairman of BJC Health System in St. Louis, a regional system serving eastern Missouri and southern Illinois; and chairman of the board of trustees of the American Hospital Association. I am also part of the Senior Advisors Group of the President's Council on the Year 2000 Conversion, representing the hospital field. And I'm here today on behalf of the AHA's nearly 5,000 hospitals, health systems, networks, and other providers of care.

The AHA's goal is to help America's hospitals meet the year 2000 challenge. Our focus has been and will continue to be patient care. And our efforts continue to evolve. We began by building awareness and we have attempted to help provide hospitals the tools they need to examine their operations and make changes when necessary.

Last summer, the AHA conducted an informal survey of how prepared our members were for the turn of the century. The nearly 800 responses suggest that hospitals and health systems were diligently working to prepare for the year 2000. Seventy-seven percent had developed a plan of evaluation and action. Eighty-nine percent had already inventoried existing equipment. Seventy-six percent had survey vendors and manufacturers to identify year 2000 compliant equipment. Eighty-three percent had begun making existent equipment, hardware, software, and data sources year 2000 compliant. And eighty-one percent projected that year 2000 solutions would be complete in 1999.

What are the costs of these efforts expected to be? The bottom line is America's hospitals and health systems expect to spend somewhere around $8 billion to become Y2K compliant. And much of that $8 billion will be spent this year. And this presents an immense challenge because the spending comes on top of significantly declining Medicare reimbursement.

Regardless of how much is accomplished before December 31, 1999, meeting the Y2K challenge also requires being prepared for the unknown. And that gets me to the current phase of the AHA's Y2K efforts: contingency planning.

Contingency planning means asking and answering all the "what if" questions. These efforts need to be both internal, within hospital facilities, and external, within communities. This includes everyone that the hospital depends on, the medical equipment manufacturers, the power companies, and telecommunication companies. It also includes those who depend upon the hospital, like participants in the communities emergency services network.

We followed up in early March by distributing to each of our AHA members how-to materials for hospital contingency planning that stress the need for hospitals to plan with their community partners how to handle the Y2K induced losses or disruptions. In addition, the AHA is working with the Federal Emergency Management Administration to coordinate emergency preparedness efforts at a national level with contingency planning taking place at individual hospitals and local communities.

I applaud the efforts of the Health Care Financing Administration in their discussions about contingency planning. And as HCFA has indicated, they are confident that their payment mechanisms will not be affected by the millennium bug, but unforeseen problems could occur. It's imperative that there's communication between HCFA, HHS, and the hospital industry and providers to establish a fail-safe contingency plan. We're willing to continue to work and cooperate with HCFA to ensure that these concerns about the year 2000 are adequately addressed.

Medicare beneficiaries healthcare needs will remain constant regardless of how well we prepare for the year 2000 problems. If carrier and payment systems are affected by the millennium bug, hospitals' ability to continue providing high-quality healthcare could be severely affected. A system of advance payments based on past payment levels is one way this could be prevented and will ensure that hospitals have the resources necessary to care for Medicare patients in the event of any Y2K disruption.

We urge that this continually be monitored and there be appropriate legislation authorizing such a system and have HCFA make its contingency plans public.

Mr. Chairman, American hospitals and health systems, their State associations, and the AHA are partners in the effort to prepare for the year 2000. We encourage Congress and our Federal agencies to work with us as well and we'll continue to cooperate with all the agencies to ensure a smooth and healthy transition into the new millennium.

This concludes my remarks, and I will be glad to answer any questions.

[The prepared statement follows:]

Statement of Fred Brown, Vice Chairman, BJC Health Systems, St. Louis, Missouri, and Chairman, Board of Trustees, American Hospital Association

Mr. Chairman, I am Fred Brown, vice chairman of BJC Health Systems in St. Louis and chairman of the Board of Trustees of the American Hospital Association (AHA). I am here on behalf of the AHA's nearly 5,000 hospitals, health systems, networks, and other providers of care. I am also privileged to be a Senior Advisor to the President's Council on Year 2000 Conversion, representing the hospital field.

The AHA and its members are committed to taking whatever steps are necessary to prevent potential Year 2000 problems from interrupting the smooth delivery of high-quality health care. We appreciate this opportunity to update you on our efforts, to outline the role that the AHA has taken in aiding the health care field, and to highlight some areas in which the government and its agencies can help as they play their critical roles in this historic effort.

PROGRESS ON Y2K COMPLIANCE

The AHA last summer conducted an informal survey of how prepared our members were for the turn of the century. The nearly 800 responses suggest that hospitals and health systems are diligently working to prepare for the Year 2000, and are committed to the smooth delivery of patient care without interruptions. Respondents represented individual hospitals and multi-hospital systems in urban and rural areas. Some highlights:

- 77% had developed a systematic plan of evaluation and action.
- 89% had already inventoried existing equipment.
- 76% had surveyed vendors/manufacturers to identify Year 2000-compliant equipment.
- 83% had begun making existing equipment, hardware, software and data sources Year 2000 compliant.
- 81% projected that their Year 2000 solutions would be complete in 1999.

I'll use my organization, BJC Health System in St. Louis, to personify what these statistics mean. At BJC, Y2K has been the focus in the information systems department for more than 18 months. The first priority of all Y2K projects is, of course, any equipment that is directly related to patient care. We feel comfortable with our progress so far. We will continue working diligently throughout 1999 to ensure that the Year 2000 change occurs with minimal disruption in our facilities. Since the last half of 1997, our information services department's primary focus has been Y2K. Dozens of individuals have been solely dedicated to examining computer codes, programs and computer-assisted medical devices to ensure that they will work in the new millennium. Along with information services, BJC's material services department is playing a critical role in our Y2K compliance. Materials services is primarily working with vendors and their related equipment, and with clinical engineering, which oversees all patient-related equipment in BJC's hospitals and facilities.

THE COSTS OF COMPLIANCE

What are the costs of Y2K compliance expected to be? The AHA is releasing today a new survey that looks into that question. The survey was sent to 2,000 hospital and health system CEOs early last month. Five hundred and six surveys were returned, an excellent 25.3 percent response rate. The results, quite frankly, point to a huge financial investment by hospitals and health systems. The bottom line is that America's hospitals and health systems expect to spend somewhere around $8 billion to become Y2K compliant.

Smaller hospitals, those with fewer than 100 beds, will spend close to $1 billion on Y2K fixes, or an average of $435,000 each. Hospitals with between 100 and 300 beds will spend $2.5 billion, an average of $1.2 million each. Hospitals with 300–500 beds will spend nearly $2 billion, or $3.4 million each. The largest amount of spending, $2.2 billion, will occur at hospitals that have more than 500 beds.

Much of the $8 billion that hospitals expect to spend on Y2K compliance will be spent this year. This presents an immense challenge, because that spending comes on top of significantly declining Medicare reimbursement brought by the Balanced Budget Act (BBA) of 1997. The BBA reduced payments to hospitals by $44.1 billion over five years. Further reductions, like those proposed in the Administration's recent budget proposal, would make a terrible burden even more onerous.

THE ROLE OF AHA AND OTHER ASSOCIATIONS

Hospitals and health systems face the same kinds of Y2K concerns as other critical sectors of our nation. However, hospitals are unique. They have a special place

in America's social services safety net. Every community in America relies on its local hospital to be ready to provide high-quality health care services on demand, 24 hours a day. It is therefore very important that the public understand that hospitals have been very aggressive in their efforts to ensure the seamless delivery of health care services before, during, and after the turn of the century. And it is important for hospitals to have a contingency plan in place.

Protecting Public Confidence, Staying Abreast of Progress

The AHA, in collaboration with our state, regional and metropolitan associations and other key strategic partners, is working hard to stress to our member hospitals the importance of managing the Y2K issue from a public confidence perspective. We are developing tools to counsel hospitals and health systems about how to talk with the public about Y2K and health care. A Y2K Communications Action Kit is being developed that will be distributed in early March to all our state associations, which they will then distribute to our members. Our members will be urged and encouraged to adapt the materials in the kits for use in their communities. The kit will include tools and samples of how to communicate to various audiences about the Y2K issue.

We are continuing our efforts to make sure that hospitals and health systems have the latest information on what their colleagues and other organizations are doing to address the Y2K problem. And we are helping them learn about potential solutions.

Our State Issues Forum, which tracks state-level legislative and advocacy activities, is hosting biweekly conference calls dedicated entirely to the Year 2000 issue. On these calls, state hospital association and AHA staff share information. A special AHA task force on the Year 2000 problem has been drawing up timelines for action to make sure our members get the latest information and know where to turn for help.

Articles are appearing regularly in AHA News, our national newspaper, in Hospitals and Health Networks, our national magazine for hospital CEOs, in Trustee, our national magazine for volunteer hospital leadership, and in several other national publications that are published by various AHA membership societies. Several of these societies, such as the American Society for Healthcare Engineering and the American Society for Healthcare Risk Management, are deeply involved in helping their members attack the millennium bug in their hospitals.

In addition, the AHA Web site has become an important clearinghouse of information on the Year 2000 issue, including links to other sites with information that can help our members.

Contingency Planning

The AHA believes that the best approach for hospitals to manage potential disruptions on January 1, 2000, is to anticipate them. Specifically, it is incumbent upon hospitals to prepare now to respond to the potential loss or disruption of any essential hospital processes or services. These efforts need to be directed both internally across hospitals' facilities, and externally within communities. This would include working with such entities as utility companies, emergency medical services, and other health care providers.

The AHA, along with state, regional and metropolitan hospital and health system associations, is working hard to make sure that America's hospitals and health systems are informed about, educated on, and assisted with Year 2000 contingency planning. We recently distributed to every AHA member an executive briefing on hospital contingency planning. This briefing emphasizes the interdependent nature of health care, and stresses the need for hospitals to plan in advance, with their key partners, how they will handle potential Y2K-induced losses or disruptions.

This executive briefing will be followed up in early March by "how-to" materials for hospital contingency planning, including a business continuity planning guide and a set of alternate operating procedures that address the most mission-critical processes of hospitals. The AHA also is working with the Odin Group's VitalSigns 2000 project, which draws on leadership from health care provider, payer, pharmaceutical, and supplier sectors to develop a pamphlet that will help consumers understand Y2K and health care.

In addition, the AHA will be working with the Federal Emergency Management Administration to coordinate emergency preparedness efforts at a national level with contingency planning taking place at individual hospitals in local communities. At a meeting scheduled for March, we will bring together representatives of major health systems and health care manufacturing and supply companies to discuss how we can provide guidance to the health care field on issues related to Y2K prepared-

ness and concerns about health care equipment and pharmaceutical supply and stockpiling.

THE ROLE OF THE FDA

Of course, if hospitals are to communicate realistically with their communities about Y2K readiness, they must receive realistic communications from manufacturers about the Y2K readiness of medical devices and equipment. While health care providers can inventory their thousands of devices and pieces of equipment, the information about whether these devices are Year 2000-compliant *must come from the manufacturers*. Several organizations, both public and private, have undertaken concerted efforts to collect this information. Key among them are the Veterans Administration, the Food and Drug Administration (FDA), and a consortium of state hospital associations and the AHA, through the Security Third Millennium product. The AHA has urged the FDA to play a lead role in getting manufacturers to report on the Y2K compliance of their products, and the FDA has responded. The Center for Devices and Radiological Health (CDRH), the arm of the FDA responsible for regulating the safety and effectiveness of medical devices, has taken a number of steps to ensure that manufacturers of medical devices address potential Year 2000 problems. We commend the center for its actions. And we commend the many manufacturers that have made available important information about their products' Y2K status.

However, some of the information that has been reported has not been reported in a way that is helpful. Therefore, the FDA must require manufacturers to improve the quality of information that hospitals receive. This involves important issues such as good descriptions of how a product might be affected if it is not Y2K compliant. It also includes ensuring that manufacturers specifically report which of their devices and products are Y2K compliant, instead of just reporting about those products that may not yet be compliant.

We also urge the FDA to take further steps in two specific areas. The first is to mandate that non-reporting manufacturers report on the Y2K readiness of their products. The second is for the FDA to adopt a rumor control function. There are a lot of rumors and anecdotal stories about the implications of the turn of the century being spread—on the Internet, for example—that need to be reined in. We urge the FDA to establish itself as the place where people go to get the truth.

THE ROLE OF HCFA

On average, America's hospitals and health systems receive roughly half of their revenues from government programs like Medicare and Medicaid. If that much revenue were to be suddenly cut off, hospitals could not survive, and patient care could be jeopardized. Hospitals would not be able to pay vendors. They would not be able to purchase food, supplies, laundry services, maintain medical equipment—in short, they would not be able to do the job their communities expect of them. All this would occur even as hospitals and health systems faced the substantial costs of addressing their own Year 2000 system needs—costs that are not recognized in the calculation of current Medicare payment updates.

We applaud the Health Care Financing Administration's (HCFA) announcement that the Fiscal Year 2000 PPS update will no longer have to be delayed while the agency prepares its computer systems for Y2K. We congratulate the agency's personnel for tackling the problem in such a way that it apparently will no longer require nearly $300 million in payment updates to be held back from the hospitals that need them. However, our congratulations are tempered by our concern that HCFA has not yet announced that it has an adequate contingency plan in place.

Even if HCFA and its contractors express confidence that their payment mechanisms will not be affected by the millennium bug, unforeseen problems could crop up. Therefore, it is imperative that HCFA establish a fail-safe contingency plan in case HCFA or its contractors' payment mechanisms somehow fail at the turn of the century. We have offered to work with HCFA to ensure that these short-and long-term concerns about the Year 2000 are adequately addressed.

Medicare beneficiaries' health care needs will remain constant, regardless of how well we are prepared for Year 2000 problems. If carrier and fiscal intermediary payment systems are clogged up by the millennium bug, hospitals' ability to continue providing high-quality health care could be severely affected. A system of advance payments, based on past payment levels, is one way that this could be done. It would ensure that hospitals have the resources necessary to care for Medicare patients. We urge Congress to enact legislation to authorize such a system, and require that HCFA subject such contingency plans to public comment.

HCFA also must make sure its contractors—including Medicare+Choice plans—take steps to ensure that their performance will not be interrupted by Year 2000 problems caused by the millennium bug. HCFA should make readily available its work plan, and progress reports, for bringing the contractors and Medicare+Choice plans into compliance and monitor their efforts. Letting providers know what changes may be required of them is also important. This would allow providers, contractors and plans to prepare simultaneously and ensure that their systems are compatible.

It is important to note that Medicare is not the only payer for hospital services. Similar payment delays could occur if private health insurers and, in the case of Medicaid, individual states, have not addressed their own Year 2000 problems. HCFA has the authority and leverage to prevent this from happening, and we urge the agency to exercise that authority.

THE ROLE OF CONGRESS

As I have described, health care providers and the associations that represent them are devoting significant time, resources and energy to preventing potential Year 2000 problems from affecting patient safety. It is essential that we all look for ways to help prepare America's health care system for the turn of the century, and Congress can play an important role. Your attention to this issue, through hearings such as this, reflects your understanding of the gravity of the situation.

One major step toward Y2K compliance occurred when Congress passed its "Good Samaritan" legislation. By shielding from liability the sharing of information among businesses that provide it in good faith, this law encourages all parties—providers, suppliers, manufacturers, and more—to work together.

We ask you to help America's health care system avoid Year 2000 problems by taking several other steps:

- Congress should provide the FDA with any additional authority it needs to mandate reporting by manufacturers.
- Congress should authorize advance payments under Medicare. These payments, based on past payment levels, should be implemented to ensure adequate cash flow for providers in case carrier and fiscal intermediary payment systems fail due to the date change. Congress also should ensure that HCFA has adequate funding to ensure Y2K compliance, including the testing needed to demonstrate that the claims processing and payment systems work for the government, providers, contractors, and beneficiaries alike.
- There has been some talk of the need for a contingency fund to be created, from which states (in the case of Medicaid, for example) or hospitals could draw monies needed to continue operating in case of a Y2K disruption. We would be glad to be a part of any discussions concerning how such a fund should be set up.

Mr. Chairman, the Year 2000 issue will affect every aspect of American life, but few, if any, are as important as health care. America's hospitals and health systems, their state associations, and the AHA are partners in the effort to prepare for the Year 2000. We encourage Congress and our federal agencies to work with us as well. Together, we can ensure a smooth—and healthy—transition into the new millennium.

[Attachment is being retained in Committee files.]

Chairman ARCHER. Thank you, Mr. Brown.

Dr. Palmisano, if you'll identify yourself for the record, you may proceed?

STATEMENT OF DONALD J. PALMISANO, M.D., J.D., MEMBER, BOARD OF DIRECTORS, AND CHAIR, DEVELOPMENT COMMITTEE, NATIONAL PATIENT SAFETY FOUNDATION, AND MEMBER, BOARD OF TRUSTEES, AMERICAN MEDICAL ASSOCIATION

Dr. PALMISANO. Thank you, Mr. Chairman. My name is Dr. Palmisano. I am a board member of the American Medical Association, and I want to thank you for inviting me to testify today.

The year 2000 problem will affect virtually all aspects of the medical profession, most especially patient care. By nature of its work, the medical profession has to rely heavily on technology. Most all physicians use computers in their practices. They do so for scheduling, reimbursement, and increasingly for more clinical functions, such as logging patient histories. Patients and physicians also rely on medical equipment with embedded micro-chips.

With this reliance comes the risk of malfunctions due to the Y2K bug. Imagine for a moment yourself as the patient. How would you feel if a device that was monitoring your heart failed to sound an alarm when your heart slowed to a dangerous rate or if a portable defibrillator failed to function at the moment you went into ventricular fibrillation. Obviously, these events would alarm you and your physician. The risk of device malfunctions is real and it has to be anticipated and eliminated.

Although the year 2000 problem still poses significant risks for patient care and may adversely affect physicians' administrative responsibilities, the good news is that the medical profession is making significant progress. In its efforts to assist physicians to achieve compliance, the AMA has been focusing on three areas: education, communication, and cooperation.

For about a year, the AMA has been educating physicians and medical students with two of its publications, AMA News and the Journal of the American Medical Association, JAMA. We have been raising physicians' level of awareness of the year 2000 problem with numerous articles on a variety of Y2K subjects from patient safety concerns to developments in Y2K legislation. The AMA has also launched a national campaign that focuses both on education and communication. As part of this campaign, the AMA has begun holding regional seminars to talk about best to work with vendors and how to obtain necessary information about devices that could affect patient care.

We also have made available to literally hundreds of thousands of physicians a solutions manual entitled: "The Year 2000 Problem: Guidelines for Protecting Your Patients and Practice." And I have the manual here in my hand. And Members of the Committee have been given a copy of this particular manual. This booklet talks about Y2K compliance requirements, how to obtain information about medical devices, self-assessment programs, contingency plans, and a lot more. It also identifies a host of other resources for physicians to obtain help in becoming Y2K compliant.

To foster greater communication among physicians about the Y2K problem, the AMA has established a special section on its award-winning website: www.ama-assn.org. And we invite everyone to visit this site. We believe this will serve as an important interactive resource for physicians by providing regularly updated information about the millennium bug and by enabling physicians to assist each other in solving their Y2K problems.

The AMA is also promoting cooperation through our involvement with the National Patient Safety Foundation. This Foundation already coordinates efforts within the healthcare system to try and prevent avoidable patient injuries. The AMA launched the Foundation in partnership with other healthcare organizations and safety experts. In addition, we helped form the National Patient Safety

Partnership, which was convened by the Department of Veteran Affairs. It's a public-private partnership. And this has shown particular leadership on the Y2K problem, trying to increase the medical community's awareness of the issues.

We might ask ourselves what more can be done? First, we cannot become complacent. Not until we have full Y2K compliance throughout the healthcare community, and for that matter throughout all industries, can we claim success. Physicians and other healthcare advocates continue to call on medical device manufacturers to disclose immediately whether their products will malfunction. Only they have that information. The physicians and patients do not have the expertise or resources to know what devices may or may not fail. We have to rely on the manufacturers, the Congress, and the administration to ensure that they promptly disclose this vital information.

We are aware that last year, The Year 2000 Information and Readiness Disclosure Act was enacted into law. As Congress considers other methods of motivating vendors to disclose medical device information, the AMA wants to go on record as continuing to oppose any tradeoff of liability immunity for information disclosure.

Finally, we need to reassure patients that medical devices will continue to work safely regardless of the year 2000. We do not want a lack of information to cause patients to panic. The patient has to be our number one concern in all of our Y2K efforts.

Thank you very much, once again, for inviting me, Mr. Chairman and Members of the Committee, to testify on behalf of the AMA. Allow me to offer our services in working further with the Congress to effectively address this problem.

Thanks.

[The prepared statement follows:]

Statement of Donald J. Palmisano, M.D., J.D., Member, Board of Directors, and Chair, Development Committee, National Patient Safety Foundation; and Member, Board of Trustees American Medical Association

Mr. Chairman and Members of the Committee, my name is Donald J. Palmisano, MD, JD. I am a member of the Board of Trustees of the American Medical Association (AMA), a Board of Directors member of the National Patient Safety Foundation (NPSF) and the Chair of the Development Committee for the same foundation. I also practice vascular and general surgery in New Orleans, Louisiana. On behalf of the three hundred thousand physician and medical student members of the AMA, I appreciate the chance to comment on the issue of year 2000 conversion efforts and the implications of the year 2000 problem for health care beneficiaries.

INTRODUCTION

The year 2000 problem has arisen because many computer systems, software and embedded microchips cannot properly process date information. These devices and software can only read the last two digits of the "year" field of data; the first two digits are presumed to be "19." Consequently, when data requires the entry of a date in the year 2000 or later, these systems, devices and software will be incapable of correctly processing the data.

Currently, nearly all industries are in some manner dependent on information technology, and the medical industry is no exception. As technology advances and its contributions mount, our dependency and consequent vulnerability become more and more evident. The year 2000 problem is revealing to us that vulnerability.

By the nature of its work, the medical industry relies tremendously on technology, on computer systems—both hardware and software, as well as medical devices that have embedded microchips. A survey conducted last year by the AMA found that almost 90% of the nation's physicians are using computers in their practices, and

40% are using them to log patient histories.[1] These numbers appear to be growing as physicians seek to increase efficiency and effectiveness in their practices and when treating their patients.

Virtually every aspect of the medical profession depends in some way on these systems—for treating patients, handling administrative office functions, and conducting transactions. For some industries, software glitches or even system failures, can, at best, cause inconvenience, and at worst, cripple the business. In medicine, those same software or systems malfunctions can, much more seriously, cause patient injuries and deaths.

PATIENT CARE

Assessing the current level of risk attributable specifically to the year 2000 problem within the patient care setting remains problematic. We do know, however, that the risk is present and it is real. Consider for a minute what would occur if a monitor failed to sound an alarm when a patient's heart stopped beating. Or if a respirator delivered "unscheduled breaths" to a respirator-dependent patient. Or even if a digital display were to attribute the name of one patient to medical data from another patient. Are these scenarios hypothetical, based on conjecture? No. Software problems have caused each one of these medical devices to malfunction with potentially fatal consequences.[2] The potential danger is present.

The risk of patient injury is also real. Since 1986, the FDA has received more than 450 reports identifying software defects—not related to the year 2000—in medical devices. Consider one instance—when software error caused a radiation machine to deliver excessive doses to six cancer patients; for three of them the software error was fatal.[3] We can anticipate that, left unresolved, medical device software malfunctions due to the millennium bug would be prevalent and could be serious.

Medical device manufacturers must immediately disclose to the public whether their products are Y2K compliant. Physicians and other health care providers do not have the expertise or resources to determine reliably whether the medical equipment they possess will function properly in the year 2000. Only the manufacturers have the necessary in-depth knowledge of the devices they have sold.

Nevertheless, medical device manufacturers have not always been willing to assist end-users in determining whether their products are year 2000 compliant. Last year, the Acting Commissioner of the FDA, Dr. Michael A. Friedman, testified before the U.S. Senate Special Committee on the Year 2000 Problem that the FDA estimated that only approximately 500 of the 2,700 manufacturers of potentially problematic equipment had even responded to inquiries for information. Even when vendors did respond, their responses frequently were not helpful. The Department of Veterans Affairs reported last year that of more than 1,600 medical device manufacturers it had previously contacted, 233 manufacturers did not even reply and another 187 vendors said they were not responsible for alterations because they had merged, were purchased by another company, or were no longer in business. One hundred two companies reported a total of 673 models that were not compliant but should be repaired or updated this year.[4] Since July 1998, however, representatives of the manufacturers industry have met with the Department of Veterans Affairs, the FDA, the AMA and others to discuss obstacles to compliance and have promised to do more for the health care industry.

ADMINISTRATIVE

Many physicians and medical centers are also increasingly relying on information systems for conducting medical transactions, such as communicating referrals and electronically transmitting prescriptions, as well as maintaining medical records. Many physician and medical center networks have even begun creating large clinical data repositories and master person indices to maintain, consolidate and manipulate clinical information, to increase efficiency and ultimately to improve patient care. If these information systems malfunction, critical data may be lost, or worse—

---

[1] "Doctors Fear Patients Will Suffer Ills of the Millennium Bug; Many Are Concerned That Y2K Problem Could Erroneously Mix Medical Data—Botching Prescriptions and Test Results," Los Angeles Times, Jan. 5, 1999, p. A5.

[2] Anthes, Gary H., "Killer Apps; People are Being Killed and Injured by Software and Embedded Systems," Computerworld, July 7, 1997.

[3] *Id.*

[4] Morrissey, John, and Weissenstein, Eric, "What's Bugging Providers," Modern Healthcare, July 13, 1998, p. 14. Also, July 23, 1998 Hearing Statement of Dr. Kenneth W. Kizer, Undersecretary for Health Department of Veterans Affairs, before the U.S. Senate Special Committee on the Year 2000 Technology Problem.

unintentionally and incorrectly modified. Even an inability to access critical data when needed can seriously jeopardize patient safety.

Other administrative aspects of the Y2K problem involve Medicare coding and billing transactions. In the middle of last year, HCFA issued instructions through its contractors informing physicians and other health care professionals that electronic and paper claims would have to meet Y2K compliance criteria by October 1, 1998. In September 1998, however, HCFA directed Medicare carriers and fiscal intermediaries not to reject or "return as unprocessable" any electronic media claims for non-Y2K compliance until further notice. That notice came last month. In January 1999, HCFA instructed both carriers and fiscal intermediaries to inform health care providers, including physicians, and suppliers that claims received on or after April 5, 1999, which are not Y2K compliant will be rejected and returned as unprocessable.

We understand why HCFA is taking this action at this time. We genuinely hope, however, that HCFA, to the extent possible, will assist physicians and other health care professionals who have been unable to achieve Y2K compliance by April 5. We have been informed that HCFA has decided to grant physicians additional time, if necessary, for reasonable good faith exceptions, and we strongly support that decision. Physicians are genuinely trying to comply with HCFA's Y2K directives. In fact, HCFA has already represented that 95% of the electronic bills being submitted by physicians and other Medicare Part B providers already meet HCFA's Y2K filing criteria. HCFA must not withhold reimbursement to, in any sense, punish those relatively few health care professionals who have lacked the necessary resources to meet HCFA's Y2K criteria. Instead, physicians and HCFA need to continue to work together to make sure that their respective data processing systems are functioning properly for the orderly and timely processing of Medicare claims data.

We also hope that HCFA's January 1999 instructions are not creating a double standard. According to the instructions, HCFA will reject non-Y2K compliant claims from physicians, other health care providers and suppliers. HCFA however has failed to state publicly whether Medicare contractors are under the same obligation to meet the April 5th deadline. Consequently, after April 5th non-compliant Medicare contractors will likely continue to receive reimbursement from HCFA while physicians, other health care providers, and suppliers that file claims not meeting HCFA's Y2K criteria will have their claims rejected. This inequity must be corrected.

Medicare administrative issues are of critical importance to patients, physicians, and other health care professionals. In one scenario that took place in my home state of Louisiana, Arkansas Blue Cross & Blue Shield, the Medicare claims processor for Louisiana, implemented a new computer system—intended to be Y2K compliant—to handle physicians' Medicare claims. Although physicians were warned in advance that the implementation might result in payment delays of a couple of weeks, implementation problems resulted in significantly longer delays. For many physicians, this became a real crisis. Physicians who were treating significant numbers of Medicare patients immediately felt significant financial pressure and had to scramble to cover payroll and purchase necessary supplies.[5]

We are encouraging physicians to address the myriad challenges the Y2K dilemma poses for their patients and their practices, which include claims submission requirements. The public remains concerned however that the federal government may not achieve Y2K compliance before critical deadlines. An Office of Management and Budget report issued on December 8, 1998, disclosed that the Department of Health and Human Services is only 49% Y2K compliant.[6] In a meeting last week, though, HCFA representatives stated that HCFA has made significant progress towards Y2K compliance, specifically on mission critical systems. In any case, we believe that HCFA should lead by example and have its systems in compliance as quickly as possible to allow for adequate parallel testing with physician claims submission software and other health care professionals. Such testing would also allow for further systems refinements, if necessary.

---

[5] "Year 2000 Bug Bites Doctors; Glitch Stymies Payments for Medicare Work," The Times-Picayune, June 6, 1998, page C1.

[6] "Clinton Says Social Security is Y2K Ready," Los Angeles Times, December 29, 1998, p. A1. See "Government Agencies Behind the Curve on Y2K Issue," Business Wire, January 28, 1999 (stating that Computer Week on November 26, 1998 reported only a 34% Y2K compliance level for the Department of Health and Human Services).

REIMBURSEMENT AND IMPLEMENTATION OF BBA

To shore up its operations, HCFA has stated that it will concentrate on fixing its internal computers and systems. As a result, it has decided not to implement some changes required under the Balanced Budget Act (BBA) of 1997, and it plans to postpone physicians' payment updates from January 1, 2000, to about April 1, 2000.

In the AMA's view, the Y2K problem is and has been an identifiable and solvable problem. Society has known for many years that the date problem was coming and that individuals and institutions needed to take remedial steps to address the problem. There is no justification for creating a situation where physicians, hospitals and other providers now are being asked to pay for government's mistakes by accepting a delay in their year 2000 payment updates.

HCFA has indicated to the AMA that the delay in making the payment updates is not being done to save money for the Medicare Trust Funds. In addition, the agency has said that the eventual payment updates will be conducted in such a way as to fairly reimburse physicians for the payment update they should have received. In other words, the updates will be adjusted so that total expenditures in the year 2000 on physician services are no different than if the updates had occurred on January 1.

We are pleased that HCFA has indicated a willingness to work with us on this issue. But we have grave concerns about the agency's ability to devise a solution that is equitable and acceptable to all physicians.

Also, as it turns out, the year 2000 is a critical year for physicians because several important BBA changes are scheduled to be made in the resource-based relative value scale (RBRVS) that Medicare uses to determine physician payments. This relative value scale is comprised of three components: work, practice expense, and malpractice expense. Two of the three—practice expense and malpractice—are due to undergo Congressionally-mandated modifications in the year 2000.

In general, the practice expense changes will have different effects on the various specialties. Malpractice changes, to some modest degree, would offset the practice expense redistributions. To now delay one or both of these changes will have different consequences for different medical specialties and could put HCFA at the eye of a storm that might have been avoided with proper preparation.

To make matters worse, we also are concerned that delays in Medicare's reimbursement updates could have consequences far beyond the Medicare program. Many private insurers and state Medicaid agencies base their fee-for-service payment systems on Medicare's RBRVS. Delays in reimbursement updates caused by HCFA may very well lead other non-Federal payers to follow Medicare's lead, resulting in a much broader than expected impact on physicians.

CURRENT LEVEL OF PREPAREDNESS

Assessing the status of the year 2000 problem is difficult not only because the inventory of the information systems and equipment that will be affected is far from complete, but also because the consequences of noncompliance for each system remain unclear. Nevertheless, if the studies are correct, malfunctions in noncompliant systems will occur and equipment failures can surely be anticipated. The analyses and surveys that have been conducted present a rather bleak picture for the health care industry in general, and physicians' practices in particular.

The Odin Group, a health care information technology research and advisory group, for instance, found from a survey of 250 health care managers that many health care companies by the second half of last year still had not developed Y2K contingency plans.[7] The GartnerGroup has similarly concluded, based on its surveys and studies, that the year 2000 problem's "effect on health care will be particularly traumatic . . . [l]ives and health will be at increased risk. Medical devices may cease to function."[8] In its report, it noted that most hospitals have a few thousand medical devices with microcontroller chips, and larger hospital networks and integrated delivery systems have tens of thousands of devices.

Based on early testing, the GartnerGroup also found that although only 0.5–2.5 percent of medical devices have a year 2000 problem, approximately 5 percent of health care organizations will not locate all the noncompliant devices in time.[9] It determined further that most of these organizations do not have the resources or

[7] "Health Care Not Y2K-Ready—Survey Says Companies Underestimate Need For Planning; Big Players Join Forces," InformationWeek, January 11, 1999.

[8] GartnerGroup, Kenneth A. Kleinberg, "Healthcare Worldwide Year 2000 Status," July 1998 Conference Presentation, p. 2 (hereinafter, GartnerGroup).

[9] *Id.* at p. 8.

the expertise to test these devices properly and will have to rely on the device manufacturers for assistance.[10]

As a general assessment, the GartnerGroup concluded that based on a survey of 15,000 companies in 87 countries, the health care industry remains far behind other industries in its exposure to the year 2000 problem.[11] Within the health care industry, the subgroups which are the furthest behind and therefore at the highest risk are "medical practices" and "in-home service providers."[12] The GartnerGroup extrapolated that the costs associated with addressing the year 2000 problem for each practice group will range up to $1.5 million per group.[13]

REMEDIATION EFFORTS—AMA'S EFFORTS

We believe that through a united effort, the medical profession in concert with federal and state governments can dramatically reduce the potential for any adverse effects within the medical community resulting from the Y2K problem. For its part, the AMA has been devoting considerable resources to assist physicians and other health care providers in learning about and correcting the problem.

For nearly a year, the AMA has been educating physicians through two of its publications, AMNews and the Journal of the American Medical Association (JAMA). AMNews, which is a national news magazine widely distributed to physicians and medical students, has regularly featured articles over the last twelve months discussing the Y2K problem, patient safety concerns, reimbursement issues, Y2K legislation, and other related concerns. JAMA, one of the world's leading medical journals, will feature an article written by the Administrator of HCFA, explaining the importance for physicians to become Y2K compliant. The AMA, through these publications, hopes to raise the level of consciousness among physicians of the potential risks associated with the year 2000 for their practices and patients, and identify avenues for resolving some of the anticipated problems.

The AMA has also developed a national campaign entitled "Moving Medicine Into the New Millennium: Meeting the Year 2000 Challenge," which incorporates a variety of educational seminars, assessment surveys, promotional information, and ongoing communication activities designed to help physicians understand and address the numerous complex issues related to the Y2K problem. The AMA is currently conducting a series of surveys to measure the medical profession's state of readiness, assess where problems exist, and identify what resources would best reduce any risk. The AMA already has begun mailing the surveys, and we anticipate receiving responses in the near future. The information we obtain from this survey will enable us to identify which segments of the medical profession are most in need of assistance, and through additional timely surveys, to appropriately tailor our efforts to the specific needs of physicians and their patients. The information will also allow us to more effectively assist our constituent organizations in responding to the precise needs of other physicians across the country.

One of the many seminar series the AMA sponsors is the "Advanced Regional Response Seminars" program. We are holding these seminars in various regions of the country and providing specific, case-study information along with practical recommendations for the participants. The seminars also provide tips and recommendations for dealing with vendors and explain various methods for obtaining beneficial resource information. Seminar participants receive a Y2K solutions manual, entitled "The Year 2000 Problem: Guidelines for Protecting Your Patients and Practice." This seventy-five page manual, which is also available to hundreds of thousands of physicians across the country, offers a host of different solutions to Y2K problems that physicians will likely face. It raises physicians' awareness of the problem, year 2000 operational implications for physicians' practices, and identifies numerous resources to address the issue.

In addition, the AMA has opened a web site (URL: www.ama-assn.org) to provide the physician community additional assistance to better address the Y2K problem. The site serves as a central communications clearinghouse, providing up-to-date information about the millennium bug, as well as a special interactive section that permits physicians to post questions and recommended solutions for their specific Y2K problems. The site also incorporates links to other sites that provide additional resource information on the year 2000 problem.

On a related note, the AMA in early 1996 began forming the National Patient Safety Foundation or "NPSF." Our goal was to build a proactive initiative to prevent

[10] *Id.*
[11] *Id.* at p. 10.
[12] *Id.* at p. 13.
[13] *Id.*

avoidable injuries to patient in the health care system. In developing the NPSF, the AMA realized that physicians, acting alone, cannot always assure complete patient safety. In fact, the entire community of providers is accountable to our patients, and we all have a responsibility to work together to fashion a systems approach to identifying and managing risk. It was this realization that prompted the AMA to launch the NPSF as a separate organization, which in turn partnered with other health care organizations, health care leaders, research experts and consumer groups from throughout the health care sector.

One of these partnerships is the National Patient Safety Partnership (NPSP), which is a voluntary public-private partnership dedicated to reducing preventable adverse medical events and convened by the Department of Veterans Affairs. Other NPSP members include the American Hospital Association, the Joint Commission on Accreditation of Healthcare Organizations, the American Nurses Association, the Association of American Medical Colleges, the Institute for Healthcare Improvement, and the National Patient Safety Foundation at the AMA. The NPSP has made a concerted effort to increase awareness of the year 2000 hazards that patients relying on certain medical devices could face at the turn of the century.

RECOMMENDATIONS

As an initial step, we recommend that the Administration or Congress work closely with the AMA and other health care leaders to develop a uniform definition of "compliant" with regard to medical equipment. There needs to be clear and specific requirements that must be met before vendors are allowed to use the word "compliant" in association with their products. Because there is no current standard definition, it may mean different things to different vendors, leaving physicians with confusing, incorrect, or no data at all. Physicians should be able to spend their time caring for patients and not be required to spend their time trying to determine the year 2000 status of the numerous medical equipment vendors with whom they work.

We further suggest that both the public and private sectors encourage and facilitate health care practitioners in becoming more familiar with year 2000 issues and taking action to mitigate their risks. Greater efforts must be made in educating health care consumers about the issues concerning the year 2000, and how they can develop Y2K remediation plans, properly test their systems and devices, and accurately assess their exposure. We recognize and applaud the efforts of this Committee, the Congress, and the Administration in all of your efforts to draw attention to the Y2K problem and the medical community's concerns.

We also recommend that communities and institutions learn from other communities and institutions that have successfully and at least partially solved the problem. Federal, state and local agencies as well as accrediting bodies that routinely address public health issues and disaster preparedness are likely leaders in this area. At the physician level, this means that public health physicians, including those in the military, organized medical staff, and medical directors, will need to be actively involved for a number of reasons. State medical societies can help take a leadership role in coordinating such assessments.

We also must stress that medical device and software manufacturers need to publicly disclose year 2000 compliance information regarding products that are currently in use. Any delay in communicating this information may further jeopardize practitioners' efforts at ensuring compliance. A strategy needs to be developed to more effectively motivate all manufacturers to promptly provide compliance status reports. Additionally, all compliance information should be accurate, complete, sufficiently detailed and readily understandable to physicians. We suggest that the Congress and the federal government enlist the active participation of the FDA or other government agencies in mandating appropriate reporting procedures for vendors. We highly praise the Department of Veteran Affairs, the FDA, and others who maintain Y2K web sites on medical devices and offer other resources, which have already helped physicians to make initial assessments about their own equipment.

We are aware that the "Year 2000 Information and Readiness Disclosure Act" was passed and enacted into law last year, and is intended to provide protection against liability for certain communications regarding Y2K compliance Although the AMA strongly believes that information must be freely shared between manufacturers and consumers, we continue to caution against providing liability caps to manufacturers in exchange for the Y2K information they may provide, for several reasons. First, as we have stated, generally vendors alone have the information about whether their products were manufactured to comply with year 2000 data. These manufacturers should disclose that information to their consumers without receiving an undue benefit from a liability cap.

Second, manufacturers are not the only entities involved in providing medical device services, nor are they alone at risk if an untoward event occurs. When a product goes through the stream of commerce, several other parties may incur some responsibility for the proper functioning of that product, from equipment retailers to equipment maintenance companies. Each of these parties, including the end-user—the physician—will likely retain significant liability exposure if the device malfunctions because of a Y2K error. However, none of these parties will typically have had sufficient knowledge about the product to have prevented the Y2K error, except the device manufacturer. To limit the manufacturer's liability exposure under these circumstances flies in the face of sound public policy.

We also have to build redundancies and contingencies into the remediation efforts as part of the risk management process. Much attention has been focused on the vulnerability of medical devices to the Y2K bug, but the problem does not end there. Patient injuries can be caused as well by a hospital elevator that stops functioning properly. Or the failure of a heating/ventilation/air conditioning system. Or a power outage. The full panoply of systems that may break down as our perception of the scope of risk expands may not be as easily delineated as the potential problems with medical devices. Building in back-up systems as a fail-safe for these unknown or more diffuse risks is, therefore, absolutely crucial.

As a final point, we need to determine a strategy to notify patients in a responsible and professional way. If it is determined that certain medical devices may have a problem about which patients need to be notified, this needs to be anticipated and planned. Conversely, to the extent we can reassure patients that devices are compliant, this should be done. Registries for implantable devices or diagnosis-or procedure-coding databases may exist, for example, which could help identify patients who have received certain kinds of technologies that need to be upgraded and/or replaced or that are compliant. This information should be utilized as much as possible to help physicians identify patients and communicate with them.

As we approach the year 2000 and determine those segments of the medical industry which we are confident will weather the Y2K problem well, we will all need to reassure the public. We need to recognize that a significant remaining concern is the possibility that the public will overreact to potential Y2K-related problems. The pharmaceutical industry, for instance, is already anticipating extensive stockpiling of medications by individuals and health care facilities. In addition to continuing the remediation efforts, part of our challenge remains to reassure patients that medical treatment can be effectively and safely provided through the transition into the next millennium.

CONCLUSION

We appreciate the Committee's interest in addressing the problems posed by the year 2000, and particularly, those problems that relate to physicians. Because of the broad scope of the millennium problem and physicians' reliance on information technology, we realize that the medical community has significant exposure. The Y2K problem will affect patient care, practice administration, and Medicare/Medicaid reimbursement. The AMA, along with the Congress and other organizations, seeks to better educate the health care community about Y2K issues, and assist health care practitioners in remedying, or at least reducing the impact of, the problem. The public and private sectors must cooperate in these endeavors, while encouraging the dissemination of compliance information.

Chairman ARCHER. Thank you, Doctor.

Our next witness is Mr. Curtis Lord. And if you'll identify yourself for the record, you may proceed?

STATEMENT OF CURTIS LORD, CHIEF EXECUTIVE OFFICER, FIRST COAST SERVICE OPTIONS, BLUE CROSS AND BLUE SHIELD ASSOCIATION OF FLORIDA, ON BEHALF OF BLUE CROSS AND BLUE SHIELD ASSOCIATION

Mr. LORD. Thank you, Mr. Chairman and Members of the Committee, for the opportunity to testify today. I'm Curtis Lord, chief executive officer, First Coast Service Options, a subsidiary of Blue

Cross and Blue Shield of Florida. I'm here on behalf of the Blue Cross and Blue Shield Association.

For more than 30 years, Blue Cross and Blue Shield plans have partnered with the government to handle the day to day work of paying Medicare claims accurately and timely. We are extremely proud of our role as Medicare contractors and the impressive performance record we've achieved.

My testimony today focuses on three areas: our progress to assure that Y2K computer adjustments are made correctly and on time; why new contractor reforms are unwise; and the critical need for stable and adequate funding for all contractor operations.

First, Y2K readiness is a top priority for Medicare contractors. I'm pleased to report we are making excellent progress toward ensuring that our mission-critical Medicare payment systems are millennium ready. HCFA has reported that as of December 31, 1998, all 78 contractor systems were fully renovated and 54 had self-certified with acceptable qualifications. According to HCFA, the remaining contractors are on target to self-certify by March 31, 1999.

We are working closely with HCFA and our external vendors to make sure that all qualifications to our certifications are resolved during the first quarter of the year. Additionally, because Medicare systems are not static, we will continue testing during 1999 in order to re-certify their readiness by November the 1st.

Let me now describe for you the efforts my company has made to become Y2K ready. We began preparing for Y2K readiness in 1997 with the formation of a Y2K project team and the creation of a comprehensive Y2K readiness plan. In accordance with our plan, we inventoried software and hardware, reviewed our telecommunications environments, assessed and renovated codes, upgraded hardware to make it Y2K compliant and established a simulated production environment. We then ran test cases or test claims through the entire claims processing system to ensure that the system processes the claims with the same result both before and after the Y2K renovation. We tested over 12,000 claims using eight key dates that span from late December 1999 through March 1, 2000. Based on the results of these tests, we were able to certify that the mission-critical systems we maintain are Y2K compliant as of December 31, 1998.

This year we will continue all levels of testing and plan to test an additional 10,000 claims before re-certifying compliance to HCFA by November 1. This will include additional tests with providers who submit claims electronically to assure that they can submit bills to us and that we can receive them and provide remittance advice and payment.

And, importantly, although we don't expect failure, we are developing and will test extensive contingency plans designed to help us prepare for potential problems and restore normal service in the most timely and cost-effective manner.

Overall, we will involve hundreds of our staff and spend approximately $9.4 million ensuring our Medicare carrier and intermediary operations are Y2K ready.

Although there is still much to be done, significant and steady progress has been made. We are confident that Medicare contractors will be ready to pay claims properly on and beyond January

1, 2000. Our objective is to ensure that beneficiaries and providers continue to receive the excellent customer service they expect and deserve.

Second, HCFA is again proposing legislation to dramatically restructure the Medicare contracting process. This legislation would permit HCFA to fragment the functions of current contractors. Mr. Chairman, we do not believe this is a wise strategy for a number of reasons, not the least of which is that it could impede contractors' progress toward Y2K readiness. We believe the most effective manner to improve Medicare administration is to set appropriate performance standards for contractors, enforce them, and terminate the contracts of those not performing at the required levels.

The last point I would like to make is that stable and adequate funding is absolutely critical to achieve excellence in performance. While the additive MIP funding provided by this Committee in 1996 is helping us strengthen our efforts to fight fraud and abuse, funding for the larger majority of contractor operations remains subject to the annual appropriations process and the tight budget limits that apply to those funds. We believe that finding a reliable and stable funding source for all Medicare contractor operations is imperative and would like to work with both HCFA and this Committee to assure that the contractors receive the administrative resources necessary to manage Medicare effectively.

Thank you. I would be happy to answer any questions the Committee may have.

[The prepared statement follows:]

Statement of Curtis Lord, Chief Executive Officer, First Coast Service Options, Blue Cross and Blue Shield Association, of Florida, on behalf of Blue Cross and Blue Shield Association

Mr. Chairman and Members of the Committee, I am Curtis Lord, CEO of First Coast Service Options, a subsidiary of Blue Cross and Blue Shield of Florida. I am testifying on behalf of the Blue Cross and Blue Shield Association, the organization representing 52 independent Blue Cross and Blue Shield Plans throughout the nation who provide health coverage to over 70 million people.

I appreciate the opportunity to testify before you today to report on the excellent progress Blue Cross and Blue Shield Plans are making to assure Medicare systems will function properly in 2000.

The Medicare program is administered through a successful partnership between the private industry and the Health Care Financing Administration (HCFA). Since 1965, Blue Cross and Blue Shield Plans have played a leading role in administering the program. They have contracted with the federal government to handle much of the day-to-day work of paying Medicare claims accurately and in a timely manner.

Nationally, Blue Cross and Blue Shield Plans process over 90 percent of Medicare Part A claims and about 67 percent of all Part B claims. At BCBS of Florida, we process about 5 million Part A claims and 50 million Part B claims each year.

RESPONSIBILITIES OF MEDICARE CONTRACTORS

Medicare contractors have four major areas of responsibility:

1. Paying claims: Medicare contractors process all the bills for the traditional Medicare fee-for-service program. In FY 2000, it is estimated that contractors will process over 900 million claims, more than 3.5 million every working day.

2. Providing Beneficiary and Provider Customer Services: Contractors are the main point of routine contact with the Medicare program for both beneficiaries and providers. Contractors educate beneficiaries and providers about Medicare and respond to about 40 million inquiries annually.

3. Handling Appeals for Payment: Contractors handled more than 7 million hearings and appeals for reconsideration of initial payment determinations last year. In FY 2000, HCFA expects the cost of processing appeals and hearings to rise by ten percent.

4. Fighting Medicare Fraud, Waste and Abuse: Contractors saved $8 billion in 1997—yielding $17 in Medicare savings for every $1 invested from activities to review claims—by assuring services are medically necessary and by detecting possible fraud and abuse.

We are extremely proud of our role as Medicare contractors. Contractors are:

• Cost-effective—operating on administrative budgets that represent only 1 percent of Medicare benefit payments.

• Efficient—having a track record of quickly and accurately implementing major programmatic changes under extremely tight time frames; and

• On the first line of defense against fraud and abuse—aggressively fighting Medicare fraud and abuse with additional funding provided by this Committee in 1996 for the Medicare Integrity Program (MIP). BCBSA had long urged Congress to appropriate increased funding for these efforts. We are now seeing the positive impact of enhanced contractor efforts. Just this month, the HHS Inspector General reported a 45 percent reduction in Medicare overpayments since 1996.

My testimony today focuses on three areas:

I. Our progress to assure that Year 2000 computer adjustments are made correctly and on time;

II. Why new contractor reforms are unwise and could jeopardize our efforts to fight fraud and abuse; and

III. The critical need for stable and adequate funding for all contractor operations.

I. Progress on Efforts to Assure Year 2000 Readiness

Year 2000 readiness is a top priority for Medicare contractors. Medicare contractors are making excellent progress to ensure Medicare payment systems are renovated and tested for millennium readiness. HCFA has reported that, as of December 31, 1998, all 78 contractors' systems were fully renovated and 54 had self-certified with acceptable qualifications. According to HCFA, the remaining contractors are on target to self-certify by March 31, 1999. We are working closely with HCFA and with our external vendors to make sure that all qualifications are resolved.

While Plans have made significant progress, much remains to be done in 1999. Contractors are reporting to HCFA weekly on the resolution of any self-certification qualifications. Additionally, because Medicare systems are not static, contractors will continue testing during 1999 in order to recertify their readiness by November 1, 1999. The objective is to ensure that all Medicare systems will operate successfully in future years without exception. Toward this end, all Medicare systems must be completely renovated, tested, and implemented.

In addition to testing, contractors are focusing on contingency plans and the readiness preparation of the provider communities. Contingency plans, which will also be completed by March 31, 1999, are designed to ensure business continuance, minimize any disruptions, and expedite solutions of any Y2K associated problems that may arise. Based on HCFA guidance, contractors are developing contingency plans for a minimum of two possible situations: (1) a 150 to 200 percent increase in the submission of paper claims; and (2) a lack of access to the Medicare beneficiary eligibility database known as the common working file. To ensure their contingency plan's feasibility, contractors are developing their plans in conjunction with their Y2K testing to identify the areas that are most susceptible to Y2K errors. These contingency plans will be tested by June 30, 1999.

Provider readiness is a major issue for HCFA and for contractors. Last December, HCFA made available to all Medicare providers support materials intended to assist them in becoming Y2K ready. In addition, HCFA sent a letter to providers on January 12, 1999, advising them that they needed to become Y2K compliant. The letter included a sample Provider Y2K Readiness Checklist as well as the website addresses where information was available.

HCFA has asked contractors to work with providers to help them become Y2K compliant. Contractors have conducted numerous outreach efforts, including holding seminars and briefings on Y2K readiness, and mailing bulletins and newsletters to providers stressing the importance of becoming Y2K ready. To help providers become compliant, contractors supply Y2K compliant billing software to providers at their request free of charge. Contractors also are conducting systems tests with providers to ensure readiness.

Let me describe for you the efforts my company has made to become ready. We began planning for Y2K renovation in 1997 with the goal of paying or denying Medicare claims correctly on and after January 1, 2000. By December 31, 1998, we had inventoried software and hardware, reviewed the LAN and WAN environments, assessed millions of lines of code, renovated code, retired modules, upgraded hardware

to make it Y2K compliant, tested each module, and established a simulated production environment.

We then ran test cases—test claims—through the entire claims processing system to ensure that the system processes the claims, with the same result, both before and after the Y2K renovation. This is a full simulation of production. We want to be sure that all steps in the process are capable of supporting business after 2000. We tested over 12,000 claims using 8 different dates that spanned late December 1999 to early January 2000, and February 28 through March 1, 2000. Based on the results of these tests, we were able to certify Y2K compliance to HCFA as of December 31, 1998.

This year, we will continue all levels of testing, and plan to test an additional 10,000 claims and recertify compliance to HCFA by November 1. It is critically important that all changes from HCFA be completely tested. We will test with providers who submit bills electronically to assure that they can submit claims to us, and that we can receive them and provide remittance advice. And, importantly, although we don't expect failure, we are developing and testing contingency plans for all mission critical applications and business partners.

We have 25 people devoted full-time to the Y2K project. Dozens of additional people supported Y2K testing in 1998 on a part-time basis. These numbers will increase to hundreds of people as recertification testing and contingency planning testing and rehearsals reach intense levels in mid-1999.

BCBSA Efforts with HCFA to Ensure Y2K Readiness

BCBSA and Medicare contractors have been working closely with HCFA on readiness issues. Last year, BCBSA worked with HCFA to find an agreeable contract amendment related to Year 2000 compliance. Although there was some disagreement over the language of the contract amendment that HCFA originally sent us to sign, I would like to clarify that at no time did contractors refuse to become Y2K ready. BCBSA had several concerns with the amendment because it would have required contractors to assume liability for compliance of all vendors (e.g., financial institutions, facilities managers who control elevator programming, etc.) and face civil monetary penalties. HCFA acknowledged that it had drafted the amendment too broadly and agreed to work with contractors to rewrite the amendment.

In addition, BCBSA worked with HCFA to develop a formal process to assure regular communication on Y2K issues. In response to a BCBSA recommendation, HCFA established a steering committee chaired by HCFA's chief information officer and vice-chaired by BCBSA. I serve on this committee. The operation of the steering committee has facilitated very constructive and useful dialogue between contractors and HCFA about Year 2000 compliance.

The committee has met with the HCFA Administrator and meets monthly with many of the agency's key directors and other top management staff. HCFA credits its progress in meeting the Y2K challenge in large part due to the outstanding effort and commitment of HCFA staff and the contractors. We look forward to continuing these cooperative efforts with HCFA.

In reviewing the issues related to Year 2000 readiness, the committee should be aware of three additional issues that have made Year 2000 readiness activities challenging:

• Significant Change in Direction: Originally, many of the system changes that were necessary for readiness would have been accomplished by the conversion of all Medicare contractors to the Medicare Transaction System (MTS). As you know, the MTS initiative was terminated in 1997. As a result, contractors have been required to make significant changes that, in the absence of the MTS initiative, they would have been working on for a long time.

• Transition to New Standard Systems: Instead of converting to the MTS system, HCFA had directed contractors to transition to a single Part A and a single Part B system. In some cases, this conversion to different systems would have diluted experienced contractor and HCFA staff from focusing on critical millennium readiness activities. As a result, HCFA approved a request by several contractors to delay transition requirements so they could focus on Year 2000 issues.

• Numerous and Broad Programmatic Demands: HCFA already has said that it will not be able to implement all of the BBA requirements because of the need to concentrate on Year 2000 efforts. We continue to recommend to HCFA that as many non-Year 2000 system changes as possible should be removed from contractor workloads so that experienced technical resources can be devoted to assuring Year 2000 readiness.

This is even more critical now as we work on the testing and retesting phase of our readiness efforts. Every time a change in a system is introduced (e.g., a change in the Part A deductible, updated physician or hospital payment rates, etc.), each

contractor must retest their entire system to make sure the new changes are compatible with Y2K.

II. Contractor Reform is Not Necessary

HCFA's FY 2000 budget once again includes a legislative proposal to dramatically restructure the Medicare contracting process. This effort to make broad changes in contract authority is not a new initiative. For several years, HCFA has been seeking contractor reform legislation to give the agency broad authority to fragment the functions of current contractors. While we have not yet seen the details of this current proposal, our understanding is that it is similar to previous legislation.

We believe that contractor reform provisions are unwise and unnecessary for the following reasons:

1. It could jeopardize services to beneficiaries and providers: HCFA's proposal would eliminate the requirement that Medicare contractors have experience working with the Medicare program and would not even require that entities be familiar with health claims processing. Allowing HCFA to contract with organizations unfamiliar with Medicare's intricate payment methodologies could reduce payment accuracy, delay payments to providers, and reduce the quality of service providers and beneficiaries expect.

2. It could undermine HCFA's efforts to administer its other initiatives effectively: Potentially, HCFA would have to manage many new contractors for claims processing services with entities unfamiliar with Medicare. These new contracts would require strict management by HCFA at a time when HCFA has many other new responsibilities, including BBA and HIPAA. With these other large workloads, we believe the agency does not have the resources, staff, or expertise to implement this type of new procurement activity.

3. It is based on an untested Medicare Integrity Program: HCFA has just begun to implement the new contracting provisions for the Medicare Integrity Program (MIP). As of yet, no contracts have been awarded. Moreover, HCFA's strategy to split the MIP functions from the Program Management (PM) functions in Medicare is not yet tested. Due to the historical and functional integration of claims processing, customer service, and fraud and abuse activities, separating PM and MIP functions could jeopardize future fraud and abuse detection. PM and MIP are not autonomous services, and require constant coordination and communication in a rapidly changing Medicare program. Further authority for HCFA to significantly revise contracting relationships is premature.

I would also call your attention to the HHS Inspector General's recommendations in the CFO report. The IG is specifically concerned that instability of Medicare contractors could reduce the ability to fight Medicare fraud and abuse. Given the recent improvements in fighting fraud and the significant programmatic challenges ahead, it simply does not make sense to pursue an unnecessary restructuring of the program.

4. It would place Medicare contractors under legislative constraints that exceed other government contractors: For example, the legislation eliminates the requirement that HCFA pay termination costs to contractors that leave the Medicare program. This provision would make Medicare contracts different than any other type of government contract, including defense contracts. The Federal Acquisition Regulations (FAR) require that the government pay contractors reasonable termination costs. There is no basis to treat Medicare contractors differently.

5. HCFA's proposals could impede contractors' progress to become Y2K ready: At this point, HCFA's proposal would not improve the Year 2000 problem and, in fact, could make it much worse. Contractors unfamiliar with the Medicare program would have the added burden of having to learn its extremely complex rules and regulations while simultaneously working to achieve millennium readiness. Moreover, the testing requirements for contractor certification are extremely complex given the number of links contractors have with external systems (e.g., HCFA, banks, providers, etc.). It is highly unlikely that HCFA would be able to identify a new contractor that could meet the certification requirements.

Finally, contractor reform is unnecessary to ensure the quality of Medicare contractors. HCFA currently has the authority to replace or terminate contractors for poor performance.

HCFA has claimed this proposal would increase the cost effectiveness of contractor operations. However, this legislation has no positive effect on the budget. It does not reduce expenditures for Medicare contractors. More importantly, inexperienced contractors may be more apt to make improper payments, which could further threaten the solvency of the trust funds.

Success in Medicare claims administration requires that HCFA and the contractors work together toward their mutual goal of accurate and timely claims payment. This partnership should extend to planning the future of Medicare contract administration. We believe the most effective manner to proceed in strengthening Medicare administration is to raise performance standards, aggressively enforce them, and terminate the contracts of those not performing at the required level.

III. Stable and Adequate Funding is Critical

As Medicare's first line of defense against fraud and abuse, Medicare contractors require adequate funding in order to meet the demands of the program and to effectively combat fraud and abuse.

The President's FY 2000 budget proposes $1.27 billion for Medicare contractors, virtually the same funding level as 1999. Given the following, this budget represents a cut to contractor funding compared to FY 1999:

1. User Fees: Of the $1.27 billion proposed for contractors, $93 million is dependent on proposed new user fees from providers, which have previously been rejected by this Committee. Failure to authorize the user fee could mean a $93 million cut for contractors.

2. Y2K: The President's budget does request $150 million in addition to the $1.27 billion for HCFA millennium readiness. It is unclear, at this point, whether or how much of these proposed funds would be made available for Medicare contractors' Y2K needs.

3. BBA and HIPAA: Additional funds will be needed to cover a significantly greater workload next year, including:

- Implementing BBA provisions, including new prospective payment systems for inpatient rehabilitation facilities and outpatient hospital care.
- Implementing HIPAA administrative simplification provisions, including the national payer identifier initiative and the development of transaction and security standards for electronic processing of claims.

Adequate funding also is critical to maintain anti-fraud efforts and to prevent further service reductions to beneficiaries and providers. An independent study commissioned by BCBSA last year indicates that contractor funding will be significantly strained by the increased anti-fraud and abuse detection efforts under the newly enacted MIP. The report shows that every 10 percent increase in MIP funding will result in a $13 million increase in contractor costs due to increased appeals, inquiries, and hearings.

Additionally, a letter published in a recent Health Affairs journal, signed by 14 health policy experts, stressed the need for more Medicare administrative funding. Specifically, the letter stated that "HCFA's ability to provide assistance to beneficiaries, monitor the quality of provider services, and protect against fraud and abuse has been increasingly compromised by the failure to provide the agency with adequate administrative resources."

We believe that finding a reliable and stable funding source for Medicare contractors is critical. In the President's budget, HCFA indicated a willingness to explore alternative funding options for Medicare administrative activities. We support HCFA's efforts and would like to work with HCFA and Congress to move toward a stable and reliable funding source.

Conclusion

Let me reiterate that Medicare contractors are working diligently to become millennium ready. This is a monumental task, and we will face a number of challenges as we complete it. Medicare contractors are committed to meeting these challenges just as they have done in the past.

Congress should reject HCFA's request to legislate far-reaching changes to the Medicare contractor program. Contractor reform raises fundamental issues and implications for the Medicare program. In fact, contractor reform would introduce change, confusion, and diversion of resources at a time when experience and focus is important. Alternatively, HCFA should tell contractors exactly what standards they want contractors to meet. Let contractors meet these standards; otherwise, HCFA can terminate our contracts.

Finally, given the importance of Medicare to its beneficiaries, providers, and the nations' economy, it is critical that the administrative resources necessary to manage the program effectively be provided.

Chairman ARCHER. Thank you, Mr. Lord.

Ms. Archer, if you'll identify yourself for the record, you may proceed?

STATEMENT OF DIANE ARCHER, EXECUTIVE DIRECTOR, MEDICARE RIGHTS CENTER, NEW YORK, NEW YORK

Ms. DIANE ARCHER. My name is Diane Archer. I'm the executive director of the Medicare Rights Center, a national not-for-profit organization based in New York. The Medicare Rights Center helps seniors and people with disabilities on Medicare through telephone counseling, public education, and public policy work. I thank you for this opportunity to testify today.

We recognize that the U.S. Government and corporate America are taking Y2K issues seriously, and we hope their efforts will result in a smooth transition to the year 2000 for everyone on Medicare. But we do have concerns that people on Medicare could face serious healthcare access problems.

First, at the Federal level, our foremost concern is healthcare access for the 6.6 million seniors and people with disabilities in Medicare HMOs. HCFA is working hard to ensure that its own systems are Y2K compliant. But HCFA cannot guarantee that Medicare HMOs will be Y2K compliant. As you know, unlike original Medicare, most HMOs require prior authorization for specialty care. Unless the Medicare HMOs are Y2K compliant, we could see a significant increase in the number of people on Medicare who because of system failures can't get authorization for the care they need with potentially devastating consequences.

Consider this potential scenario: it is February 2000 and a Medicare HMO enrollee goes to the hospital with stomach pains. The doctor calls the HMO requesting approval to perform a Medicare-covered procedure to alleviate the pain. The HMO doesn't have the systems in place to find the patient's name on its database or can't use the computer to determine whether the service is covered and therefore doesn't give authorization. As a result, the woman does not get the care she needs.

We are concerned about how HCFA protects people in Medicare HMOs when they can't get care because of Y2K system failures and how it holds these HMOs accountable. What tools does HCFA have at its disposal to ensure that HMOs provide people on Medicare with the care they need?

HCFA has taken a strong first step in requiring all of its contractors to submit Y2K compliance forms. But, as you know, these statements are not admissible in a court of law.

We also wonder what advice we should be giving our clients about joining a Medicare HMO or other Medicare private health plan in November 1999 to begin on January 1, 2000. Should we advise people to secure an affidavit of Y2K compliance from their HMOs that's legally admissible in a court of law or should we recommend that they withdraw from their Medicare HMOs for the 3 month period between December 1999 and February 2000 if they wish to avoid the risk of not getting the care they need because of

HMO system failures? If not, we wonder how seniors and people with disabilities can protect themselves?

We recommend that HCFA set up a special hotline for people to call if they're denied access to care because of Y2K problems. We also urge that some mention of Y2K access to care issues be included in the Medicare and You handbook.

But the Y2K issue brings to the surface the Federal Government's limited ability to ensure that people on Medicare get the healthcare they need from the private health plans that contract with HCFA.

At the State level, we're concerned that system failures caused by inadequate preparation for Y2K on the part of local Medicaid and Social Security offices will slow down or undermine the application process for programs that pay Medicare premiums and coinsurance for people with low-incomes. HCFA should institute a system to ensure that the Social Security Administration does not wrongly drop these people from Medicare because of Y2K system failures at State Medicaid offices.

Finally, at the individual level, it's critical that those people on Medicare who rely on prescription drugs and computer chip driven medical equipment keep getting the medicine and equipment they need without interruption when the year 2000 begins. We recommend that HCFA should sponsor a series of public service announcements telling people on Medicare, their friends and family members that they should speak with their doctors and pharmacies to ensure availability of their prescription during the transition to the year 2000. And that if they use a medical device, they should check with their doctor or supplier in advance to make sure that the equipment is Y2K compliant.

It's our job as professionals who work closely with seniors and people with disabilities on Medicare to educate our clients on how to get the care they need when they need it. We hope that Congress and HCFA will do whatever possible to make sure that people on Medicare keep getting the care they need in the new millennium.

Thank you. I'll be happy to answer questions.

[The prepared statement follows:]

Statement of Diane Archer, Executive Director, Medicare Rights Center, New York, New York

My name is Diane Archer. I am the Executive Director of the Medicare Rights Center, a national not-for-profit organization based in New York City. MRC helps seniors and people with disabilities on Medicare through telephone counseling, public education, and public policy work. MRC, under a contract with the New York State Office for the Aging, with funding from the Health Care Financing Administration, operates a telephone hotline. Each year, we field approximately 50,000 hotline calls from people with Medicare questions and problems and provide direct assistance on a variety of Medicare issues to more than 7,000 individual callers. I thank the Committee on Ways and Means for this opportunity to testify on how the transition to the year 2000 may affect people on Medicare.

We recognize that the United States government and corporate America are taking Y2K issues seriously, and we hope their efforts will result in a smooth transition to the year 2000 for everyone on Medicare. Otherwise, people on Medicare could face serious health care access problems. Today, I am going to talk about some access to care problems that could arise.

First, at the federal level, our foremost concern is health care access for the more than 6 million seniors and people with disabilities in Medicare HMOs. We applaud HCFA's efforts to ensure that its own systems are Y2K-compliant. But HCFA can-

not guarantee that Medicare HMOs will be Y2K-compliant. As you know, most HMOs require prior authorization for specialty care. Unless the Medicare HMOs are Y2K-compliant, we could see a significant increase in the number of people on Medicare who, because of system failures, can't get authorization for the care they need, with potentially devastating consequences.

Consider this potential scenario: it is February 2000 and a Medicare HMO enrollee goes to the hospital with stomach pains. The doctor calls the HMO requesting approval to perform a Medicare-covered procedure to alleviate her pain. The HMO does not have the systems in place to find the patient's name on its database or can't use the computer to determine whether the service is covered and therefore does not give authorization. As a result, the woman does not get the care she needs.

We wonder what advice we should be giving our clients about joining a Medicare HMO or other Medicare private health plan in November 1999 to begin enrollment on January 1, 2000. Should we advise people to secure an affidavit of Y2K-compliance from their HMOs that is legally admissible in a court of law? Or, should we recommend that they withdraw from their Medicare HMOs for the three-month period between December 1999 and February 2000 if they wish to avoid the risk of not getting the care they need because of HMO system failures? If not, we wonder how seniors and people with disabilities can protect themselves. We strongly recommend that HCFA set up a special hotline for people to call if they are denied access to care because of Y2K problems. We also urge that some mention of Y2K access to care issues be included in the Medicare & You handbook.

We are concerned about how HCFA protects people in Medicare HMOs when they cannot get care because of Y2K system failures, and how it holds these HMOs accountable. What tools does HCFA have at its disposal to ensure that HMOs provide people on Medicare with the care they need?

HCFA has taken a strong first step in requiring all of its contractors to submit Y2K compliance forms. But, as you know, these statements are not admissible in a court of law. And in the past HCFA has lacked the staff and resources to properly oversee its contracting agents.[1] The Y2K issue brings to the surface the federal government's limited ability to ensure that people on Medicare get the health care they need from the private health plans that contract with HCFA.

Second, at the state level, we are concerned that system failures caused by inadequate preparation for Y2K on the part of local Medicaid and Social Security offices will slow down or undermine the application process for QMB, SLMB, QI–1 and QI–2. These programs help many low-income people on Medicare pay for their health care coverage. The application process is already slow and difficult in many states, and system failures could prevent even more people from getting these benefits and the care and coverage they need and are due. HCFA should institute a system to ensure that the Social Security Administration does not drop dually-eligible people from Medicare because of Y2K system failures at state Medicaid offices.

Finally, at the individual level, it is critical that those seniors and people with disabilities on Medicare who rely on prescription drugs and computer-chip driven medical equipment keep getting the medicine and equipment they need without interruption when the year 2000 begins. Although overseeing this continuity of care is outside of HCFA's legal jurisdiction, HCFA has an important role in educating people on Medicare on what they need to do to ensure that the transition to Y2K goes smoothly for them. We believe that HCFA should sponsor a series of public service announcements telling people on Medicare, their friends, and family members that: one—they need to check with their doctors and pharmacy to ensure availability of their prescriptions during the transition to the year 2000, and two—if they use a medical device, then they should check with their doctor or supplier in advance to make sure that the equipment is Y2K-compliant.

People on Medicare have already lived through many changes and hardships. Most do not own a computer. They are probably not overly concerned with the ability of computer systems to transition smoothly into the year 2000. We do not want to instill fear in people on Medicare. It is our job, as professionals who work closely with seniors and people with disabilities on Medicare, to educate our clients on how to get the care they need when they need it. We are telling our clients to ask their doctors, pharmacists, and medical suppliers if they are Y2K-compliant. We hope that Congress and HCFA will do whatever possible to make sure that people on Medicare keep getting the care they need in the new millenium. Thank you.

---

[1] An Office of Inspector General report finds that HCFA has neither the staff nor resources to oversee Medicare HMOs. Department of Health and Human Services, Office of Inspector General, April 1998, Report Numbers: OEI–01–96–00190 and OEI–01–96–00191.

Chairman ARCHER. Our next and last witness of the day is Joel Willemssen. Welcome back again. And if you'll officially identify yourself for the record, you may proceed?

STATEMENT OF JOEL C. WILLEMSSEN, DIRECTOR, CIVIL AGENCIES INFORMATION SYSTEMS, ACCOUNTING AND INFORMATION MANAGEMENT DIVISION, U.S. GENERAL ACCOUNTING OFFICE

Mr. WILLEMSSEN. Yes, sir, Mr. Chairman. Joel Willemssen with the General Accounting Office. Thank you. And as requested, I'll briefly summarize our statement on Medicare Y2K and then very briefly on the overall readiness of the healthcare sector.

Regarding Medicare Y2K, we originally reported our concerns with this nearly 2 years ago. At that time, the level of HCFA management attention focused on Y2K was minimal. Instead much of the agency's systems focus was on a failed effort, known as the Medicare Transaction System, which was intended to replace existing part A and part B core computing systems. As we've previously testified, this effort was terminated after about $80 million had been spent and not one line of software had been delivered. It's important to keep that history in mind as we look at the huge challenge HCFA is now up against.

We reported last fall that with its late start on Y2K, HCFA faced the prospect of having too much to do in too little time. Many of the basic Y2K management practices that should have been in place were not. Our conclusions and recommendations to the administrator reflected our concern about the high level of risks facing HCFA. HCFA has been very responsive to our recommendations. And the administrator is to be commended for making Y2K the agency's top priority and directing a number of actions to more effectively manage this project.

Among these many actions has been an important commitment to develop business continuity and contingency plans to help ensure that no matter what beneficiaries will receive care and providers will be paid.

Despite that progress, we still have serious concerns with HCFA and Medicare Y2K. First, HCFA's reported external systems progress on Y2K has been highly overstated. HCFA and HHS recently reported that 54 of 78 contractor systems were compliant as of December 31. In fact, none of these 54 should have been reported as compliant. All of them had important exceptions, some of them very significant. Such qualifications included a major system failing to recognize 00 as a year as well as 2000 as a leap year.

According to HCFA officials, they reported these systems as compliant because the qualifications were minor problems that should not take much time to address. This is at variance with HCFA's independent verification and validation contractors' interpretation. The contractor found the qualifications to be critical, most requiring a major to moderate level of effort to resolve.

Among the other issues that HCFA needs to address: One, HCFA still needs an integrated schedule that identifies a critical path of all the key tasks it needs to complete. Two, it lacks a risk manage-

ment process. Three, HCFA still has thousands of data exchanges that must be renovated and tested. Four, and maybe most importantly, HCFA faces a huge amount of testing in 1999. First, changes to resolve the existing qualifications will need to be re-tested. Second, testing must still take place with full production level software. Third, there are other changes that will be going into effect, from mandated changes that will also have to be re-tested.

And all of this testing will ultimately determine whether HCFA's mission-critical systems are, indeed, going to be year 2000 compliant. But given the magnitude of the challenge ahead, it's absolutely critical that the administrator sustain her commitment to complete and test business continuity and contingency plans so that even if system failures occur, HCFA will be positioned with back-up plans.

Beyond Medicare, and just very briefly looking at the broader healthcare sector, there is reason for concern about Y2K readiness, not because of what we know, but because of what we don't know. The extent of information available on the readiness of the healthcare sector is generally very limited. In recent months there has been some good progress made, especially in the biomedical equipment area. But more will need to be done in the limited time remaining.

That concludes the summary of my statement. I would be pleased to address any questions you might have.

[The prepared statement follows:]

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

Mr. Chairman and Members of the Committee: We appreciate the opportunity to join in today's hearing and share information on the readiness of automated systems that support the nation's delivery of health benefits and services to function reliably without interruption through the turn of the century. This includes the ability of Medicare to provide accurate benefits and services to millions of Americans and the overall readiness of the health care sector, including such key elements as biomedical equipment used in the delivery of health services. Successful Year 2000—or Y2K—conversion is critical to these efforts.

In a report issued last year, we concluded that the progress made by the Department of Health and Human Services' (HHS) Health Care Financing Administration (HCFA)—and its contractors—in making its computers that process Medicare claims Year 2000 compliant was severely behind schedule in areas including repair, testing, and implementation.[1] Further, we made numerous recommendations to improve key HCFA management practices which we found to be lacking or inadequate. This morning I would like to briefly discuss our findings from that report and our suggestions for strengthening HCFA's Y2K activities, describe actions taken on those recommendations, and provide our perspective on where HCFA stands today.

Beyond Medicare, the level of information on a national level concerning Year 2000 compliance throughout the health care sector—including providers, insurers, manufacturers, and suppliers—is limited. As we reported last fall, this was true of biomedical equipment routinely used in the delivery of health care.[2] Such equipment includes medical devices such as cardiac defibrillators and monitoring systems that can record, process, analyze, display, and/or transmit data. Today, I would like to share information in this area with you as well.

---

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

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

HCFA'S ABILITY TO PROCESS MEDICARE CLAIMS INTO THE NEXT CENTURY

As the nation's largest health care insurer, Medicare expects to process over a billion claims and pay $288 billion in benefits annually by 2000. The consequences, then, of its systems' not being Year 2000 compliant could be enormous. We originally highlighted this concern in May 1997, making several recommendations for improvement.[3] In our report of last September we warned that although HCFA had made improvements in its Year 2000 management, serious challenges remained to be resolved in a short period of time. Specifically, we reported that less than a third of Medicare's mission-critical systems had been fully renovated, and none had been validated or implemented. Further, in terms of the agency's key management practices necessary to adequately direct and monitor its Year 2000 project, HCFA had not:

- developed an overall schedule and critical path to identify and rank Y2K tasks to help ensure that they could be completed in a timely manner;
- implemented risk management processes necessary to highlight potential technical and managerial weaknesses that could impair project success;
- planned for or scheduled end-to-end testing to ensure that program-wide renovations would work as planned; or
- effectively managed its electronic data exchanges, thereby increasing the risk that Y2K errors would be transferred through data exchanges from one organization's computer systems to those of another.

The Office of Management and Budget (OMB) also had concerns. In its December 8, 1998, summary of Year 2000 progress reports of all agencies for the reporting quarter ending November 13, 1998, it concluded that while HCFA had made significant progress in renovating its internal and external systems, the agency remained a serious concern due to the remediation schedule of its external systems. OMB further stated that Medicare contractors would have to make an intensive, sustained effort to complete validation and implementation of their mission-critical systems by the governmentwide goal of March 31, 1999. OMB designated HHS as a tier 1 agency on its three-tiered rating scale since it had made insufficient progress in addressing the Year 2000 problem.

Our conclusions and recommendations to the HCFA Administrator reflected our concerns about the high level of risk and large number of tasks still facing HCFA. We reported that it was more critical than ever that HCFA have sound business continuity and contingency plans in place that can be implemented should systems failures occur. Our specific recommendations included that HCFA:

- rank its remaining Year 2000 work on the basis of an integrated project schedule and ensure that all critical tasks are prioritized and completed in time to prevent unnecessary delays,
- develop a risk management process,
- define the scope of an end-to-end test of the claims process and develop plans and a schedule for conducting such a test,
- ensure that all external and internal systems' data exchanges have been identified and agreements signed among exchange partners, and
- accelerate the development of business continuity and contingency plans.

HCFA'S ACTIONS TO ACHIEVE COMPLIANCE

HCFA has been responsive to our recommendations, and its top management is actively engaged in its Year 2000 program. HCFA's Administrator has made Year 2000 compliance the agency's top priority and has directed a number of actions to more effectively manage this project. For example, HCFA has established a "war room" for real-time monitoring of Year 2000 renovation, testing, and implementation activities. In addition, the agency established seven contractor oversight teams to monitor progress. HCFA also strengthened its outreach efforts: on January 12, 1999, the Administrator sent individual letters to each of the 1.25 million Medicare providers in the United States, alerting them to take prompt Year 2000 action on their information and billing systems. Three days later the Administrator sent a letter to Congress, with assurances that HCFA is making progress and stressing that physicians, hospitals, and other providers must also meet the Y2K challenge. HCFA also offered to provide speakers in local congressional districts.

To more effectively identify and manage risks, HCFA is relying on multiple sources of information, including test reports, reports from its independent validation and verification (IV&V) contractors, and weekly status reports from its recently

---

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

established contractor oversight teams. In addition, HCFA has stationed staff at critical contractor sites to assess the data being reported to them and to identify problems.

HCFA is also more effectively managing its electronic data exchanges. HCFA now reports having a complete data exchange inventory of nearly 8,000 internal exchanges and over 255,000 external data exchanges. HCFA also issued instructions to its contractors (carriers and fiscal intermediaries) to inform providers and suppliers that they must submit Medicare claims in Year 2000-compliant data exchange format by April 5 of this year. The status of each of these data exchanges is being tracked by HCFA staff.

HCFA has also more clearly defined its testing procedures. It published additional testing guidance in November 1998 that provided a policy for external systems that requires multiple levels of testing for each system, including:

• *Unit level testing*: testing of the individual software component using test cases that exercise all component functionality. For the standard claims processing system, this includes full functional testing of claims processing policy and program integrity edits.

• *Simulated future date testing*: testing of the individual software component using tools to simulate that the date has been rolled forward.

• *Compliance testing*: testing in a fully Year 2000-compliant environment with real future dates to verify that the system is Year 2000 compliant.

HCFA also plans to perform end-to-end testing with its Year 2000-compliant test sites. These end-to-end tests are to include all internal systems and contractor systems; however, they will not include testing with banks and providers. Finally, HCFA has begun to use a Year 2000 analysis tool to measure testing thoroughness, and its IV&V contractor is assessing test adequacy on the external systems (e.g., test coverage and documentation).

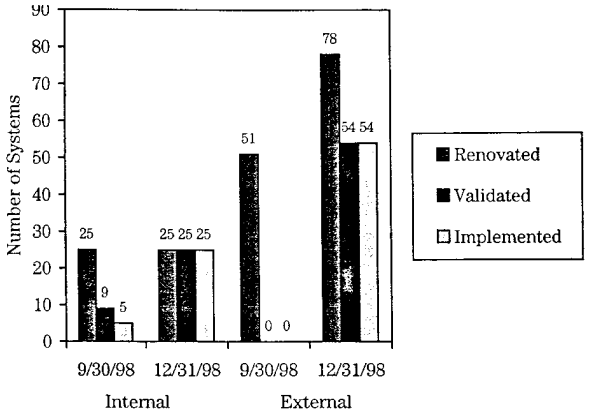
The final area in which HCFA has demonstrated progress is developing business continuity and contingency plans to ensure that, no matter what, beneficiaries will receive care and providers will be paid. HCFA has established cross-organizational workgroups to develop contingency plans for the following core business functions: health plan and provider payment, eligibility and enrollment issues, program integrity, managed care, quality of care, litigation, and telecommunications. HCFA's draft plans document its business impact analysis; the contingency plans are expected to be completed by March 31 of this year, and testing of the plans by June 30.

REPORTED STATUS OF HCFA'S MISSION-CRITICAL SYSTEMS

HCFA operates and maintains 25 internal mission-critical systems; it also relies on 78 external mission-critical systems operated by contractors throughout the country to process Medicare claims. These external systems include six standard processing systems and the "Common Working File." Each contractor relies on one of these standard systems to process its claims, and adds its own front-end and back-end processing systems. The Common Working File is a set of databases located at nine sites that works with internal and external systems to authorize claims payments and determine beneficiary eligibility.

HCFA's reporting of its readiness for next January sounds quite positive as stated in the most recent HHS Y2K quarterly progress report to OMB. According to this report, dated February 10, as of December 31, 1998, all 25 of HCFA's internal mission-critical systems were reported to be compliant, as were 54 of the 78 external systems. Figure 1 shows HCFA's reported status, compared with what it reported on September 30, 1998.

Figure 1: Reported Status of HCFA's Mission-Critical Systems



Source: HCFA quarterly reports to HHS

REPORTED PROGRESS IS HIGHLY OVERSTATED

HCFA's reported progress on its external mission-critical systems is considerably overstated. In fact, none of the 54 systems reported compliant by HCFA was Year 2000 ready as of December 31, 1998. All 54 external systems that were reported as compliant have important associated qualifications (exceptions), some of them very significant. Such qualifications included a major standard system that failed to recognize "00" as a valid year, as well as 2000 as a leap year; it also included systems that were not fully future date tested.

According to HCFA officials, they reported these systems as compliant because these qualifications were "minor problems" that should not take much time to address. This is at variance with the IV&V contractor's interpretation. More specifically, the IV&V contractor found that the qualifications reported by all systems contractors were critical, most requiring a major to moderate level of effort to resolve.

A specific example of a system reported as compliant with qualifications is the Florida standard system, used by 29 contractors. This system had one qualification that consisted of 22 test failures. The IV&V contractor characterized this failure experience as significant. HCFA reports that these failures were corrected with a January 29, 1999, software release. However, in a February 16, 1999, IV&V status report, Blue Cross of California—a user of the Florida standard system—found that date test problems remained. In another example, the EDS MCS standard system that is used by 10 contractors had 25 qualifications; these included 9 problems that were not future date tested. HCFA now reports that future date testing of the January software release of the EDS MCS system is 92 percent complete.

As these examples illustrate, these systems are not yet Year 2000 compliant, and the 39 contractors that use these two standard systems likewise cannot be considered compliant. Further, according to the IV&V contractor, two critical qualifications associated with each of the standard systems affect all external contractor systems: (1) HCFA-supplied systems that contractors use in claims processing were delivered too late to them for required testing to be performed; and (2) the claims processing data centers' hardware, software, and telecommunications were not completely compliant.

The IV&V contractor acknowledges that Medicare claims processing systems have made progress toward Year 2000 compliance over the past year, yet the various qualifications inevitably mean that some renovation and a significant amount of retesting still needs to be accomplished before these systems can be considered compliant. To HCFA's credit, it issued a memorandum in early January requesting Medicare carriers and fiscal intermediaries to resolve these qualifications by March 31, the federal target date for Year 2000 compliance. The notice stated that Medicare systems with unresolved Y2K problems affecting claims processing functions must be corrected, tested, and installed in production. As part of our ongoing work for the Senate Special Committee on Aging, we will be monitoring the resolution of these qualifications closely.

OTHER CRITICAL RISKS/CHALLENGES THAT REMAIN

The February 16, 1999, report of HCFA's IV&V contractor stated that an integrated schedule that tracks all major internal system activities needs to be established. It added that system-specific information—including time, test scheduling, and resource considerations—needs to be more fully developed in order to achieve a robust, trackable schedule. We agree. In fact, this is consistent with our previous recommendation that remaining Y2K work be ranked on the basis of a schedule that includes milestones for renovation and testing of all systems, and that it include time for end-to-end testing and development and testing of business continuity and contingency plans.[4] Such a schedule is even more important for the external systems because of their greater number, complexity, and interdependencies. HCFA still lacks an integrated schedule that identifies a critical path. Without this, it will be difficult for HCFA management to identify important dependencies in this complex environment and to prioritize its remaining work in the time that remains.

HCFA also lacks a formal risk management process—something to identify all risks and their interdependencies, assess their impact, establish time frames for mitigation and criteria for successful mitigation, and ensure that the criteria are followed. The one system that was intended to serve as its comprehensive risk management system does not contain current information, according to the IV&V contractor.

HCFA's systems—both internal and external—exchange data, both among themselves and with the CWF, other federal agencies, banks, and providers. Accordingly, it is important that HCFA ensure that Y2K-related errors will not be introduced into the Medicare program through these data exchanges. As of February 10, 1999, HCFA reported that over 6,000 of its 7,968 internal data exchanges were still not compliant, and that over 37,000 of its nearly 255,000 external data exchanges were not compliant.[5] To ensure that HCFA's internal and external systems are capable of exchanging data between themselves as well as with other federal agencies, banks, and providers, it is essential that HCFA take steps to resolve the remaining noncompliance of these data exchanges.

In yet another critical area, HCFA faces a significant amount of testing in 1999, since changes will continue to be made to its mission-critical systems to make them compliant. First, changes to resolve the existing qualifications will need to be retested. Second, testing must still take place with full production-level software. For example, the final software release of the Common Working File before 2000 is scheduled for late June; testing will therefore be needed after that. Third, legislatively mandated changes to software that will occur through June will need to be retested as well. HCFA plans to conduct these final tests of its systems between July 1 and November 1, 1999, then recertify all mission-critical systems as compliant without qualification or exception. These final tests will ultimately determine whether HCFA's mission-critical systems are indeed Year 2000 compliant. The late 1999 time frames associated with this testing represent a high degree of risk.

In addition to such individual systems testing, HCFA must also test its systems end-to-end to verify that defined sets of interrelated systems, which collectively support an organizational core business function, will work as intended. As mentioned, HCFA plans to perform this end-to-end testing with its Year 2000 test sites. These tests are to include all internal systems and contractor systems, but will not include testing with banks and providers. HCFA has instructed its contractors that it is their responsibility to test with providers and financial institutions. Even excluding banks and providers, end-to-end testing of HCFA's internal and external systems is a massive undertaking that will need to be effectively planned and carried out. HCFA has not yet, however, developed a detailed end-to-end test plan that explains how these tests will be conducted or that provides a detailed schedule for conducting them.

A final aspect of testing concerns the independent testing contractor. The IV&V contractor's recent assessment of the independent testing contractor concluded that its strategy as currently stated "is high risk for providing effective independent testing" because of the limited number of internal systems to actually be independently tested: 8. This number was previously 22. Further, this testing will not be completed until August. The limited number of systems tested and the late completion date are not reassuring.

---

[4] GAO/AIMD–98–284, September 28, 1998.

[5] On February 23, 1999, the HCFA Administrator stated that she wanted us to note that the February 10, 1999, HHS quarterly report to OMB had a typographical error, and that the total number of internal data exchanges is 3,418 and that 309 of these are still not compliant.

Given the magnitude of HCFA's Year 2000 problem and the many challenges that continue to face it, the development of contingency plans to ensure continuity of critical operations and business processes is absolutely critical. Therefore, HCFA must sustain its efforts to complete and test its agencywide business continuity and contingency plans by June 30. Another challenge for HCFA is monitoring the progress of the 62 separate business continuity and contingency plans that will be submitted by its contractors. We will continue to monitor progress in this area.

Other issues that further complicate HCFA's Year 2000 challenge are the known and unknown contractor transitions that are to take place before January 1, 2000, and the unknown status of the managed care organizations serving Medicare beneficiaries. As reported in HHS' quarterly submission to OMB, HCFA is concerned about the possibility of Medicare contractors, fiscal intermediaries, and carriers leaving the program and notifying HCFA after June 1999. If this were to occur, the workload would have to be transferred to another contractor whose Year 2000 compliance status may not be known. According to both contractor and HCFA officials, it requires 6–12 months to transfer the claims processing workload from one contractor to another. At present, HCFA must transition the work of three carriers that are leaving the program.

HCFA is requiring the 386 managed care organizations currently serving 6.6 million Medicare beneficiaries to certify their systems as Year 2000 compliant by this April 15. These certifications may be qualified, just as with the fee-for-service contractors. If this were to occur, a formal recertification would have to be performed later this year. Until this initial certification is performed, it will remain unknown whether the managed care organizations' systems are year 2000 compliant.

To summarize HCFA's situation, the agency and its contractors have made progress in addressing issues that we have raised. However, their reported progress vastly overstates the facts. Some renovation and a significant amount of testing must still be performed this year. Until HCFA completes its planned recertification between July and November 1999, the final status of the agency's Year 2000 compliance will be unknown. Given the considerable amount of remaining work that HCFA faces, it is crucial that development and testing of HCFA's business continuity and contingency plans move forward rapidly if we are to avoid the interruption of Medicare claims processing next year.

Y2K Readiness of the Health Care Sector: Information is Limited

At this point, I would like to broaden our discussion to the Year 2000-readiness status of the health care sector, including biomedical equipment used in the delivery of health care. While it is undeniably important that Medicare systems be compliant so that the claims of health care providers and beneficiaries can be paid, it is also critical that the services and products associated with health care delivery itself be Year 2000 compliant. However, the level of information currently available on such compliance is not reassuring.

Virtually everything in today's hospital is automated—from the scheduling of procedures such as surgery, to the ordering of medication such as insulin for a diabetic patient, to the use of portable devices as diverse as heart defibrillators and thermometers. It therefore becomes increasingly important for health care providers such as doctors and hospitals to assess their health information systems, facility systems (such as heating, ventilation, and air conditioning), and biomedical equipment to ensure their continued operation at the turn of the century. Similarly, pharmaceutical manufacturers and suppliers that rely heavily on computer systems for the manufacturing and distribution of drugs must assess their processes for compliance. Given the large degree of interdependence among components of the health sector—providers, suppliers, insurance carriers, and patients/consumers—the availability and sharing of Y2K readiness information is vital to safe, efficient, and effective health care delivery.

Readiness information is limited throughout the health care sector. Specifically, the amount of data available to consumers on the Y2K readiness of health care providers, private insurers, and pharmaceutical manufacturers and suppliers is scant. This past June, for example, the American Hospital Association sent a Y2K readiness survey to about 4,700 hospitals. However, only about 17 percent of its members responded.

In May 1998, the President's Council on Year 2000 Conversion established a Health Care Working Group[6] chaired by HCFA to conduct outreach activities of the

[6] Members include federal health care agencies and professional health care associations such as the American Ambulance Association, American Hospital Association, American Medical Association, Health Industry Manufacturers Association, Joint Commission on the Accreditation of

Continued

health care sector. In response to an October 1998 request from the Chair of the President's Council to gauge the Year 2000 readiness of the health sector, several professional health care associations surveyed their membership, requesting information on the status of work completed in the Y2K assessment, renovation, validation, and implementation phases. For example, the Association of State and Territorial Health Officials and the Centers for Disease Control and Prevention (CDC) sent a Year 2000 readiness-assessment survey to 57 state and territorial health officials. According to CDC, officials of 27 states responded as of February 19, 1999, and the results are still under review. Similarly, the Generic Pharmaceutical Industry Association sent a survey to its members last December; it plans to discuss the results at a March 8, 1999, meeting of the Year 2000 Pharmaceuticals Acquisition and Distribution Committee (comprised of federal and pharmaceutical representatives). Finally, HHS' Office of the Inspector General sent a Y2K readiness survey last December to a sample of Medicare providers; it is not known at this time when the results will be available. The working group plans to gather Y2K readiness information from this sector throughout 1999, especially among smaller health care organizations.

Until such survey results are known to consumers, the Y2K readiness of key components of the health sector will remain in doubt. Because of the potential impact of the Year 2000 problem on patient care, it is critical that such readiness information be obtained and publicized. In this way consumers will have access to data that can offer some assurance that the information systems, equipment, and products used in the delivery of health care services will operate as expected when needed after the turn of the century. Conversely, the lack of such information can contribute to consumer doubt, misinformation, or even panic. It can also foster unnecessary stockpiling of drugs and the attendant drain on pharmaceutical product inventories.

Some Biomedical Equipment Status Information Available through FDA

The question of whether medical devices such as magnetic resonance imaging (MRI) systems, x-ray machines, pacemakers, and cardiac monitoring equipment can be counted on to work reliably on and after January 1, 2000, is critical to our nation's health care. To the extent that biomedical equipment uses embedded computer chips, it is vulnerable to the Y2K problem.[7] Such vulnerability carries with it possible safety risks. This could range from the more benign—such as incorrect formatting of a printout—to the most serious—such as incorrect operation of equipment with the potential to decrease patient safety. The degree of risk depends on the role the equipment plays in the patient's care.

As we reported last September,[8] FDA—which provides information from biomedical equipment manufacturers to the public through an Internet World Wide Website—had a disappointing response rate from biomedical equipment manufacturers to its request for compliance information. The FDA biomedical equipment database also lacked detailed information on the make and model of compliant equipment. Further, FDA did not require manufacturers to submit test results certifying compliance. Therefore, the adequacy of manufacturers' corrections of noncompliant equipment could not be assured.

To address these issues, we made recommendations to the Secretaries of HHS and Veterans Affairs (VA)—a key stakeholder in determining the potential effects of the century change on biomedical equipment—to determine what actions, if any, should be taken regarding manufacturers that have not provided compliance information. We also recommended that the departments (1) work jointly to develop a single data clearinghouse to provide compliance information to all users of biomedical equipment, and (2) take prudent steps to review test results for critical care/life support biomedical equipment, especially equipment once determined to be noncompliant but now deemed compliant—and make those results publicly available through FDA's central data clearinghouse.

HHS and VA agreed with our recommendation to develop a single data clearinghouse. FDA, in conjunction with VA, has established a biomedical equipment clearinghouse; it is publicly accessible through the Internet site and contains information on biomedical equipment compliance submitted to FDA by manufacturers, as well

---

Health Care Organizations, National Association of Community Health Centers, and National Association of Rural Health Clinics.

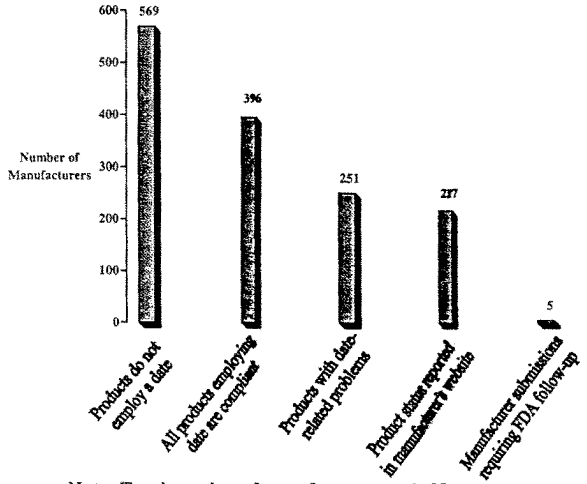
[7] Biomedical equipment refers both to medical devices regulated by HHS' Food and Drug Administration (FDA), and scientific and research instruments, which are not subject to FDA regulation.

[8] GAO/AIMD–98–240, September 18, 1998.

as information gathered by VA and the Department of Defense as part of their Year 2000 compliance projects. FDA also plans to include detailed information on the make and model of equipment reported as compliant.

In its February 10, 1999, quarterly submission to OMB, HHS reported that as of January 12, 1999, about three quarters (1,438) of 1,932 biomedical equipment manufacturers identified by FDA had submitted data to the clearinghouse. As shown in figure 2, about 40 percent of the manufacturers have products that do not employ a date, while about 17 percent reported equipment having date-related problems.

Figure 2: Biomedical Compliance Status Information Reported To FDA by Manufacturers as of January 12, 1999



Note: Total number of manufacturers = 1,438
Source: Department of Health and Human Services

Last September we reported that most manufacturers citing noncompliant products listed incorrect display of date and/or time as the Y2K problem.[9] According to VA, these cases may not present a risk to patient safety because health care providers, such as physicians and nurses, can work around the problem. Of more serious concern are situations in which devices depend on date calculations, which can be incorrect. One manufacturer cited an example of a product used for planning delivery of radiation treatment using a radioactive isotope as the source. An error in calculating the strength of the radiation source on the day of treatment could result in a dose that is too high or too low, which could have an adverse effect on the patient.[10]

HHS reports that FDA will continue to explore ways of obtaining compliance information from manufacturers who have not yet replied. In response to our recommendation that FDA and VA review test results of manufacturers' compliance certifications, VA—deferring to HHS—stated that it did not have the legislative or regulatory authority to do this. HHS, for its part, said that it lacked the available resources to undertake such a review and, further, that insufficient time remained to complete such reviews before 2000. We believe that if HHS lacks sufficient resources to review manufacturers' test results, it may want to solicit the help of federal health care providers and professional associations. Finally, HHS stated that submission of appropriate certifications of compliance is sufficient to ensure that the certifying manufacturers are in compliance. We disagree. Through independent reviews of manufacturers' test results, users of medical devices are provided with a greater level of confidence that the devices are indeed Year 2000 compliant.

In summary, there is great need for much more information available on the Y2K readiness of the health care sector. Until this information is obtained and publicized, consumers will remain in doubt as to the Y2K readiness of key health care components. In addition, while compliance status information is available for some

[9] GAO/AIMD–98–240, September 18, 1998.
[10] *Year 2000 Computing Crisis: Leadership Needed to Collect and Disseminate Critical Biomedical Equipment Information* (GAO/T-AIMD–98–310, September 24, 1998).

biomedical equipment through the FDA clearinghouse, FDA has not reviewed test results supporting manufacturers' certifications to provide the American public with a higher level of confidence that biomedical equipment will work as intended.

* * * * *

Mr. Chairman, this completes my statement. I would be pleased to respond to any questions that you or other members of this Committee may have at this time.

Chairman ARCHER. Thank you, Mr. Willemssen. Does any member wish to inquire of this panel?

Mr. Tanner.

Mr. TANNER. Thank you, Mr. Chairman. I just have one question for Mr. Brown. I understand HCFA set a target date of April the 5th for Medicare providers to submit claims that are Y2K compliant. Will the hospitals be able to meet that target date do you think?

Mr. BROWN. I think the hospitals are working toward that date, Mr. Tanner. And to take our own organization as an example, in St. Louis, our first effort and first focus was really on our total systems. The claims administration piece of that is only part of the total of our operating and patient accounting systems. We're working now doing vendor testing to be in compliance. Will we be done by April 5? Possibly not completely, but we anticipate totally by June 15.

I think the hospitals are working toward this, and I think the fact that the administrator had pointed out, that 58 percent are in compliance today, that's significant. And I think we have to put it in the perspective of hospitals' number one focus: their total operating systems and how that translates into the patient care issues and patient safety issues.

Mr. TANNER. I understand HCFA has provided some software at no cost for this purpose. Is there anything further that could be done, not that the April 5th deadline is such an important date, but just so there is no problem?

Mr. BROWN. The biggest issue to date in terms of the hospitals, in terms of the provider sector, is that that piece of software is only one piece of the total system. And so we have to be able to accommodate that within our total operating systems. And so, again, in some situations it has been very helpful. In other situations, it is not; simply because of the systems that the individual institutions have.

And there's around six major vendors across the country that really supply most of the patient accounting systems. So this is really only one piece of that and the hospitals have to really interface that in with the total.

I think the key thing that was pointed out is the communication. The issue is, once the contingency plans are established, those need to be communicated earlier, rather than later, in terms of HCFA's contingency plans. At the same time, as hospitals and physicians develop their contingency plans in their individual communities, we need to communicate that so that we are able to understand what the potential impact is. Because when you think about it, over 50 percent of the reimbursement comes from governmental

programs, primarily the Medicare and Medicaid Programs. So that could have a significant impact on the cash-flow of hospitals. And we need to understand what the contingencies are for these systems.

Mr. TANNER. Thank you, Mr. Chairman. I yield back.

Chairman ARCHER. Thank you. Are there further questions? If not, thank you very much. We appreciate your input.

And that concludes the hearing on Y2K. The Committee will stand adjourned until 4:30, at which time we will reconvene to markup.

[Whereupon, at 4:03 p.m., the hearing adjourned.]

[Submissions for the record follow:]

Statement of Jacquelyn L. Williams-Bridgers, Inspector General of the Department of State, Arms Control and Disarmament Agency, and United States Information Agency

Mr. Chairman and Members of the Committee: I am pleased to have been invited to provide a statement for the record for the Committee's hearing on the Year 2000 (Y2K) computer problem. On January 1, 2000, many computer systems worldwide may malfunction or produce inaccurate information simply because the date has changed. Unless preventive measures are successful, these failures will have a costly, widespread impact on government and private-sector organizations across the globe.

Embassies, consulates, U.S. businesses, and millions of Americans living abroad rely on their respective host countries' infrastructures to provide essential, day-to-day services such as power, water, telecommunications, and emergency services. In many areas, particularly in the developing world, these services could be disrupted if critical infrastructure components and control systems are not made Y2K compliant. Failure to resolve the Y2K problem or to implement adequate contingency plans could create havoc in the foreign affairs community, including disrupted messaging systems, hindered embassy operations such as visa and passport processing, and failed administrative functions such as payroll and personnel processing.

My office has been actively engaged with the Department of State (the Department) and our embassies overseas to assist them in meeting the millennium challenge. Of particular interest to your Committee, my of lice is also assessing the Y2K readiness of host countries where the United States maintains a diplomatic presence. Our work to date assessing host country readiness has revealed some key themes:

- Modern, industrialized countries are generally ahead of the developing world; however, some of those locations are at risk of having Y2K-related failures because they were late in establishing Y2K programs at the national level, and they are heavily reliant on computer technology in key sectors.
- Developing countries are struggling to find the financial and technical resources needed to resolve their Y2K problems; still, the relatively low level of computerization in key sectors (utilities, telecommunications, and transportation, may reduce the risk of prolonged infrastructure failures.
- Former Eastern bloc countries were late in getting started and are generally unable to provide detailed information on their Y2K remediation programs, and
- Problems related to Y2K readiness in the health care sector were apparent in nearly every location we visited.

This statement will address OIG's oversight of Y2K remediation efforts by countries that host our embassies and consulates and by the U.S. Department of State and the United States Information Agency (USIA).

OIG YEAR 2000 OVERSIGHT EFFORTS

International Y2K Efforts: Host Country Preparedness

OIG has been active in international Y2K issues through our efforts to engage host country representatives and to establish venues for information sharing and cooperation, and to collect information on the Y2K readiness of host countries where the U.S. Government maintains a presence. Since September 1998, OIG has conducted an aggressive effort to collect and analyze information on host country Y2K efforts in 25 cities in 20 countries. In addition to consulting with embassy personnel, OIG met with host country Y2K program managers; representatives from key infrastructure sectors, such as utilities, telecommunications, and transportation; and

with private sector officials to discuss their respective Y2K programs and to share information. A summary of OIG international Y2K site visits is provided in Table 1.

The information we collected about host country readiness provides general insight into a host country's efforts to reduce the impact that Y2K-related failures might have. However, I caution that this information represents the situation at a particular point in time. For example, the situation as represented by the information we collected in Mexico 5 months ago may have changed significantly since then.

Table 1.—Summary of OIG International Y2K Site Assessments

Countries/Cities Visited	Date of Visit
Mexico (Mexico City & Monterrey), Chile (Santiago), Panama (Panama City).	September 1998
South Africa (Pretoria & Capetown), Gabon (Libreville), Cameroon (Yaounde), Ethiopia (Addis Ababa).	October 1998
Hong Kong, Thailand (Bangkok), Singapore, Philippines (Manila).	October/November 1998
India (Mumbai & New Delhi)	December 1998
United Kingdom (London), Russia (Moscow), Ukraine (Kiev), Poland (Warsaw), France (Paris), Italy (Rome), Greece (Athens), Germany (Frankfurt, Bonn, & Berlin).	January 1999

OIG has provided information summaries on each of these countries to appropriate officials in the Department, the President's Year 2000 Conversion Council, the United States Information Agency (USIA), congressional committees, and other foreign affairs organizations. Generally, the information we have collected about specific countries is considered sensitive. Disclosure of such information is limited to other governments, international organizations, and entities which the Department determines may benefit in connection with their own Y2K activities.

Our work has helped to raise awareness of Y2K issues and to increase cooperation and coordination between the U.S. and its foreign partners on mutually beneficial Y2K matters. For example, the United States Embassy in Paris used our visit to develop a number of bilateral Y2K initiatives, including sharing information on health care and developing policy initiatives for assisting African countries with their Y2K efforts. In addition, our work has helped engender support for establishing a policy framework to address Y2K issues in the developing world.

OIG is also engaged in other international Y2K efforts. In accordance with a Memorandum of Understanding signed by the Secretary of State and Chile's Minister of Foreign Affairs, OIG has begun a cooperative effort to work with the Chilean Government on a number of internal audit issues. In September 1998, OIG auditors met with Chilean Government representatives to exchange ideas on addressing and enhancing Y2K-related audit methodologies.

Also, in coordination with the Organization of American States (OAS) and USIA, OIG has initiated a series of USIA Worldnet Interactives with Latin America and Canada to provide expert guidance on timely contingency planning and Y2K compliance in the sectors of health, energy, and financial institutions. In coordination with OAS and USIA, these interactive programs have been broadcast live throughout this hemisphere and worldwide via the Internet. The programs have explored problems, strategies and solutions in the areas of timely contingency planning, energy, and financial institutional readiness.

Results of OIG International Assessments

Based on our work in the countries cited above and on our assessment of other information provided by the Department, four themes have emerged relating to the potential impact the Y2K problem may have in the global arena. Our assessment of the timeliness of host country efforts to solve Y2K problems is being conducted in accordance with a phased methodology, similar to that recommended in the General Accounting Office's (GAO) Year 2000 assessment guide. The phases include awareness of the problem at the highest levels, assessment of the impact of the Y2K problem, renovation or replacement of noncompliant systems, validation of renovated or replaced systems, and finally, implementation of the revised system. According to this methodology, the renovation phase should have been completed by mid–1998 to allow sufficient time for validation and implementation. Further, testing will account for 45–50 percent of the time needed to correct a Y2K problem.

Our work has resulted in the following findings:

Inconsistent Progress in Industrialized Countries. Modern, industrialized countries, while generally ahead of the developing world in terms of identifying and acknowledging the Y2K problem, were not consistently focused or effective in their efforts. Governments in several European countries, for example, had started Y2K programs in mid–1998, and some of those programs were making only minimal progress in getting their systems renovated. The risk of Y2K-related failures is, in some respects, higher in these countries because of their high reliance on modern computers.

Lack of Financial and Technical Resources in Developing Countries. Developing countries were struggling to make headway in solving their Y2K problems. These countries were generally in the assessment phase toward the end of 1998, as they endeavored to develop effective remediation plans and to address the difficult task of finding adequate financial and technical resources to resolve Y2K issues or to develop contingency plans. The governments of some developing countries did not regard Y2K as a priority and thus had not established committees or task forces to address Y2K on a national basis. In these locations, the risk of failure in such key sectors as utilities and telecommunications will depend on the extent to which they rely on computers and embedded devices. Although these countries are generally experienced in dealing with short-term power and telecommunications outages, the question remains as to how well they can handle long-term disruptions in numerous sectors that may concurrently occur because of Y2K-related failures.

Difficulty in Assessing East European Progress. Three countries that were part of the former "Eastern bloc" were also late in getting started on Y2K remediation and generally were still in the assessment phase at the end of 1998. However, we found it difficult to obtain detailed information about the Y2K programs in these countries, thus hindering our ability to develop an overall evaluation of the progress being made. The apparent widespread use of pirated software, and the lack of information on when and where computer equipment and software were obtained in the first place, further confused the situation. Again, similar to what we found in the developing world, the prevalence of analogue technology (or none at all) will reduce the risk of major problems in telecommunications, utilities, and transportation.

Overall Lack of Y2K Readiness in the Health Care Sector. Problems related to Y2K readiness in the health care sector were apparent in nearly every location visited. The failure of an information system or a medical device in a clinic or a hospital can put lives at risk. For example, it is conceivable that a computer might cut off important life support systems after the date change because it assumes the maintenance interval has been exceeded by one hundred years. In most of the countries we visited, efforts to assess the impact of Y2K on hospital systems and medical devices did not get under way until mid–1998, leaving very little time to remediate or replace noncompliant software and devices.

The State Department has also recognized that the potential for Y2K vulnerability is not restricted to its domestic operations and has implemented measures to assess the Y2K readiness of all countries where the United States has a diplomatic presence. In November 1998, the Department sent a cable to embassies instructing them to complete a Y2K survey of their respective host country's Y2K efforts. With the survey instrument, the posts were expected to collect information on a wide array of subjects, including the effectiveness of the country's Y2K program, vulnerability to short-term economic and social turmoil, reliance on technology in key infrastructure sectors, and the status of Y2K correctional activities.

As of February 1, 1999, the Department had received responses from posts in 132 countries. The Department has tasked a group of analysts to evaluate the data contained in these surveys, as well as information from other sources, such as USIA, the World Bank, and this office as well. Based on these analyses, the Department will determine whether travel warnings should be issued concerning particular countries, or drawdown or evacuation plans should be developed for areas where the Y2K problem may pose a risk to Americans living abroad. Toward that end, on January 29, 1999, the Department issued a worldwide public announcement on the Y2K problem to inform U.S. citizens of the potential for problems throughout the world because of the millennium "bug." The notice cited specific areas of concern, including transportation systems, financial institutions, and medical care, as activities that may be disrupted by Y2K-related failures. Further, this announcement goes on to warn that all U.S. citizens planning to be abroad in late 1999 or early 2000 should be aware of the potential for problems and stay informed about Y2K preparedness in the location where they will be traveling.

OIG Work Within the Department of State and USIA

OIG is also playing a significant role in assisting the Department and USIA to meet the millennium challenge facing their respective information technology infrastructures, including computer software, hardware, and embedded devices. The Department has recognized that it is vulnerable to the Y2K problem, and over the past two years has taken steps to remediate its systems and infrastructure to prevent disruptions to its critical business processes.

The Department has established a Program Management Office (PMO), which is responsible for the overall management of the Y2K program within the Department. The PMO's responsibilities include tracking and reporting on the progress being made by the bureaus in remediating systems, providing technical advice and assistance, issuing contingency planning guidance, and certifying systems for Y2K compliancy. As of February 8, 1999, the Department reported that 61 percent of its mission-critical systems had been implemented, and it expects 90 percent to have been implemented by March 31, 1999.

OIG's first series of reviews focused on assessing internal aspects of the Department's program to ensure its systems and devices are Y2K compliant, and we highlighted a number of key Y2K issues. These included the need for more thorough data collection and accurate status reporting to the Office of Management and Budget, better tracking of applications, greater focus on the computer networks that support Department operations, more specific attention to the vulnerabilities of the Department's overseas computer networks, and more timely issuance of critical Y2K guidance.

In addition, my office has assisted in establishing a process through which the Department can certify the Y2K readiness of its mission-critical systems. The purpose of this process, which we understand is one of the most rigorous in the Federal Government, is to provide the Department's senior management with assurance that every feasible step has been taken to prevent Y2K-related failures on January 1, 2000. We assisted in writing detailed guidelines that each bureau must use in developing application certification packages for submission to PMO. In addition, through an agreement with the Under Secretary of State for Management, OIG is reviewing the adequacy of all certification packages for mission-critical systems before they are provided to the Y2K certification panel. Thus far, we have evaluated and provided our comments to the Department on seven application certification packages, and two of those have been officially certified.

* * * * *

In conclusion Mr. Chairman, our assessments in 25 foreign locations over the past 5 months have provided a mixed picture of international Y2K readiness. In some places we found convincing evidence that effective programs were in place in both the public and private sectors. In other places, however, the picture was either grim with no program in place and little progress being made, or inconclusive because the information provided did not contain sufficient detail to develop a reliable assessment.

Faced with a relentless and unforgiving deadline, countries have to make difficult decisions concerning the use of scarce resources to fix a problem that has not yet occurred. As such, over the coming months, the State Department and other U.S. Government agencies will need to revisit the information and the issues presented here in order to gain a better understanding of the potential global impact of Y2K. Only a concerted and consistent effort to collect and analyze the best information available will allow the U.S. Government and its overseas partners to adequately predict and prepare for those Y2K-related failures that occur after December 31, 1999, and to take the actions needed to protect global U.S. interests.

Statement of Thomas D. Roslewicz, Deputy Inspector General for Audit Services, U.S. Department of Health and Human Services

INTRODUCTION

Mr. Chairman and Members of the Committee, I am Thomas D. Roslewicz, Deputy Inspector General for Audit Services of the Office of Inspector General (OIG), Department of Health and Human Services (HHS). I am pleased to submit this statement for inclusion in the permanent record of today's hearing on the readiness of HHS' computer systems for the Year 2000 (hereafter Y2K). Consistent with the

focus of the hearing, this statement principally discusses the remediation efforts of the Health Care Financing Administration (HCFA) and the Administration of Children and Families (ACF).

The OIG has taken an active role in monitoring the progress being made by HCFA and other HHS agencies to remediate their mission critical systems. We have an on-going presence, both at HCFA and ACF central offices, to oversee the progress on their internal systems. We also have focused our monitoring efforts on the Medicare contractors, where we have participated in over 200 site visits with HCFA staff and HCFA's Independent Verification and Validation (IV&V) contractor. We have issued two reports to the HHS Chief Information Officer (CIO) and a number of alerts to the HCFA CIO pointing out HCFA's accomplishments as well as issues that were a concern to the OIG. Previous OIG testimony before the House Appropriations Subcommittee on Labor, HHS and Education outlined some of the more significant actions taken by HHS as well as some of our concerns. The following updates those actions and summarizes the results of our current reviews.

But first I'd like to point out the benefit of the Y2K effort. The Y2K remediation, while monumental, also created an opportunity for HHS to collectively assess—and improve—the efficiency of its critical core business processes. Longstanding hardware and software problems are being corrected, configuration management is being improved, and the need for consistent dialogue between program managers and Information Technology (IT) staff is now recognized. We believe the result will be an increasingly better delivery of services by HHS to its constituents.

SUMMARY

The HHS continues to place Y2K remediation as its highest IT priority, with a particular focus on the systems that process billions of dollars each year for the Medicare program. Bi-weekly meetings continue with the Deputy Secretary, the HHS CIO, and Agency heads and CIOs. IV&V certification for compliance is required for all HHS agencies and independent testing is also required for HCFA's major systems (i.e., seven standard or "shared" systems, two of its Common Working File [CWF] host sites and eight of its most critical internal systems). This independent testing is to be done by a contractor other than the IV&V contractor.

The HHS permitted agencies to reassess their initial inventory of mission critical systems, thus allowing them to focus resources on their core business processes. This resulted in a substantial reduction in the number of Department-wide mission critical systems from 490 to 290. For HCFA and the ACF, this reassessment did not result in any change in their total number of mission critical systems. It did, however, change the composition of the HCFA internal systems designated as mission critical.

HHS maintained December 31, 1998 as its deadline for all mission critical systems to be Y2K compliant, thus allowing a full year for recertification and post-implementation testing. Unlike ACF, which reported that it met the December 31 due date and generally completed its IV&V certifications, HCFA stated that it never planned IV&V certification for either its internal or external systems. Instead the IV&V contractor was to participate in the remediation process and to "witness" the certification testing being done by the internal system owners and the Medicare contractors. In the case of the internal systems, the IV&V contractor was to issue a "witness report" on that phase of remediation.

To meet the December 31 due date, HCFA accepted self-certification of compliance from internal system owners and self-certifications with "except-for" statements from its Medicare contractors. The OIG's review of these exception statements found that some appear to be significant. For example, an exception reported for the Fiscal Intermediary Standard System (FISS), a system used by about 30 Medicare contractors, is the inability of one of the system's modules to recognize leap years as well as its continuing use of the two position year instead of the four position year and century. While apparently significant, these exceptions, given the size of the FISS (over 2,000 individual modules), must be evaluated to determine their true impact. In general, we believe that exceptions such as these may have a domino affect on system users, as they might be unable to certify their internal sub-systems before receiving a certified version of the shared systems.

According to HCFA, these exceptions will be resolved before the Office of Management and Budget's (OMB) deadline of March 31, 1999. The HCFA also points out that all but one of its external systems, that being the Arkansas Part A Standard System (APASS) used by seven Part A contractors, are currently in production. The HCFA believes that this extended production period allows ample time for remediation of the exceptions reported as well as of any unforeseen problems surfaced. The

HCFA expects to certify by the March 31 due date and to recertify systems during the summer of 1999 with all systems recertified by November 1, 1999.

With regard to APASS, the Arkansas Blue Cross and Blue Shield, the system maintainer, could not both renovate and test the quality of code changes and still meet the December 31 due date. This became apparent when a significant number of users began requesting software corrections that hampered the contractor's ability to timely complete its code renovations. The contractor subsequently requested, and HCFA approved, an alternate remediation plan calling for date relief. On January 27, 1999, Arkansas Blue Cross and Blue Shield distributed a Y2K compliant production version of software to all its users. These users are now testing APASS integration with their internal systems to determine compliancy by March 31, 1999. Arkansas's certification statement is pending the results of user testing. According to HCFA, all users have indicated that they would complete certification by March 31, 1999.

Issues such as those mentioned above were due, in part, to an underestimation of the complexity and magnitude of the Year 2000 problem. It was initially viewed as an IT problem that could be resolved by the IT specialists when, in fact, it was both an IT and business operation problem requiring attention from all levels of management. This underestimation was evidenced by the milestone schedules prepared by the HHS agencies, especially with regard to HCFA. The early schedules had all phases of the Year 2000 model compressed into the last 2 months of the calendar year with no recognition of system interdependencies (i.e., "end-end testing"). Consequently, it was impossible for management to get a true "snap shot" of its remediation progress. In the case of HCFA, this resulted in costly delays in making key management decisions for system conversions and transitions, contingency planning, developing test plans, and requesting legislative relief. To remedy the situation, HCFA centralized its Y2K remediation effort by creating residence teams at key contractor sites. These teams report directly to HCFA headquarters. We believe this action further strengthens the HCFA's ability to immediately identify an ongoing or developing problem at a Medicare contractor and, equally important, immediately strategize a solution to the identified problem.

As agencies approach OMB's March 31, 1999 deadline, the focus of system owners must now shift to end-to-end testing to ensure that all critical core business processes are Y2K compliant and functioning correctly. Testing of Medicare claims processing systems must include testing between contractors, testing of the interface with provider systems as well as testing the interface with the HHS' payment system with the U.S. Treasury. Results of recent monitoring visits to Medicare contractors have demonstrated the importance of testing. For example:

- A November 1998 visit to the Computer Sciences Corporation (CSC), the system maintainer for the CWF, determined that neither CSC nor the previous system maintainer had planned to future date test the third release of the 1998 changes to CWF. Our concern was that unless the changes made to the CWF in the third release were future date tested prior to January 1, 2000, the possibility existed that any changes which were not Y2K compliant would not be detected until it was too late. In the same alert, we reported a traceability matrix was needed to ensure sufficient test coverage. This matrix is a general control to ensure that all necessary tests are conducted against pass/fail criteria and are quality reviewed. The HCFA believes that changes made to the CWF in the third release were future date tested during the testing of the fourth release. We intend to follow-up on these issues.
- A December visit to Blue Cross/Blue Shield of Oklahoma (BCBSOK) identified weaknesses in the contractor's testing plan. Although 96 percent of the claims processed by BCBSOK are received electronically, only on-line claims that are entered directly into the FISS are being tested. As a result of our discussions with BCBSOK officials, the contractor agreed to create a batch of electronic claims for additional testing through the entire claims process.
- A December visit to Blue Cross/Blue Shield of North Carolina, a Fiscal Intermediary (FI) that uses the APASS, determined that the contractor needed: (i) a formal Y2K test plan, written test procedures, and documented test case scenarios for its APASS testing; (ii) a quality assurance plan to ensure the quality of its Y2K testing; (iii) a configuration management plan specific to Medicare, i.e., a plan of procedures to be followed when Medicare applications are designed, developed, and modified, and (iv) a formal contingency plan. We will follow-up on resolution of these findings during our next site visit.

The Committee can be assured that we will continue our work in this most important area. The HCFA has accomplished a lot, but much more needs to be done. Their present remediation strategy is aggressive, high-risk, leaving little room for error. We will be monitoring efforts of both the HCFA central office and the Medicare contractors, with a focus on compliance testing, including end-to-end testing.

We will continue our practice of reporting our concerns to the appropriate HHS officials so that timely action can be taken to facilitate the remediation process. We appreciate this opportunity to discuss HHS' systems' readiness for the Year 2000.

Statement of White House Conference on Small Business

THE IMPACT OF YEAR 2000 TRANSITION ON SMALL BUSINESSES

The undersigned are the elected Regional Chairs of Taxation representing the 2000 delegates to the White House Conference on Small Business. We were delegated the responsibility of advancing implementation of the conference's recommendations with regard to the tax issues and reporting progress back to the delegates. As the Ways and Means Committee prepares to consider the impact that the year 2000 conversion might have on the nation, the delegates to the White House Conference on Small Business want to remind you to consider the importance of the small business community to our economy. Please take into account the cost for them of updating computer software, computer hardware and other equipment because these issues are important for the growth and progress of small businesses in America.

SIMPLICITY

The single largest concern of the White House Conference on Small Business was dealing with the overall complexity of government and the complexity of the tax code in particular. Allocating and reporting income taxes and payroll taxes is the one common experience of every business and may be the only interaction that most businesses have with the federal government. Simplifying the tax process would, therefore, improve the situation for every small business. Studies have shown that it costs small businesses more to comply with the tax code, and considerably more in comparison to each dollar of sales, than it costs large businesses. Small businesses have fewer sales over which to spread the cost.

This is true for the cost allocation of the expenses related to the year 2000 conversion. Small businesses do have some tools, § 179 expensing, for example, which could help them, but the committee should make an extra allowance to help them meet what could be a dramatic one-time expenditure.

REGULAR EXPENSING—INTERNAL REVENUE CODE § 179

The expensing limit of IRC § 179 will be gradually increased to $25,000 (by the year 2003) from its current level as provided for in the Small Business Job Protection Act passed by Congress in 1996. The small business community appreciated the attention Congress gave to this issue, but would urge greater increases and quicker implementation. Expensing is perhaps one of the most useful tax simplifiers for small business; however its use still remains limited. In addition, Congress did not correspondingly raise the $200,000 limit on purchases. These days, one piece of machinery (even for a very small business) can exceed this limit, effectively eliminating many small businesses from any benefits.

SOFTWARE EXPENSING & THE YEAR 2000

First, we, the Regional Chairs for Taxation of the White House Conference on Small Business, would like to point out that the allocation of costs for software is already a cloudy area with or without the year 2000 problem. We feel a way Congress could make a tremendous contribution is to permanently allow expensing in the year a business purchases software obtained for business purposes. It is practically impossible to declare with certainty what the useful life of software is within a business. With the pace of technology, useful life gets shorter and shorter as better products that exploit hardware advances seem to hit the market continuously.

This basic problem is multiplied by the year 2000 conversion that many small businesses do not fully understand. The cost to them to upgrade their computer software and hardware might be considerable. But software and hardware may only scratch the surface of the problem. Identifying and correcting buried chips in everyday equipment may really explode the costs. Think of computerized heating, cooling, and security systems. Consider all the cell phones, business telephone systems, dispatcher systems, beepers, fax machines and Xerox machines. A small business needs

to also look at their automobiles, trucks and other heavy equipment. The list goes on and on.

We believe it serves public policy to provide incentives to help small businesses assess their exposure to the problem and purchase new software as soon as possible. This will insure the continuity and free flow of business in 2000. The full cost to small business to assess the threat and then to test and replace equipment as necessary should be deductible in the year of expense. The Process should be kept as simple as possible and would not involve a major revenue outlay since these costs are already recoverable through expensing, or depreciation—capitalization.

In 1996, the Gartner Group estimated that the year 2000 problem would cost $600 billion to fix. Later estimates by Lloyds of London have been as high as $1 trillion. Economist Ed Yardeni has estimated that there is a 35% chance of a global recession because some businesses will be unable to deal with their year 2000 problems. And, unlike most projects, the final due date can not be changed with the year 2000 problem—the year 2000 will arrive whether we are ready or not.

The Federal Reserve is currently predicting that 1% to 7% of U.S. businesses will fail because of the year 2000 problem. The Board is encouraging all businesses to address the problem as early as possible. The Small Business Administration and the Department of Commerce are encouraging all small businesses to make plans to assess the situation now so that actions can be taken in a timely manner. Many of the affected businesses will need new items of software and hardware, and we would urge that the materials immediately be deemed able to be expensed.

SUMMARY

In general, the White House Conference has urged Congress to investigate the simplest ways to help small businesses solve their problems. We would like to see legislation to increase § 179 expensing and permit small businesses to write off in the year of purchase any expense related to year 2000 conversion but without regard for those expenses to the limits of the current § 179. If, for budget purposes, the bill must be limited, we suggest limits along the lines of those in HR 179 offered by Representative Thurman, that generously push up the expensing amount.

As always, the White House Conference Tax Chairs would like to recommend that any changes that are considered by the Committee be analyzed for their impact on small businesses and that representatives of the small business community be included in future hearings on the subject.

We would like to work with you, your colleagues, and your staff to help you better understand the importance of these proposals to small businesses and the U.S. economy. Thank you for your time and attention to this matter.

THE WHITE HOUSE CONFERENCE TAX CHAIRS

Region 1: Debbi Jo Horton, Providence, Rhode Island
Region 2: Joy Turner, Piscataway, New Jersey
Region 3: Jill Gansler, Baltimore, Maryland
Region 4: Jack Oppenheimer, Orlando, Florida
Region 5: Paul Hense, Grand Rapids, Michigan
Region 7: Edith Quick, St. Louis, Missouri
Region 8: Jim Turner, Salt Lake City, Utah
Region 9: Sandra Abalos, Phoenix, Arizona
Region 10: Eric Blackledge, Corvallis, Oregon

○