STATUS UPDATE ON THE YEAR 2000 PROBLEM

HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

OF THE

COMMITTEE ON GOVERNMENT REFORM AND OVERSIGHT HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTH CONGRESS

SECOND SESSION

JUNE 10, 1998

Serial No. 105–183

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

U.S. GOVERNMENT PRINTING OFFICE

52–528 WASHINGTON : 1998

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-058377-2

AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

COMMITTEE ON GOVERNMENT REFORM AND OVERSIGHT

DAN BURTON, Indiana, *Chairman*

BENJAMIN A. GILMAN, New York
J. DENNIS HASTERT, Illinois
CONSTANCE A. MORELLA, Maryland
CHRISTOPHER SHAYS, Connecticut
CHRISTOPHER COX, California
ILEANA ROS-LEHTINEN, Florida
JOHN M. McHUGH, New York
STEPHEN HORN, California
JOHN L. MICA, Florida
THOMAS M. DAVIS, Virginia
DAVID M. McINTOSH, Indiana
MARK E. SOUDER, Indiana
JOE SCARBOROUGH, Florida
JOHN B. SHADEGG, Arizona
STEVEN C. LATOURETTE, Ohio
MARSHALL "MARK" SANFORD, South Carolina
JOHN E. SUNUNU, New Hampshire
PETE SESSIONS, Texas
MICHAEL PAPPAS, New Jersey
VINCE SNOWBARGER, Kansas
BOB BARR, Georgia
DAN MILLER, Florida
RON LEWIS, Kentucky

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

BERNARD SANDERS, Vermont (Independent)

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

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

STEPHEN HORN, California, *Chairman*

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

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

EX OFFICIO

DAN BURTON, Indiana

HENRY A. WAXMAN, California

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

CONTENTS

	Page
Hearing held on June 10, 1998	1
Statement of:	
Callahan, John, Assistant Secretary, Management and Budget, Department of Health and Human Services	37
Curtis, William, Special Assistant for the year 2000, Command, Control, Communication and Intelligence, Department of Defense	55
Lewis, Howard, Jr., Acting Chief Information Officer, Department of Energy	73
Smith, Marshall, Acting Deputy Secretary, Department of Education	44
Willemssen, Joel, Director, Accounting and Information Management Division, U.S. General Accounting Office, accompanied by Jack Brock, Director, Government-wide Defense Information Systems	9
Letters, statements, etc., submitted for the record by:	
Callahan, John, Assistant Secretary, Management and Budget, Department of Health and Human Services, prepared statement of	39
Curtis, William, Special Assistant for the year 2000, Command, Control, Communication and Intelligence, Department of Defense:	
Information concerning resource availability	101
Information concerning weapon systems	100
Prepared statement of	57
Horn, Hon. Stephen, a Representative in Congress from the State of California, prepared statement of	4
Lewis, Howard, Jr., Acting Chief Information Officer, Department of Energy:	
Information concerning emergency management plans	106
Prepared statement of	75
Smith, Marshall, Acting Deputy Secretary, Department of Education, prepared statement of	47
Willemssen, Joel, Director, Accounting and Information Management Division, U.S. General Accounting Office:	
Information concerning Canada reallocating resources	90
Prepared statement of	12

STATUS UPDATE ON THE YEAR 2000 PROBLEM

WEDNESDAY, JUNE 10, 1998

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

The subcommittee met, pursuant to notice, at 11 a.m., in room 2154, Rayburn House Office Building, Hon. Stephen Horn (chairman of the subcommittee) presiding.

Present: Representatives Horn and Kucinich.

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

Mr. HORN. This is the hearing to be held on the status update on the year 2000 problem. I have called on the President to designate the year 2000 problem as a national priority. The American people deserve to be protected from this computer virus of sorts, which is mainly a management problem. There have been too many delays. Progress fixing this problem continues to be too slow, and we are rapidly running out of time. Now is the time for the President to designate the year 2000 problem as a national priority.

Why am I concerned that the American people may suffer unnecessarily because of administration delay? Over 2 years ago, on April 16, 1996, this subcommittee held the first congressional hearing on this issue. At that hearing we established: first, that the problem is very real; second, the consequences could be serious; and, third, that there is little time to accomplish a lot of hard work.

When we started, there were 1,355 days remaining until the unmovable deadline of January 1, 2000. Today, there are only 570 days remaining. Fifty-eight percent of the available time has past. Unfortunately, the Federal Government is only 39 percent compliant today, and we are definitely behind.

We have continuously pushed the President, the Office of Management and Budget, the Departments, and the agencies to work harder and work faster. Some agencies, such as the Social Security Administration, are doing a great job. They deserve our commendation, and they have received it for 2 years. However, if you look at the report card we issued only 8 days ago, only 4 agencies received an A, 16 agencies received C or worse, and 10 agencies received D or F. Overall, the administration earned an F, and that is simply not acceptable. We cannot allow Defense, Energy, Education, Health and Human Services, our witnesses today, to fail.

On this report card, we included four additional criteria. On our first report card, way back in 1996, agencies received an A just for having a good plan. We have continued to raise the hurdle from plans and promises to real results. On our last report card, 90 percent of the grade was based on mission-critical systems only, with 10 percent on additional criteria. This time our report card based 80 percent of the grade on mission-critical systems, with 20 percent additional criteria.

The contingency plans are crucial. It is not sufficient to just consider alternative computer systems. Agencies must plan for continuity of business operations under very adverse conditions.

Telecommunications are also crucial. Telecommunication systems link together most computer systems. Telecommunications are also a simple backup when computer systems fail. I should be able to phone somebody and say, "hey, my computer is down, but please send me whatever it is I need anyhow, and we will sort out the computer records later." Obviously, if the phones are down, that simple backup won't work.

Embedded systems are the sleeping giant in the year 2000 problem. Tiny little computer chips embedded in control devices are everywhere in industry throughout the world. They can stop an automobile assembly line, a chemical plant, or an electric utility grid. It is the responsibility of the Federal Government to fix its own embedded chip problem, especially in particular areas such as Defense.

Further, it is the responsibility of the administration to provide leadership on this problem, which has been sorely lacking until recently. The President should use the bully pulpit to make sure these problems are well-known and understood by the American citizens.

We hear constantly from people who are becoming knowledgeable in this area: Should I take my money out of the bank before January 1, 2000? Should I not buy a plane ticket for January 1, 2000? We need to reassure people that something is being done; and we need, in the agencies, to get something done.

External data exchanges are also crucial. Most systems pass data from computer to computer. Consider a simple bank check which may go through dozens of computer systems. Unfortunately, dirty data from one computer can bring down another computer system. Even if your system is fixed, another system may bring it down.

The Office of Management and Budget has proven once again, with the year 2000 problem, that there is no "M" in OMB. OMB has been particularly poor at defining the agency progress reporting requirements. As our recommended monthly reporting content chart shows, we need only 24 numbers to determine progress in all areas. Today's quarterly reports have dozens of irrelevant numbers and sometimes hundreds of pages, and they only cover the first row of the recommended table.

DOD, although behind, is already providing the vast majority of what we really need. If DOD can do this, so, too, can the rest of the agencies. It only requires that OMB help manage the problem, rather than their current baby-sitting exercise.

These are all issues that affect not only the Federal Government but the entire country. The administration must fix its own year

2000 computer problems. Plus, the administration has a responsibility to the American people, again, to provide leadership. The President must take that role and should designate the year, as we have said several times before, a national priority.

We cannot afford any further delay. We cannot afford any more foot-dragging. We cannot accept major agencies being late. That is why some of you are here today. We cannot tolerate thousands of the Federal Government's mission-critical systems failing.

So, with that, gentlemen, I now yield to my colleague, the distinguished member of this committee, the ranking minority member, Mr. Kucinich of Ohio.

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

DAN BURTON, INDIANA
CHAIRMAN
BENJAMIN A. GILMAN, NEW YORK
J. DENNIS HASTERT, ILLINOIS
CONSTANCE A. MORELLA, MARYLAND
CHRISTOPHER SHAYS, CONNECTICUT
STEVEN SCHIFF, NEW MEXICO
CHRISTOPHER COX, CALIFORNIA
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. McHUGH, NEW YORK
STEPHEN HORN, CALIFORNIA
JOHN L. MICA, FLORIDA
THOMAS M. DAVIS III, VIRGINIA
DAVID M. McINTOSH, INDIANA
MARK E. SOUDER, INDIANA
JOE SCARBOROUGH, FLORIDA
JOHN SHADEGG, ARIZONA
STEVE C. LaTOURETTE, OHIO
MARSHALL "MARK" SANFORD, SOUTH CAROLINA
JOHN E. SUNUNU, NEW HAMPSHIRE
PETE SESSIONS, TEXAS
MIKE PAPPAS, NEW JERSEY
VINCE BROWNBACK, KANSAS
BOB BARR, GEORGIA
ROB PORTMAN, OHIO

ONE HUNDRED FIFTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM AND OVERSIGHT

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
MINORITY (202) 225–5051
TTY (202) 225–6852

HENRY A. WAXMAN, CALIFORNIA
RANKING MINORITY MEMBER
TOM LANTOS, CALIFORNIA
BOB WISE, WEST VIRGINIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
GARY A. CONDIT, CALIFORNIA
CAROLYN B. MALONEY, NEW YORK
THOMAS M. BARRETT, WISCONSIN
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
CHAKA FATTAH, PENNSYLVANIA
ELIJAH E. CUMMINGS, MARYLAND
DENNIS KUCINICH, OHIO
ROD R. BLAGOJEVICH, ILLINOIS
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
JIM TURNER, TEXAS
THOMAS H. ALLEN, MAINE
HAROLD E. FORD, JR., TENNESSEE

BERNARD SANDERS, VERMONT
INDEPENDENT

Chairman Horn
Opening Statement
June 10, 1998
"Status Update on the Year 2000 Problem"

I have called on the President to designate the Year 2000 problem as a National Priority. The American people deserve to be protected from this computer problem. There have been too many delays. Progress fixing this problem continues to be too slow. We are rapidly running out of time. Now is the time for the President to designate the Year 2000 problem as a National Priority.

Why am I concerned that the American people may suffer unnecessarily because of Administration delay? Over two years ago, on April 16, 1996, this subcommittee held the first Congressional hearing on the Year 2000 problem. At that hearing we established: one, that the problem is real, two, that the consequences could be serious and, three, that there is little time to accomplish a lot of hard work.

When we started there were 1,355 days remaining until the unmoveable deadline of January 1, 2000. Today, there are only 570 days remaining. 58% of the available time has past. Unfortunately, the Federal Government is only 39 percent compliant today. We are definitely behind.

Worse, the rate of progress has slowed down. The acceleration promised by the Administration has not happened yet. Assuming the Administration continues its current rate of progress, thousands of Federal Mission-Critical Systems will NOT be compliant before the OMB March 1999 deadline.

We have continuously pushed the President, the Office of Management and Budget, and the Departments and agencies to work harder, work faster, work smarter. The President did not act until February 4th of 1998, almost 2 years after we started.

The Office of Management and Budget is still not taking the problem seriously, with only a couple of part-time people working on the Year 2000 problem.

Some agencies, such as the Social Security Administration, are doing a great job and deserve commendation. However, if you look at the Report Card we issued only 8 days ago, only 4 agencies got an A. 16 agencies got a C or worse. And, 10 agencies got a D or F.

Overall the Administration earned an F. This is not acceptable. We can not allow Defense, Energy, Education, and Health and Human Services, our witnesses today, to fail. The Administration must work harder, faster, smarter.

In fact, our earlier estimate of 62% complete at OMB's deadline was too generous. We have since calculated a weighted average that shows only 55% done at OMB's March 1999 deadline. On this basis the rate of progress slowed by 4% instead of 2%. Using either calculation the basic message is the same: the Administration is NOT accelerating, rather, it is slowing down.

On this report card we included 4 additional criteria. On our first report card, back in 1996, agencies got an A, just for having a good plan. We have continued to raise the hurdle from plans and promises to real results. On our last report card, 90 percent of the grade was based on Mission-Critical Systems Only, with 10 percent on additional criteria. This time, our report card bases 80 percent of the grade on Mission-Critical Systems, with 20 percent on additional criteria.

Contingency Plans are critical. The Government Accounting Office and I have been pushing better contingency planning. It is not sufficient to just consider alternative computer systems. Agencies must plan for continuity of business operations under adverse conditions.

Telecommunications are also critical. Telecommunications systems link together most computer systems. Telecommunications are also a simple backup when computer systems fail. I should be able to phone somebody and say my computer is down, but please send me whatever it is I need anyway, and we will sort out the computer records later. Obviously, if the phones are down, that simple backup will not work.

Embedded Systems are the sleeping giant in the Year 2000 problem. Tiny little computer chips, embedded in control devices, are everywhere in industry. They can stop an automobile assembly line, a chemical plant, or the electric utility grid. It is the responsibility of the Federal Government to fix its own embedded chip problem, especially, in particular areas like Defense. Further, it is the responsibility of the Administration to provide leadership on this problem. The President should use his "bully pulpit" to make sure that these problems are well known.

External Data Exchanges are also critical. Most systems pass data from computer to computer. Consider a simple bank check which may go through dozens of computer systems. Unfortunately, dirty data from one computer can bring down another computer system. Even if your system is fixed, another system may bring it down.

The Office of Management and Budget, has proven once again with the Year 2000 problem, that there is no "M" in OMB. OMB has been particularly poor at defining the agency progress reporting requirements. As our Recommended Monthly Reporting Content chart shows, we need only 24 numbers to determine progress in all areas. Today's quarterly reports have dozens of irrelevant numbers and sometimes hundreds of pages and they only cover the first row of my recommended table. DOD, although behind, is already providing the vast majority of what we really need. If DOD can do this, so too can the rest of the agencies. It only requires that OMB help manage this problem, rather than their current baby-sitting exercise.

These are all issues that affect not only the Federal Government, but the entire country. The Administration must fix its own Year 2000 computer problems. Plus, the Administration has a responsibility to the American people to provide leadership.

Where you work, where you shop, and even where your children go to school will be affected. Manufacturing, finance, and agriculture will be affected. The American economy can be seriously affected. Federal, State, and Local governments will be affected. The American people can be seriously affected.

The President must take a leadership role.

The President should designate the Year 2000 problem as a National Priority. We can not afford further delay and foot dragging. We can not accept major agencies being late. We can not tolerate thousands of the Federal Government's Mission-Critical Systems failing.

Now is the time for the President to designate the Year 2000 problem as a National Priority. The American economy must be protected. The American people must be protected.

Congress has been pushing this issue hard for over two years.

Now is the time for the President to designate the Year 2000 problem as a National Priority.

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

I want to thank the chairman for his leadership on the year 2000 computer issue. As our guests here today know, this subcommittee has been actively tracking and often encouraging progress at Federal agencies on their Y2K efforts. Our country is marching rapidly toward the next century and toward a test of our resourcefulness and preparedness. We will soon find out whether our bridge to the 21st century is Y2K compliant.

Today, we will have an opportunity to discuss substantial challenges facing four Federal agencies who appear to be among the farthest behind. We will hear about their problems and consider how to help. Some of these agencies face obstacles from their private contractors who are not progressing quickly enough. For example, the Department of Health and Human Services and Energy operate, in large part, through their contractors. HHS contractors have not yet completed their systems assessment. I might add, Mr. Chairman, the contractual relationship between many private vendors and Government agencies is an integral part of the Y2K problem, and I think this committee does well to explore that.

The sheer number and size of the systems that the Department of Defense must convert is staggering. Moreover, their systems are global in reach and, by definition, what affects the Department of Defense affects the security of this country.

I am sure that our witnesses here are familiar that agencies do face serious funding constraints. They may need more money and more flexibility in reprogramming money while it is still timely. Agencies must now simultaneously fix their systems and develop contingency and business continuity plans. They must assure that they have the time and funds to conduct meaningful end-to-end testing of their compliant systems to make sure they will work in the real world of January 1, 2000.

Moreover, agencies will be increasingly expected to reach out to both domestic and foreign entities to educate and assist in their conversion efforts. Our world is interdependent, and the Y2K issue starkly demonstrates this reality.

I am particularly concerned with alerting State, local, and city governments to their potential vulnerabilities and assisting in preparation. We in Congress, of course, have an opportunity in helping to make sure that local governments, constituents, and private sector industries have the resources they will need to enter the millennium as seamlessly as possible.

As I understand it, the Department of Education has proposed a joint initiative with our subcommittee to help get Members of Congress involved in outreach to the schools in their districts. This is a great idea, and we must encourage similar efforts in other agencies. For example, HHS has many active relationships with entities at State and local levels, and once HHS is able to effectively get its house in order on this, its resources could also be communicated throughout this country.

Mr. Chairman, I think every agency, in its reach throughout this Nation, as they are able to firm up the Y2K protocols within their own agencies, would have the chance to communicate to their interested constituency across this country and tell them how you did it and how they can do it.

A great deal of attention is, of course, today going to be focused on the local agencies' Y2K efforts, necessarily so, because a huge amount of work remains to be done. But just be aware that we in Congress are also aware that we can use our local contacts, connections, speaking engagements, meetings with constituents to get the word out about the year 2000 problem. We are presented daily with opportunities to raise the awareness of people on this issue, and we need to make the most of each one.

I want to conclude by noting that Chairman Horn has worked tirelessly to raise awareness of this issue; and, for that, people all over this country should be most grateful.

I am sure that each of our witnesses today have been similarly consumed in this difficult challenge. I hope that each one of the witnesses will continue to work on this process, building a bridge to the next century that is Y2K compliant.

Mr. Chairman, again, I want to thank you for your efforts. I will return briefly. I have a markup right down the hall in Education, and I will have my staff here to take notes. I will be back to participate, at least in Q and A.

So thank you all for being here today, and I will look forward to reading your testimony.

Mr. HORN. Well, I thank the gentleman and appreciate his generous words. You have been a great asset to this committee with your administrative experience. You and I together have about 30 years in executive work, so we can understand some of these problems.

Gentlemen, I think you know the routine here. This is a committee where we swear in all witnesses. Then, when we introduce you and insert your full statement automatically into the record. We have had a chance to go over it, so we would like you to summarize it.

We have some time here this morning. If you want to take 8 minutes or something, that is fine. Then we would like, once you are done, to have the questions and a dialog between both panelists and those on this side of the wood and you on the other side of the wood in these rather cumbersome hearing rooms.

If you would stand and raise your right hands.

[Witnesses sworn.]

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

I just want to make sure—with Joe Willemssen, you are accompanied by Jack Brock, who is Director of the Government-wide Defense Information Systems.

Mr. Willemssen is Director of the Accounting and Information Management Division, U.S. General Accounting Office.

Please begin and thank you.

STATEMENT OF JOEL WILLEMSSEN, DIRECTOR, ACCOUNTING AND INFORMATION MANAGEMENT DIVISION, U.S. GENERAL ACCOUNTING OFFICE, ACCOMPANIED BY JACK BROCK, DIRECTOR, GOVERNMENT-WIDE DEFENSE INFORMATION SYSTEMS

Mr. WILLEMSSEN. Thank you, Mr. Chairman. Thank you for inviting us to testify today. As requested, I will briefly summarize our statement.

Our statement today will cover two overall areas. First, I will cover the major reasons why the Federal Government will not be able to fix all of its systems in time; and, second, cover what we believe the chairman of the Conversion Council and OMB now need to do to minimize disruptions of critical services to the American public.

As our chart over here illustrates, the progress over the last year by the 24 Federal departments and agencies has generally been too slow. As reported by OMB a year ago, about 21 percent of all the mission-critical systems of these 24 agencies were considered Y2K compliant. A year later, we are now at 40 percent. If this rate of progress were to continue, it is clear that many individual mission-critical systems will not be compliant in time.

However, there are several additional factors contributing to this bleak outlook. First, a great deal of work remains for agencies to renovate and validate systems. According to last month's reports, nine agencies have renovated less than 40 percent of their mission-critical systems due to be fixed, with two agencies having renovated less than 15 percent. This leaves little time for critical testing activities, which the experts say will take at least 50 percent of the total time of the year 2000 program.

Second, agencies are counting on replacement systems in many instances to solve their year 2000 compliance problem; and given the Federal Government's track record on replacement systems, of not being able to often deliver those systems when promised, these replacement efforts generally should be viewed as high risk.

Third, agencies are going to need a significant amount of time for end-to-end testing of multiple systems that have individually been deemed year 2000 compliant. Such end-to-end testing tries to ensure that systems collectively supporting a key business area or key business process operate as intended. Without such testing, systems individually deemed as compliant may not work as expected when linked with other systems.

The quarterly reports also show that five agencies are reporting that they have not yet completed their assessments of systems. That is almost a year behind OMB's governmentwide target. Only 11 agencies reported that they had completed the inventories and/or assessments of telecommunications, and only six of the agencies reported that they had completed inventories and/or assessments of their embedded systems. Overall, this kind of slow progress shown in the quarterly reports reinforces the need for the Conversion Council to implement the key recommendations that we have previously made.

First is priority setting. We have recommended the Council Chairman establish governmentwide and agency-specific priorities based on criteria such as adverse health and safety impacts, na-

tional defense, adverse financial impact, and economic repercussions. The chairman disagreed with this recommendation, stating that agencies have already established priorities and that the Council's focus at this time should be to assist agencies as they work on their mission-critical systems, adding that it may be necessary at a later date to further prioritize systems.

We believe the time to make those decisions and to set priorities is now, while agencies still have the time to correct, validate, and implement their most essential systems. If priorities are not clearly set now, the Government may find that less critical systems are compliant but that some of its highest priority functions are unavailable.

It is interesting to note, in contrast to our country's approach, Canada has established national year 2000 priorities. Currently, it has 44 national priorities, covering areas such as food production, safety, income security, and national defense. According to Canada's year 2000 program director, that country wants to ensure that, at a minimum, these priority areas are fully addressed in the time remaining before 2000.

Mr. HORN. Mr. Willemssen, just to get the record clarified, you referred to the Chair several times of the Conversion Council, and who is that?

Mr. WILLEMSSEN. John Koskinen.

Mr. HORN. Assistant to the President?

Mr. WILLEMSSEN. Yes, sir.

Mr. HORN. Fine. I just wanted to get the record straight as to who is what here.

Mr. WILLEMSSEN. In conjunction with that priority setting, it is also important for Mr. Koskinen to identify the lead agencies, to take responsibility for ensuring that end-to-end operational testing is performed across organizational boundaries and that independent verification and validation of such testing also occur.

Regarding enhanced agency reporting, OMB has acted on some of our recommendations. Specifically, OMB has asked additional organizations to begin providing information on their year 2000 progress. The resulting reports can be very helpful in determining overall progress, identifying risks and raising additional issues.

For example, the report submitted by the U.S. Postal Service shows it plans to spend over half a billion dollars on its year 2000 effort and intends to implement its mission-critical projects by September of this year. However, the report also indicates that the Postal Service has 21 percent of its 335 mission-critical systems still in the assessment phase. This, obviously, raises questions about whether the Postal Service's own target of this September is realistic.

Turning to contingency planning. The chairman of the Council, Mr. Koskinen, and OMB have taken needed action to require agencies to develop business continuity plans. However, much work remains in this area, as we found only four agencies reporting that they had drafted contingency plans for their key business processes.

Another area of concern is that OMB's reports are mainly based on agency reports that have not been consistently independently reviewed. Without such independent reviews, agencies reported

year 2000 status may be inaccurate. Given this, it is important that Mr. Koskinen and OMB require agencies to develop an independent verification strategy to involve inspector generals or other independent organizations in reviewing agency year 2000 progress.

Also, obtaining and retaining adequate and skilled staff for the year 2000 effort is another critical area. In their current quarterly reports, we found 10 agencies and departments describing problems that they or their contractors are encountering in obtaining and/or retaining information technology personnel. Mr. Koskinen agreed with our recommendation to develop an overall personnel strategy, and he has formed a Workforce Issues Group to address this area.

As you mentioned in your opening statement, beyond the Federal Government, it is important that we also address key economic sectors. However, we currently do not know the overall extent of our Nation's vulnerability to the year 2000 or the extent of our readiness. No nationwide assessment has been undertaken to gauge this. We, therefore, recommended that the Council orchestrate a broad assessment of the Nation's year 2000 readiness, to include identifying and assessing the risks of the Nation's key economic sectors. We are aware that the Council has no plans to develop such an assessment; and, without this, the Council will not be in a position to identify areas of weakness and develop mechanisms to mitigate those weaknesses.

In summary, as we move closer to 2000, the magnitude of what must be done is becoming more clear, but, unfortunately, it is also becoming even more daunting than originally envisioned. Aggressive leadership on this issue will therefore be required if we are to avert major negative consequences.

That concludes a summary of our statement, Mr. Chairman. Thank you.

Mr. HORN. Well, as usual, that is a very thorough statement.

We appreciate all you do, not only here in the hearings but, just to spread some of the heat, I should note that I depend on you to check all the grades we have done here to make sure we are being fair. You have told me in some places we shoud be harder, and we appreciate that advice. We appreciate all that your staff has done in looking at various agencies before we hold these hearings.

[The prepared statement of Mr. Willemssen follows:]

Mr. Chairman and Members of the Subcommittee:

We are pleased to join you again today to discuss the computing crisis--of which you are well aware--posed by the upcoming change of century. No major organization, public or private, is immune from potential disruption, including a wide spectrum of government programs vital to Americans. As the world's most advanced and most dependent user of information technology, the United States possesses close to half of all computer capacity and 60 percent of Internet assets.[1] As a result, the year 2000 presents a particularly sweeping and urgent challenge for entities in this country.[2]

For this reason, in February 1997 we designated the Year 2000 problem as a high-risk area[3] for the federal government, and have published guidance[4] to help organizations successfully address the issue. Since that time we have issued over 40 reports and testimony statements detailing specific findings and recommendations related to the Year

---

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

[2]For the past several decades, automated information systems have typically represented the year using two digits rather than four in order to conserve electronic data storage space and reduce operating costs. In this format, however, 2000 is indistinguishable from 1900 because both are represented only 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.

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

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

2000 readiness of a wide range of federal agencies.[5] The common theme has been that serious vulnerabilities remain in addressing the federal government's Year 2000 readiness, and that much more action is needed to ensure that federal agencies satisfactorily mitigate Year 2000 risks to avoid debilitating consequences.

My testimony today will discuss the results of the most recent reports submitted to the Office of Management and Budget (OMB) on the slow progress made by the federal government in achieving Year 2000 compliance. In light of the pace of this progress, I will then provide our views on what needs to be done now to minimize disruptions to critical services.

PROGRESS IN ADDRESSING YEAR 2000 CONTINUES AT SLOW PACE

As our chart illustrates, since May 1997 OMB and the government's 24 largest departments and agencies have reported slow progress in achieving Year 2000 compliance of their mission-critical information systems.[6] In May 1997 OMB reported

---

[5]A listing of our publications is included as an attachment to this statement.

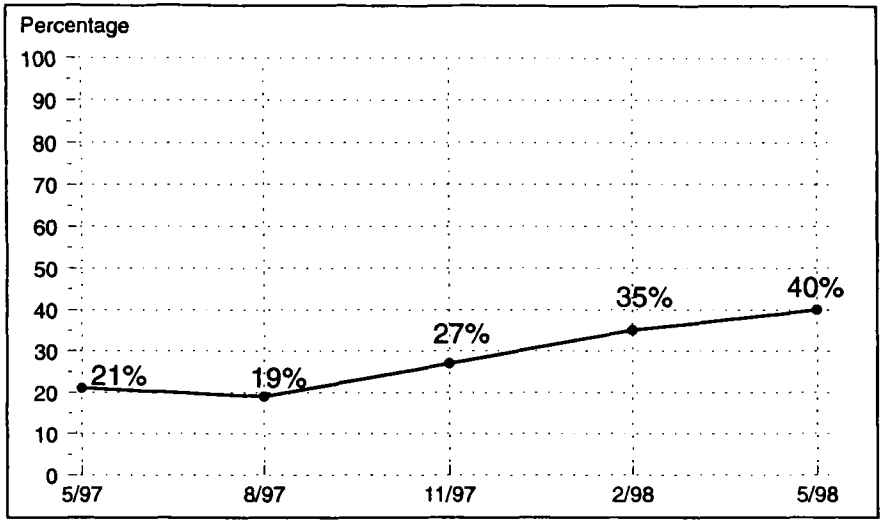
[6]OMB has required the following departments and agencies to report their Year 2000 readiness progress on a quarterly basis since May 1997: the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Housing and Urban Development, Interior, Justice, Labor, Transportation, Treasury, State, and Veterans Affairs; and the Agency for International Development, Central Intelligence Agency, Environmental Protection Agency, Federal Emergency Management Agency,

that about 21 percent of the government's mission-critical systems (1,598 of 7,649) were Year 2000 compliant.[7] A year later--as of last month--these departments and agencies reported a total of 2,914 systems as compliant--about 40 percent of the 7,336 mission-critical systems in their current inventories. Unless progress improves dramatically, a substantial number of mission-critical systems will not be Year 2000 compliant in time.

General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, and Social Security Administration. The Central Intelligence Agency's reports are classified.

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

Figure 1: Mission-Critical Systems Reported Year 2000 Compliant, May 1997-May 1998.



A great deal of work likewise remains for agencies to meet OMB's interim target dates for renovation and validation of systems (September 1998 and January 1999, respectively). For example, according to last month's agency reports, 9 have renovated less than 40 percent of their mission-critical systems due to be fixed, with 2 agencies having renovated less than 15 percent. This leaves little time for critical testing activities that leading organizations estimate will require at least 50 percent of total Year 2000 program time. As of last month, 16 of the 24 agencies reported that less than half of their systems requiring Year 2000 changes have completed validation.

Also of concern is that OMB, the President's Council on Year 2000 Conversion, and the Congress lack sufficient information with which to judge the progress of systems to be replaced. Agencies are not required to report on the status of specific mission-critical systems due to be replaced rather than renovated--more than 1000 systems (23 percent) of the government's noncompliant mission-critical systems--unless those systems are 2 months or more behind schedule. As we have been reporting, given the federal government's poor record of delivering new systems capabilities when promised, and the immutability of the Year 2000 deadline, these replacement efforts are at high risk; it is therefore essential that reliable information be available that accurately reflects agencies' progress in implementing replacement systems. Accordingly, we previously recommended that agencies report to OMB on their progress in implementing systems intended to replace noncompliant systems.[8]

Agencies will also need a significant amount of time for essential end-to-end testing of multiple systems that have individually been deemed Year 2000 compliant. Such end-to-end testing seeks to ensure that systems collectively supporting a core business function or area operate as intended. Without such testing, systems individually deemed as compliant may not work as expected when linked together with other systems in an operational environment. These systems include not only those owned and managed by the organization, but also any external systems with which they interface. For example,

---

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

the Federal Aviation Administration's Enhanced Traffic Management System monitors flight plans nationwide, controlling high-traffic situations and alerting airlines and airports to bring in more staff during times of extra traffic. Since it must exchange data with airlines' flight planning systems in order to accomplish this, end-to-end testing is essential, and would include systems for all entities involved, as well as their supporting telecommunications.

Last month's quarterly reports also disclosed other indicators that agencies and departments may not be operationally ready for the Year 2000. For example:

- Five agencies (the Departments of Defense, Health and Human Services, Justice, Transportation, and the Treasury) reported that they had not completed assessment of their systems--almost a year behind OMB's governmentwide target of June 1997. Because these departments have taken so long to assess the readiness of their systems, it will be increasingly difficult for them to renovate and fully test all of their mission-critical systems in time.
- Only 11 of the 24 agencies reported that they had completed inventories and/or assessments of their telecommunications systems. Without compliant telecommunications systems, agencies will find it extremely difficult to carry out basic operations.
- Only six of the agencies reported that they had completed inventories and/or assessments of their embedded systems. These are special-purpose computers built into other devices; they are important because many devices built or

renovated within the last 20 years use them to control, monitor, or assist in operations.

RISK OF YEAR 2000 DISRUPTIONS REQUIRES LEADERSHIP AND ACTION

As a result of federal agencies' slow progress, the public faces the risk that critical services could be severely disrupted by the Year 2000 computing crisis. Financial transactions could be delayed, airline flights grounded, and national defense affected. The many interdependencies that exist among the levels of governments and within key economic sectors of our nation could cause a single failure to have wide-ranging repercussions.

The February issuance of an executive order establishing the President's Council on Year 2000 Conversion was an important step in addressing these risks. The council Chair is to oversee federal agency Year 2000 actions as well as be the spokesman in national and international forums; coordinate with state, local, and tribal governments; promote appropriate federal roles with respect to private-sector activities; and report to the President--in conjunction with OMB--on a quarterly basis.

As we testified in March,[9] the council must take strong action to avert this crisis. In a report issued in April, we detailed specific recommendations.[10] We are encouraged by action taken in response to some of our recommendations. In other areas, however, the Chair has disagreed, and some actions have not been initiated.

The current Year 2000 progress reports of most large agencies reinforce the need for the council to implement these recommendations. At this point, I would like to review the major areas in which we continue to believe that action is essential, and update the Subcommittee on what has been done.

- *Priority Setting*. We previously testified that it was unlikely that all mission-critical systems could be made Year 2000 compliant in time.[11] We therefore recommended that the Chair of the Conversion Council establish governmentwide and agency-specific priorities for the most mission-critical business processes and supporting systems, using criteria such as the potential for adverse health and safety effects, adverse financial effects on American citizens, detrimental effects on national security, and adverse economic consequences.

---

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

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

[11]GAO/T-AIMD-98-101, March 18, 1998.

In response, the Chair stated that agencies have established priorities by identifying their mission-critical systems. He further said that the council's focus at this time should be to assist agencies as they work to ensure that all of their mission-critical systems are ready for the year 2000, adding that it may be necessary at a later date for agencies to further prioritize these systems.

This approach is inconsistent with the crisis nature of the problem and does not reflect the lack of progress of the 24 agencies in correcting their mission-critical systems. The most recent set of quarterly reports reinforces our view that the time to make difficult decisions and set priorities is now, while agencies can still correct, validate, and implement essential systems. If priorities are not clearly set, the government may find that less critical systems are compliant but that some of its highest priority functions are unavailable--but could have been corrected had appropriate resources and attention been properly focused earlier.

In contrast to our country's approach, Canada has established national Year 2000 priorities. Currently, it has 44 national priorities covering areas such as national defense, food production, safety, and income security. According to Canada's Year 2000 program director, Canada wants to ensure that, at a minimum, these priority areas are fully addressed in the time remaining before 2000.

- ***End-To-End Testing***. Agencies must also ensure that their mission-critical systems can reliably exchange data with other systems and that they are protected from errors that can be introduced by external systems. To achieve this goal, agencies must perform end-to-end testing for their critical core business processes. The purpose of end-to-end testing is to verify that a defined set of interrelated systems, which collectively support an organizational core business area or function, work as intended in an operational environment. For example, agencies that administer key federal benefits payment programs, such as the Department of Veterans Affairs, exchange data with the Department of the Treasury which, in turn, interfaces with various financial institutions to ensure that benefits checks are issued. In addition, Department of Defense systems interface with thousands of systems belonging to foreign military sales customers, private contractors, other federal agencies, and international organizations such as the North Atlantic Treaty Organization.

In the case of the year 2000, many systems in the end-to-end chain will have been modified or replaced. As a result, the scope and complexity of the testing--and its importance--is dramatically increased, as is the difficulty of isolating, identifying, and correcting problems. Consequently, agencies must work early and continuously with their data exchange partners so that end-to-end tests can be effectively planned and executed. We therefore recommended, for the selected priorities, that lead agencies be designated to take responsibility for ensuring that end-to-end operational testing of

processes and supporting systems is performed across organizational boundaries, and that independent verification and validation of such testing likewise be ensured.

In response to our recommendation, the Chair stated that agencies are currently developing such plans and obtaining independent verification and validation for their systems. He added that the council and OMB will monitor these activities and that if any difficulty arises in getting agencies to cooperate with respect to end-to-end testing, either he or OMB will intervene to resolve the matter.

Because time is short and thorough end-to-end testing of Year 2000-compliant systems and processes across organizational boundaries is essential to ensuring that services will be delivered, a more active approach is needed to ensure accountability and timely decision making. Unless responsibility is clearly assigned, it will be difficult to ensure that all organizations participate constructively and without delay. Further, the Conversion Council will also have to assume leadership and take whatever actions are warranted should difficulties arise in obtaining needed participation and cooperation from state and local governments and the private sector.

- ***Central Reporting Issues***. OMB's reports to the Congress--based on quarterly agency progress reports--have not fully reflected the true progress of the federal government toward Year 2000 systems compliance because not all agencies have been required to report and, further, OMB's reporting requirements have been incomplete. Accordingly,

we recommended (1) requiring that additional agencies that play a significant role, such as the Securities and Exchange Commission, also report quarterly to OMB; (2) requiring agencies to report on the status of their efforts to replace systems, not just on renovating those being fixed; and (3) specifying the particular steps that must be taken to complete each phase of a Year 2000 program (i.e., assessment, renovation, validation, and implementation).

OMB has acted on these recommendations. Specifically, on March 9 and April 21, 1998, OMB issued a memorandum to an additional 31 and 10 organizations, respectively, requiring that they provide information on their Year 2000 progress. The resulting reports from these organizations can further assist the Conversion Council, OMB, and the Congress in gauging progress to date, identifying risks, and raising additional issues. For example, the report submitted by the U.S. Postal Service shows that it plans to spend over $500 million on its Year 2000 effort and intends to implement its mission-critical projects by September 1998. However, the report also indicates that 21 percent of its 335 mission-critical systems are still in the assessment phase. This raises questions about whether the Postal Service's own target of this September is realistic.

In addition to requesting reports from other organizations, in its April 28, 1998, quarterly reporting guidance, OMB requested that agencies provide information on the oversight mechanism(s) used to ensure that replacement systems are on schedule. It also specified

that agencies should ensure that their reporting on the completion of phases is consistent with the CIO Council's best practices guidance and our enterprise readiness guide.[12]

While we acknowledge the actions that have been taken to improve the agency reporting process, it is clear that the progress of several major departments and agencies toward ensuring Year 2000 compliance continues to be insufficient. Accordingly, the Chair of the Conversion Council and OMB must begin requiring more frequent reporting, especially for those agencies not making sufficient progress. Such reporting would enable problems and delays to be surfaced more quickly so that necessary actions could be taken immediately. Accordingly, we now recommend that the Chair and OMB require, at an absolute minimum, monthly Year 2000 reports from those agencies not making sufficient progress.

▪ ***Business Continuity and Contingency Planning***. Business continuity and contingency plans should be formulated to respond to two types of failures: predictable (such as system renovations that are already far behind schedule) and unforeseen (such as a system that fails despite having been certified as Year 2000 compliant or one that, it is later found, cannot be corrected by January 1, 2000, despite appearing to be on schedule today). Therefore, agencies that develop contingency plans only for systems currently behind schedule are not addressing the need to ensure the continuity of even a minimal level of core business operability in the event of unforeseen failures. As a result, when

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

unpredicted failures occur, agencies will be without well-defined responses and may not have enough time to develop and test effective alternatives.

Moreover, contingency plans cannot focus solely on agency systems. Federal agencies depend on data provided by business partners, as well as services provided by the public infrastructure (e.g., power, water, transportation, and voice and data telecommunications). One weak link anywhere in the chain of critical dependencies can cause major disruptions to business operations. Given these interdependencies, it is imperative that contingency plans be developed for all critical core business processes and supporting systems, regardless of whether these systems are owned by the agency. Further, those program managers responsible for core business processes should take a leading role in developing business continuity and contingency plans because they best understand their business processes and how problems can be resolved. In this manner, business continuity and contingency planning generally complements, rather than competes with, the agency's Year 2000 remediation activities. Accordingly, we recommended that the Chair require agencies to develop contingency plans for all critical core business processes.

The Chair agreed. In addition, in March 1998 OMB clarified its contingency plan instructions,[13] stating that such plans should be developed for all core business functions.

---

[13]Progress on Year 2000 Conversion, U.S. Office of Management and Budget, as of February 15, 1998.

Moreover, OMB and the CIO Council adopted our draft guide providing information on business continuity and contingency planning issues common to most large enterprises as a model for federal agencies.[14] Further, in its April 28, 1998, instructions, OMB asked agencies to describe their processes and activities for developing such contingency plans.

Although these are positive steps, much work on contingency planning remains to be completed. In their May 1998 quarterly reports to OMB, only four agencies reported that they had drafted contingency plans for their core business processes.

▪ *Independent Verification*. OMB's assessment of the current status of federal Year 2000 progress is predominantly based on agency reports--reports that have not been consistently reviewed or independently verified. Without such independent reviews, OMB and the Conversion Council have little assurance that they are receiving accurate information.

We have, in fact, found cases in which agencies' systems conversion status as reported to OMB has been inaccurate. For example, the Department of Agriculture reported 15 systems as compliant, even though they were still under development or merely planned.[15] (The department plans to delete these systems from its list of compliant

---

[14]GAO/AIMD-10.1.19, March 1998 [exposure draft].

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

systems in its next quarterly report.) In another example, the Defense Finance and Accounting Service had not performed adequate testing to assert that certain systems it had reported as compliant were capable of transitioning into the year 2000. Specifically, managers of three systems reported as compliant indicated that they had performed some tests on the transfer and storage of dates, but had not completed all necessary Year 2000 compliance testing.[16]

Agencies' May 1998 quarterly reports describe current or planned verification activities, which include internal management processes, reviews by agency inspectors general, and contracts with vendors for independent verification and validation. While this has helped provide assurance that some verification is taking place, the full scope of verification activities required by OMB has not been articulated. Accordingly, we recommended that the Chair require agencies to develop an independent verification strategy to involve inspectors general or other independent organizations in reviewing agency Year 2000 progress.

The Chair agreed that independent assessments of agencies' Year 2000 programs and their testing and planning approaches are important, and stated that he and OMB will consider issuing more explicit directions to agencies on independent verification,

---

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

especially with regard to establishing standards for the type of verification and evaluation desired. We are not aware that any such directions have yet been issued.

▪ *Workforce Issues*. Obtaining and retaining adequate and skilled staff for the Year 2000 challenge has been an increasing concern. In their current quarterly reports, 10 of the 24 agencies and departments describe problems that they or their contractors have encountered in obtaining and/or retaining information technology personnel. However, no governmentwide strategy has existed to address recruiting and retaining information technology personnel with the appropriate skills for Year 2000-related work. Accordingly, we recommended that the Chair of the Conversion Council develop a personnel strategy to include (1) determining the need for various information specialists, (2) identifying needed administrative or statutory changes to waive reemployment penalties for former federal employees, and (3) identifying ways to retain key Year 2000 staff in agencies through the turn of the century.

The Chair agreed. On April 30 he stated that the Council would be working with several agencies, including the Office of Personnel Management (OPM), to examine options for ensuring an adequate number of qualified people to perform Year 2000 work. One specific action was taken on March 30, when OPM issued a memorandum stating that the Year 2000 problem was an "unusual circumstance" that would allow it to grant agencies waivers to allow them to rehire former federal personnel on a temporary basis without financial penalty. The memorandum also advised agencies of their ability to

make exceptions to the biweekly limitation on premium pay when the head of an agency or designee determines that an emergency involving a direct threat to life or property exists. In addition, the Council has formed a Year 2000 workforce issues working group chaired by the Deputy Secretary of Labor. We have an ongoing review focused on assessing overall Year 2000-related personnel issues.

▪ *The Nation's Year 2000 Status*. Beyond the federal government, no one knows the overall extent of our nation's vulnerability to Year 2000 risks, or the extent of our readiness. No nationwide assessment that includes the private and public sectors has been undertaken to gauge this. Accordingly, we recommended that the Council orchestrate a broad assessment of the nation's Year 2000 readiness, to include identifying and assessing the risks of the nation's key economic sectors, including risks posed by international linkages and by the failure of critical infrastructure components. Although the Chair did not directly address this recommendation in his response to our report, we are aware that the council has no plans to develop such an assessment. Without a nationwide assessment of the nation's Year 2000 status, the council will not be in a well-informed position to identify or prioritize areas of weakness and develop mechanisms to solve or mitigate those weaknesses.

Also, a coordinated, public/private effort, under the leadership of the executive branch, could provide a forum and bring together the major players in each key economic sector to effectively coordinate the nation's Year 2000 efforts and ensure that all sectors, as well

as sector interdependencies, are being adequately addressed. Further, public/private forums, under the direction and oversight of the Conversion Council, could be instrumental in developing business continuity and contingency plans to safeguard the continued delivery of critical services for each key economic sector. While we do not foresee the federal government as dictating policy or requiring specific solutions, it is, however, uniquely positioned to publicize the Year 2000 computing crisis as a national priority; take a leadership role; and identify, assess, and report on the risks and necessary remediation activities associated with the nation's key economic sectors. Such plans would be all the more effective because they would bring to bear the combined and considerable influence of the federal government, state and local governments, and the private sector.

Although the Chair agreed that the Conversion Council should view the Year 2000 crisis as more than a federal systems problem and should adopt a global perspective, he disagreed with our recommendation to establish a national coordination structure using public/private partnerships in appropriate sector-based forums. He stated that the Council needs to be a catalyst, facilitator, and coordinator, but not creator and direct manager of new national forums for specific sectors of the economy.

Nevertheless, in April and May 1998, the Chair established five working groups (telecommunications, energy, financial institutions, emergency preparedness, and workforce issues) composed of federal agencies. In addition, he has identified 29 sectors

headed by federal agency sector coordinators. The Chair has not provided these groups with formal, written guidance, objectives, or expectations. He has, however, told them to focus on developing a coordinated outreach plan and establish communications with public and private parties within each sector, and to monitor the Year 2000 readiness of each sector. In order for these outreach efforts to be fruitful, the working groups and coordinators will need accurate and complete information on the Year 2000 status and plans of these sectors.

It will not be enough for the Conversion Council to act as catalyst, facilitator, and coordinator. The council must also posture itself to provide Year 2000 leadership for the nation as a whole. To provide such leadership, the council must develop an approach to receiving the best guidance directly from the private sector and state and local government bodies, in addition to views and perspectives garnered by federal agency executives.

- - - - -

In summary, as the amount of time to the turn of the century shortens, the magnitude of what must be accomplished becomes more daunting. Greater leadership and coordination of disparate efforts is essential if government programs are to meet the needs of the public 19 months from now. The Conversion Council must play a central role in ensuring that agency action not only stays on track, but accelerates significantly.

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

GAO REPORTS AND TESTIMONY ADDRESSING THE YEAR 2000 CRISIS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

National Weather Service: Budget Events and Continuing Risks of Systems Modernization (GAO/T-AIMD-98-97, March 4, 1998)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

USDA Information Management: Extensive Improvements Needed in Managing Information Technology Investments (GAO/T-AIMD-97-90, May 14, 1997)

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

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

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

(511460)

Mr. HORN. We now go to Mr. Callahan, John Callahan, who is Assistant Secretary, Management and Budget, Department of Health and Human Services. Welcome.

STATEMENT OF JOHN CALLAHAN, ASSISTANT SECRETARY, MANAGEMENT AND BUDGET, DEPARTMENT OF HEALTH AND HUMAN SERVICES

Mr. CALLAHAN. Chairman Horn, thank you for inviting us here today. I have submitted a written statement for the record and would make a brief oral statement summarizing my testimony.

I would like to make six main points about the Department's efforts to make our computer systems millennium compliant.

First, accountability; we welcome the scrutiny and oversight of the subcommittee. We will be fully accountable to you and to the President and Vice President on year 2000 compliance. Your oversight is both proper and necessary. We have a full system of accountability in the Department, running from the Chief Information Officer in each agency to that agency's head, to me, the Deputy Secretary, and the Secretary.

Second, funding; making our computer systems year 2000 compliant is costly. This year already we are in the process of channeling an additional $61 million to HCFA for its work with Medicare contractors for their year 2000 compliant efforts.

We are continuing to reexamine fiscal year 1999 year 2000 budget requests, and we are mindful of the Senate setting aside $3.25 billion in emergency appropriations for that purpose. It will be our job to make sure that agencies realistically budget for their compliance efforts.

Third, personnel; HHS was the first agency to seek OPM approval for the hiring of retired civil servants to do year 2000 work. Already we have hired nine retirees at HCFA and have suitable authorization to hire more at agencies that require such personnel. Furthermore, we are prepared to consider moving among our agencies key computer personnel from agencies that have completed their year 2000 work to ones that have not.

Fourth, and this is a point that Congressman Kucinich mentioned, the legal authority to do the year 2000 job. Here, the main concern that we have is that Congress consider and pass the Medicare contractor legislation that has been forwarded to you in February and, more recently, in May. This will help HCFA work more aggressively with Medicare contractors in making their external systems year 2000 compliant. In the future, it will broaden the number of processing providers that HCFA can turn to for efficient and timely processing of Medicare claims. This legislation has the strong backing of the administration as well as the backing of the President's year 2000 counselor, Mr. John Koskinen.

Fifth, outreach; the Department has supplied information on all its State data exchanges to the National Association of State Information Resource Executives. These data exchanges, as well as our local government and private sector data exchanges, have been fully identified and will be tested for year 2000 compliance.

The Department has also, as you know, posted an FDA web site which provides pertinent and timely information on the compliance status of medical devices. We are now working with all our agen-

cies to have them establish year 2000 web sites and to engage in aggressive outreach with their stakeholders and service providers to alert them to their need to make their computer systems millennium compliant.

Finally, and most importantly, contingency plans and independent validation and verification contractors. All our agencies have IV&V contractors or internal IV&V efforts on hand and are making arrangements for year 2000 testing of their data and computer systems. As Department Chief Information Officer, I will have full and complete access to these IV&V reports so that progress on our year 2000 efforts can be validated.

Also, we are due to receive all agency year 2000 contingency plans on June 15. It will be our intention to analyze these plans closely and to put them into effect when we believe that we cannot meet our year 2000 deadlines. It is most important, as you and others have recognized, to make a seamless transition into the millennium, even in the event that some of our systems may not be year 2000 compliant.

In short, accountability, adequate funding, provision of personnel, strengthened legal authority, constructive outreach, strong validation, and suitable contingency planning are the basic elements of our year 2000 effort. We will strive to do our best in all these areas, and we will be fully accountable to the President, to the Congress, and to this subcommittee for all our year 2000 work.

Thank you. That concludes my oral statement, and I will be happy to answer any questions the subcommittee might have.

Mr. HORN. Thank you very much.

[The prepared statement of Mr. Callahan follows:]

INTRODUCTION

Good morning. I am John Callahan, Assistant Secretary of the Department of Health and Human Services for Management and Budget (ASMB) and Chief Information Officer (CIO). I am pleased to appear before this Subcommittee to provide you with a report on the accomplishments and the challenges faced by the Department of Health and Human Services (HHS) in assuring that our systems are Millennium compliant.

The Secretary, the Deputy Secretary, and I have declared the Year 2000 date issue to be our highest information technology priority. We have taken and will continue to take actions to ensure that HHS information systems are Year 2000 compliant.

We have involved all parts of our organization, including staff with expertise in information systems, budget, human resources, and acquisition management in solving the Year 2000 problem. No matter what else we do and what other initiatives we undertake, we must ensure that our ability to accomplish the Department's mission is not impaired.

For this reason, we have established December 31, 1998 as our internal deadline for Year 2000 compliance of mission critical systems. This was done in order to provide a full year of operations in which to detect and remedy any adverse interactions among HHS systems and those of our many service partners, including other Federal agencies, states and local governments, tribes, and contractors.

MISSION CRITICAL SYSTEMS REASSESSMENT

In order to better focus HHS remediation efforts on the most highly critical systems, we asked the Operating Division (OPDIV) Chief Information Officers (CIOs) to provide a brief synopsis of each mission critical system, and where warranted, to reclassify those systems that were not truly mission-critical, either because they were only of local importance with no critical interfaces, or because they were originally misclassified . We believe the reclassification will improve our ability to ensure that the HHS OPDIVs concentrate primarily on the systems that help us to serve the most people, most especially those that pay Medicare claims and issue grant payments.

The system reclassifications are reflected in our May Quarterly Report to OMB. In the February Quarterly Report, HHS listed the original inventory of 491 mission critical systems. Of these, 187, or 38%, were Year 2000 compliant. Had we continued with this base, our compliance would have been 42 % for the quarter ending March 31.

As a result of system reclassification, we are now reporting 289 mission critical systems, a reduction of 202 systems. Of these systems, 98, or 34%, were compliant as of the quarter ending March 31. I am pleased to report that HHS has made an additional 10 mission critical systems compliant since the reporting period ending March 31. ACF has added seven compliant systems, HCFA has added two compliant systems, and CDC has added one compliant system. This brings our total compliance to 108 of 289 systems, or 37%. We will continue to monitor the HHS OPDIVs' progress closely, using our monthly reporting system to ensure that our OPDIVs are continuing to improve the rate of system compliance and to ensure that system remediation efforts remain on schedule.

Based on the May 15 quarterly report, above average performance in the compliance of mission critical systems is reported by SAMHSA, which is 80% compliant; FDA is 51.5% compliant, CDC is 58.5% compliant HRSA is 60% compliant, and NIH is 50 % compliant.

HHS' YEAR 2000 EFFORT

To meet our Year 2000 responsibilities, we have taken a series of strong administrative actions. We have encouraged aggressive reallocation of funds, where necessary, to meet Year 2000 deadlines; we have established direct reporting lines between staff working on year 2000 activities and the Operating Division (OPDIV) Chief Information Officers. Each OPDIV CIO is responsible for regular reporting on Year 2000 efforts directly to the OPDIV head and to me, until Year 2000 date compliance is achieved.

In addition, our OPDIVs have compiled complete inventories of their system interfaces, and have contacted their interface partners. I provided a listing of state interfaces to the National Association of State Information Resources Executives (NASIRE). As decided at the April 22 meeting with NASIRE, we will provide an update of our state interfaces inventory to the General Services Administration for posting to their Year 2000 web site. We will provide monthly updates thereafter.

Because testing, including independent verification and validation (IV&V), is critical to our Year 2000 effort, we are requiring our OPDIVs to subject their systems to stringent testing and IV&V. We also know there is a possibility that, try as we might, some systems may not be fully compliant in time. Therefore, we are requiring the OPDIVs to develop contingency plans which we will receive on June 15, 1998. These plans will provide us with the operational policies needed to permit business continuity in the event of system failure.

The Deputy Secretary has asked all OPDIVs to prepare contingency plans based on the GAO guide entitled, "Year 2000 Computing Crisis: Business Continuity and Contingency Planning." We will analyze the OPDIV contingency plans carefully, and the fiscal, personnel, and operational dimensions of the plans will be fully developed with a timetable for parallel implementation of these plans if necessary.

In addition, we require all of the OPDIVs to perform Independent Verification and Validation (IV&V) for all mission critical systems to help ensure that the systems will function properly in the Year 2000. Our OPDIV, have made arrangements for IV&V, whether through the use of contractors or independent (out of the system managers' chain of command) in-house IV&V. FDA, NIH and the PSC are using a combination of contractor support and in-house resources. HCFA is using an outside contracter to do IV&V. In addition, OPDIVs are actively testing their systems. Four of six Medicare standard systems maintainers have begun to conduct future date testing.

We are taking action to retain, reemploy, and attract qualified information technology professionals, using both employment and contracting authorities. On March 31, we received Department-wide personnel authorities from the Office of Personnel Management (OPM) to waive the pay and retirement reduction for reemployed military and civilian retirees who return to work on Year 2000 remediation. To date, HCFA, has used the waiver authority to reemploy nine annuitants. HCFA also is reaching out to provider groups to help them understand the importance of this issue, since provider information systems must also be Year 2000 compliant in order to interface correctly with HCFA's.

HEALTH CARE FINANCING ADMINISTRATION CHALLENGES

Our greatest Year 2000 challenge is for HCFA's Medicare program. This program employs nearly seventy external contractors, including several shared systems maintainers, who operate and maintain a base of software programs that process 900 million fee-for-service claims payments annually for nearly 39 million Medicare beneficiaries. 75 percent of the external Medicare contractors have completed assessments of their systems. Even so, under the current law (Title XVIII of the Social Security Act) HCFA has limited authority for addressing the Year 2000 threat to Medicare systems. This situation illustrates why Medicare contracting reform has been and continues to be a Department and Administration priority. There are a number of facets to HCFA's current contracting authority that hinder HCFA's ability to require Year 2000 compliance.

Medicare claims processing contract terms are unique and differ in several important respects from typical Federal contracts awarded under Federal Acquisition Regulation. Medicare statutes require HCFA to contract for services with insurance companies only -- not computer or transaction processing firms -- and only on a cost reimbursement basis.

Intermediary and carrier contracts provide for automatic renewal on an annual basis. Furthermore, HCFA may terminate a contract only for cause and not for convenience, while contractors may leave the Medicare program with 180 days notice. It generally takes HCFA six to nine months to transfer a contractor's workload to another contractor organization.

Most importantly, because HCFA is required to reimburse its Medicare contractors for all allowable costs, the agency's ability to exert financial leverage over its contractors to direct funds toward such activities as Year 2000 compliance is limited.

HCFA has been proactive in addressing Year 2000 risks with its Medicare contractors. HCFA has proposed amendments to Medicare contracts requiring millennium compliance, and has released guidance that would provide more restrictive definitions of compliance and testing requirements. Nonetheless, we remain committed to achieve a faster pace of progress by Medicare contractors in meeting our Year 2000 goal.

As I stated earlier, problems surrounding Year 2000 compliance are an illustration of why the Administration has proposed contracting reform legislation. On February 27, 1998, and again on May 18, 1998, HHS submitted Medicare contractor reform legislation to Congress. This legislation would amend the Medicare statute regarding HCFA-contractor relations. This proposal would provide the Secretary with greater flexibility for managing the Medicare program, and allow increased discretion in contracting for claims processing and payment functions. Under this authority, the Secretary could award contracts from a larger pool of qualified contractors. We believe that this change would promote competition and potentially allow the Medicare program to obtain better value for its dollar. The new authority would also be especially helpful in allowing the Secretary to implement contingency planning that permits business continuity in the event of system failure. This proposal has received the endorsement of John Koskinen, Special Assistant to the President for Year 2000, in testimony before the Senate Governmental Affairs Committee.

The proposal would allow the Secretary to contract for Medicare functions on a best value basis as permitted by the Federal Acquisition Regulations (FAR). It would change Medicare law to permit the Secretary to follow the FAR in administrative contracting. We would then be able to determine on a case-by-case basis the most appropriate contractual arrangements, with fixed price and incentive provisions, for example.

Prompt consideration and passage of this legislation now will provide HCFA with greater leverage to proactively manage Medicare contractors.

We recognize that HCFA will continue to face a time-consuming and difficult that contractor reform alone cannot alleviate. As noted earlier, this will require additional resources to be used for contractor Year 2000 remediation, or testing and independent verification and validation. In early May, the President signed a 1998 supplemental appropriations bill directing $20 million of HCFA contractor funds to be redirected toward HCFA's Year 2000 remediation efforts.

While these funds will certainly help, HCFA still must find ways to address the shortfall. We estimate that HCFA will require additional Year 2000 funding in FY 1998 and FY 1999. In FY 1998, HCFA estimates it needs an additional $41 million. In FY 1999, HCFA may require an

additional $61 million for HCFA contractor remediation efforts. On May 29, we sent a letter to Congress notifying you of our intent to use the Secretary's one-percent authority to shift funds from other HHS activities to make the additional $41 million available for HCFA's Year 2000 efforts. While cutting funding for other activities is never easy, and all may not be happy with our choices for offsets, we would appreciate Congress' support for our effort to give HCFA the resources necessary to address this problem.

BIOMEDICAL EQUIPMENT OUTREACH EFFORTS

Our Year 2000 related activities are not limited solely to HHS programs alone. On January 21, 1998, Deputy Secretary Kevin Thurm signed a letter, sent to over 16,000 biomedical equipment manufacturers, strongly urging them to identify noncompliant products, and the actions they are taking to ensure compliance. The manufacturers are now responding to this survey developed by my office and the Food and Drug Administration (FDA). The FDA now operates and maintains a public Internet web site listing all biomedical equipment information received from the manufacturers relating to Year 2000 compliance. The web site is operational and FDA is currently posting the manufacturer responses on the Internet. This site can be accessed at **http://www.fda.gov/cdrh/yr2000.** The FDA is currently aggressively following up with manufacturers to improve the current low rate of response.

We are planning additional outreach activities, beyond the biomedical equipment issues, to inform the health and human services community in general about Year 2000 issues.

HHS also chairs two Year 2000 Conversion Council sector outreach groups. We are formulating outreach plans for the health care sector and the human services sector. We also serve as members on several other sector groups, including benefits payments, education, emergency management, food supply, science and technology, and health care and social assistance.

CONCLUSION

HHS faces substantial challenges in our Year 2000 efforts. However, let me assure you, on behalf of Secretary Shalala and Deputy Secretary Kevin Thurm, that we will continue to vigorously pursue Year 2000 remediation as our most important information technology initiative.

We recognize our obligation to the American people to assure that HHS' programs function properly now and in the next millennium.

I thank the Committee for its interest and oversight on this issue, and would be happy to answer any questions you may have.

Mr. HORN. Our next speaker is familiar with this committee, Mr. Marshall Smith, the Acting Deputy Secretary, Department of Education. Mr. Smith.

STATEMENT OF MARSHALL SMITH, ACTING DEPUTY SECRETARY, DEPARTMENT OF EDUCATION

Mr. SMITH. Thank you, Chairman Horn. I have submitted my written testimony for the record, and I would just like to give some short oral testimony to reinforce some of the issues.

I thank you for this opportunity to discuss our efforts to address the year 2000 problem. I want to begin, really, by emphasizing that we take very seriously this problem and the destruction it could create, both for the Department in the services that we provide and for our many partners and customers in a variety of different services throughout the education system.

The Department has developed a comprehensive year 2000 management plan based on the five-stage strategy recommended by the General Accounting Office: awareness, assessment, renovation, validation, and implementation. We have fully completed the awareness and assessment phases and are moving rapidly through the renovation and validation phases.

The awareness phase included the creation of a high-level year 2000 Steering Committee, which I chair, and a Departmentwide work group that includes principal office coordinators. We have hired Booz-Allen & Hamilton, a consulting firm, to help guide our year 2000 efforts and to serve as independent verifiers, and we regularly seek advice from the Department's inspector general, who is actively involved in this effort with us, particularly in the area of ensuring a sufficiently independent validation and verification process.

The assessment phase involved an agencywide inventory that identified 14 mission-critical systems that could cause the immediate failure of core Department business functions, if not year 2000 compliant. These include the delivery and oversight of roughly $45 billion in student financial aid every year.

We have also classified 25 systems as mission-important and 137 systems as mission-supportive. Failure of any of our mission-important systems could cause mid- to long-term failure of Department business functions, while the lower-risk mission-supportive systems enhance the effectiveness or efficiency of day-to-day operations but are not essential to core business functions.

To ensure that all our mission-critical systems are year 2000 compliant, we have established a firm schedule for the renovation and validation phases for our year 2000 projects, and we have contracts in place to support all of this work. The chart at the back of my written testimony highlights our progress. One-half of our mission-critical systems are in the validation phase, and we will complete renovation of all of the remaining systems by the September 1998, OMB milestone. Nine of fourteen have completed renovation today.

The chart also shows that we will complete validation implementation for 13 of the 14 mission-critical systems by January 1999, ahead of the March 1999, OMB milestone. I might mention that we have increasing confidence in these charts. We have detailed mile-

stones for each of the systems; and as we successfully meet each of the phases, it increases our belief that we can make these deadlines easily and exceed some of the deadlines. That is, coming inside them. This will allow nearly a full year to ensure that all renovated systems are running smoothly prior to January 1, 2000.

The remaining mission-critical system, the FFEL, the Federal Family Education Loan program system, is on schedule for completion by March 1999. We also are making good progress on our remaining systems. Twenty-five mission-important systems and 137 mission-supportive systems are on or ahead of schedule to meet the OMB milestones.

Many of our systems rely on accurate data exchanges, both internally and with outside partners. We have a complete inventory of these data exchanges, the most critical of which involve the Department's core financial management system. Most of the financial data exchanges, including those with other Federal agencies, are already year 2000 compliant. Those that are not will be repaired well within the OMB milestones. We will be conducting end-to-end tests of all our data exchanges to ensure year 2000 compliance.

In addition to our compliance efforts, the Department is developing contingency plans for all 14 mission-critical systems and for any mission-important system that could be at risk, if not in compliance, as a precaution against mission failure that may occur despite the best efforts of the Department and its contractors. We will complete our review of draft contingency plans this month.

The Department is actively reaching out to its many partners to raise their awareness of the year 2000 issues. Last year, I joined the executive director of the Council of Chief State School Officers in sending out a Dear Colleague letter to the chief state school officers and the deputy chief state school officers in all 50 States, the District of Columbia, and the territories.

In addition, we have just completed a joint letter on year 2000 to the National School Boards Association, which I will sign and the executive director of the National School Boards Association will sign, that will go out to some 15,000 school districts nationwide. We figure that we ought to reach the fiscally responsible parties in these matters, and the school board chair people are those parties.

The postsecondary level Department training sessions for student financial aid professionals, which will reach up to 6,000 participants, now include a year 2000 module. Department officials are also discussing year 2000 compliance at 39 national and regional conferences.

More generally, the Department has distributed over 20,000 copies of a brochure establishing a year 2000 web site and joined with other Federal agencies to coordinate outreach as part of the President's Council on Year 2000 Conversion.

In spite of these efforts, Mr. Chairman, we remain concerned by preliminary survey results showing that, while some schools are already year 2000 compliant, or claim they are, others appear to be entirely unaware of the problem. This is why I encourage you and members of this subcommittee, along with your colleagues in the

House and Senate, to raise the year 2000 issue whenever you visit school districts and postsecondary institutions back home.

The subcommittee can also help by supporting the appropriations needed to ensure the success of the Department's year 2000 project. We are requesting $12 million in fiscal year 1999 to pay year 2000 related costs.

Much work remains, but I believe the Department is on track. We are implementing a comprehensive plan for ensuring our systems are year 2000 compliant within the milestones established by OMB; developing contingency plans on the outside chance that something goes wrong; and we are working to make sure our partners are as prepared as we are for the arrival of the next century.

Thank you, and I will be happy to answer any questions.

Mr. HORN. Well, thank you very much. That is a very helpful statement that we will get back to.

[The prepared statement of Mr. Smith follows:]

Mr. Chairman and Members of the Subcommittee:

Thank you for this opportunity to discuss the Department of Education's efforts to address the Year 2000 problem. I want to begin by emphasizing that we are taking very seriously the Year 2000 problem and the disruption it could create, both for the Department and for our many partners and customers throughout our education system. Achieving Year 2000 compliance is a big challenge for the Department, but we have put in place a comprehensive plan to meet this challenge and I am confident that we will get the job done.

THE DEPARTMENT'S YEAR 2000 PLAN

We are aware of the poor grade the Department's Year 2000 efforts have received from this Subcommittee, as well as placement on OMB's "watch list" for not meeting certain milestones toward Year 2000 compliance. In response, the Department has developed a comprehensive Year 2000 Project Management Plan that includes clearly defined organizational roles and responsibilities, reporting and monitoring processes, and budget plans. We are following the five-phase strategy recommended by the General Accounting Office: awareness, assessment, renovation, validation, and implementation. We have completed the awareness and assessment phases and are moving rapidly through the renovation and validation phases.

The awareness phase included the creation of a high-level Year 2000 Steering Committee, which I chair, and which includes the Chief Financial and Chief Information Officer, the Year 2000 Project Director, and other key managers. We also have established a

Department-wide Year 2000 work group that brings together Principal Office Coordinators and is supported by the outside management consulting firm Booz-Allen & Hamilton. In addition, we regularly seek the advice of the Department's Inspector General on our Year 2000 strategy, particularly in the area of ensuring a sufficiently independent validation and verification process.

The assessment phase involved an agency-wide inventory—using methodology developed by Booz-Allen & Hamilton—that identified systems potentially affected by the Year 2000 problem and assigned them to risk categories. We identified 14 mission-critical systems that could cause the immediate failure of core Department business functions if not Year 2000 compliant. We have also classified 25 systems as mission-important and 137 systems as mission-supportive. Failure of any of our mission-important systems could cause mid- to long-term failure of Department business functions, while the lower-risk mission-supportive systems enhance the effectiveness or efficiency of day-to-day operations but are not essential to core business functions.

Of the 14 mission-critical systems, 11 are involved in the administration of the student financial assistance and student loan programs. These systems fully reflect the size and complexity of the Federal student aid enterprise, under which the Department of Education works with 6,000 postsecondary institutions, 4,800 lenders, 36 guaranty agencies, and State higher education agencies to deliver nearly $50 billion in financial assistance to 8.5 million postsecondary students. With such a large number of players and so much at stake for millions

of students and their families, this is clearly a high-risk area. We are taking great care to prevent any disruption to these essential systems and the programs they support.

ON SCHEDULE TO ACHIEVE COMPLIANCE

We have established a careful and systematic schedule for the renovation and validation phases of our Year 2000 project, and we have contracts in place to support this work. The attached chart on the status of our mission-critical systems highlights our progress. One-half of our mission-critical systems are in the validation phase, and we will complete renovation of the remaining systems by the September 1998 OMB milestone.

The Department has hired Intermetrics and Booz-Allen & Hamilton to perform the crucial independent validation and verification tasks—with oversight from the Inspector General—for our mission-critical systems. We will complete validation and implementation for 13 of the 14 mission-critical systems by January 1999, ahead of the March 1999 OMB milestone and allowing nearly a full year to ensure that all renovated systems are running smoothly prior to January 1, 2000. The remaining mission-critical system—the Federal Family Education Loan Program System—is on schedule for completion by the March 1999 OMB deadline.

We also are making good progress on ensuring Year 2000 compliance for our remaining systems. The 25 mission-important systems and 137 mission-supportive systems are on or ahead of schedule to meet the OMB milestones.

CONTINGENCY PLANS—JUST IN CASE

In addition, the Department is developing contingency plans for all 14 mission-critical systems, and for any mission-important systems that are determined to be at risk of non-compliance, as a precaution against system failures that may occur despite the best efforts of the Department and its contractors. We will complete our review of draft contingency plans this month.

REACHING OUT TO OUR PARTNERS AND CUSTOMERS

The Department is actively reaching out to its many partners—including 6,000 postsecondary institutions and 4,800 lenders that provide student loans, 15,000 local educational agencies, and State education agencies—to raise their awareness of Year 2000 issues. For example, last January I joined the Executive Director of the Council of Chief State School Officers in sending a Dear Colleague Letter to the Chief and Deputy Chief State School Officers in all 50 States, the District of Columbia, and the territories.

We also have coordinated a joint letter with the National School Boards Association that will go out to some 15,000 school districts nationwide. In addition, the Department has distributed over 20,000 copies of a brochure on the Year 2000 problem, established a Year 2000 web site (which received 15,000 hits over the past two months), and opened Year 2000 mailboxes to answer questions.

In the student financial aid area, we have contacted all major organizations about the Year 2000 problem. We sent out Year 2000 technical specifications to all higher education institutions in November 1997, and we will provide Year 2000 compliant student financial assistance software to all postsecondary institutions by January 1999. In addition, Department training sessions for student financial aid professionals—which will reach up to 6,000 participants—now include a Year 2000 module. Department officials also will discuss Year 2000 compliance at 39 regional and national conferences of the National Association of Student Financial Aid Administrators, which includes representatives from about 3,300 postsecondary institutions.

We now have a complete inventory of data exchanges, the most critical of which involve the Department's core financial management system—the Education Central Automated Processing System, or EDCAPS—and the student financial aid programs. For example, the Department's Pell Recipients Financial Management System tells EDCAPS how much money individual postsecondary institutions should receive to cover Pell Grants for eligible students.

Most EDCAPS data exchanges, including those with other Federal agencies, are already Year 2000 compliant; those that are not will be repaired within the OMB milestones. We also are working with the General Services Administration to make sure that centrally provided services like telephones and elevators are Year 2000 compliant.

Finally, as part of the President's Council on Year 2000 Conversion, we have joined with a number of other Federal agencies to coordinate outreach to key sectors of the Nation. For example, the Department is chairing a work group of Federal agencies that are targeting the education sector. We also are involved in two other White House work groups: one focused on Year 2000 preparations in the financial sector and another looking at ways to meet the demand for skilled professionals to work on the Year 2000 problem.

In spite of this wide range of outreach efforts, Mr. Chairman, we remain concerned about the Year 2000 readiness of many of our partners at the elementary, secondary, and postsecondary levels. This is why I encourage you and the Members of this Subcommittee, along with your colleagues in the House and Senate, to raise the Year 2000 issue whenever you visit school districts and postsecondary institutions back home. We know from data that we have gathered as part of our outreach efforts that many districts and institutions are at risk of major disruption when January 1, 2000 arrives. It is critical to raise awareness of the Year 2000 problem across the Nation, and Members of Congress can do much to help in that effort.

This Subcommittee can also help by supporting the appropriations needed to ensure the success of the Department's Year 2000 project. We are requesting $12 million in fiscal year 1999 to pay Year 2000-related costs.

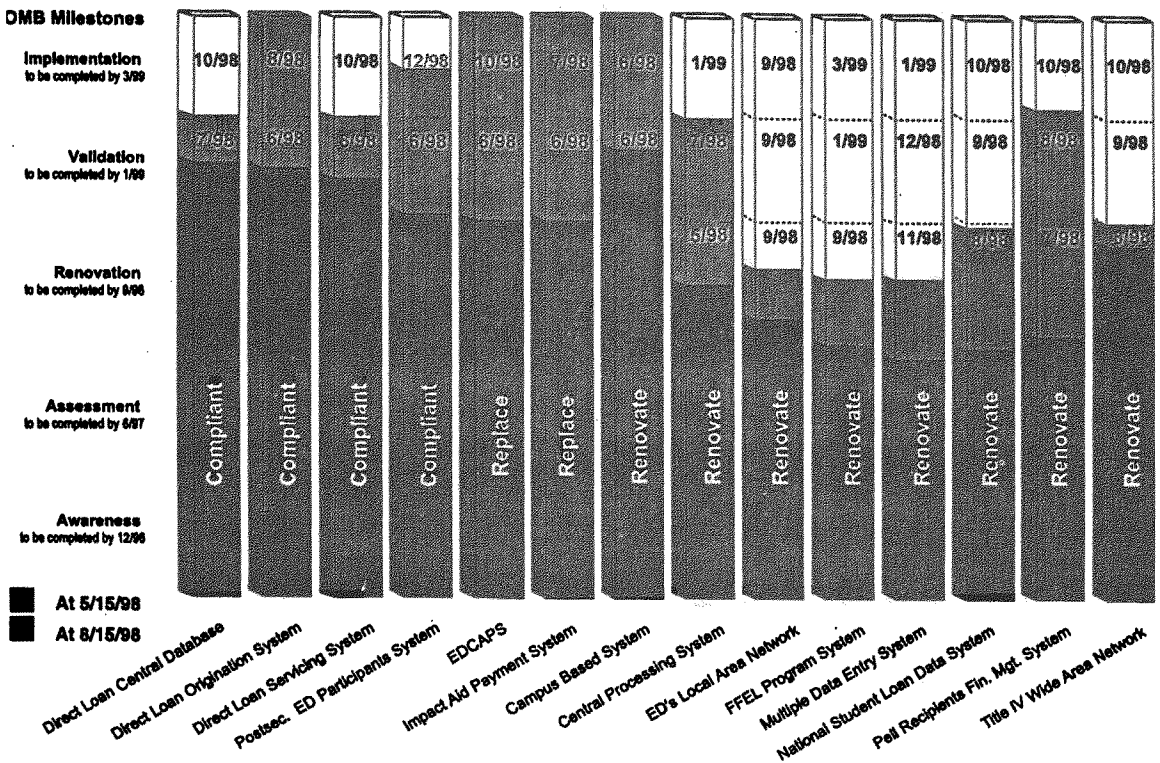
CONCLUSION

Much work remains, but I believe the Department is on track. We are implementing a comprehensive plan for ensuring that our systems are Year 2000 compliant within the milestones established by OMB, we are developing contingency plans on the outside chance that something goes wrong despite our best efforts, and we are working to make sure our partners and customers are as prepared as we are for the arrival of the next century.

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

Department of Education Year 2000 Compliance Project

Status of Mission Critical Systems as of 5/15/98 and 8/15/98



Mr. HORN. Mr. William Curtis is the Special Assistant for the year 2000, the Command, Control, Communication and Intelligence group of the Department of Defense.

Mr. Curtis.

STATEMENT OF WILLIAM CURTIS, SPECIAL ASSISTANT FOR THE YEAR 2000, COMMAND, CONTROL, COMMUNICATION AND INTELLIGENCE, DEPARTMENT OF DEFENSE

Mr. CURTIS. Good morning, Mr. Chairman and members of the committee. I am delighted to be here.

Chairman Horn, you and your subcommittee should be commended for your foresight and vigilance in bringing public awareness to this very real threat to our social and information infrastructure.

Mr. HORN. I might add that when people say they are delighted to be here, I usually remind them that they did take an oath to tell the truth.

Mr. CURTIS. Yes, sir, but in this case I am, because you are going to be a big help to me, sir.

Mr. HORN. As the shill or what?

Mr. CURTIS. I'm crazy, sir.

I have submitted a statement for the record, and I would like to make some additional comments.

First chart. Mr. Chairman, I was appointed as DOD Y2K special assistant about 60 days ago. I have read all the reports and your assessments and, fundamentally, I agree with all their findings. I got called to do a tough job. DOD has about 2,800 mission-critical systems, and we are at least 4 months behind.

Second chart. Mr. Chairman, DOD is using the GAO approved five-phased approach. DOD has a three-prong strategy to strengthen our Y2K efforts: first, improved report and evaluation; second, expanded programmatic oversight and coordination; and, third, enterprise-wide test and contingency planning. DOD's goal is to be operation capable to defend this Nation on January 1.

Next chart. DOD understands that Y2K is a global, multidimensional problem which cuts across organizational and functional boundaries. DOD faces a complex environment, with thousands of interfaces with Government agencies, commercial industry, our suppliers and trading partners, State and local governments and our allies. As Senator Bennett has said, we must focus on the whole enterprise.

We are running interface assessment workshops every 60 days in each of the 20 functional areas, cutting across all military services and defense agencies. We are involved with 18 of the 32 sectors that John Koskinen has put together in development for the Federal Government. We are working with NATO, our allies, and the coalition partners. We must make sure we can respond to any threat on January 1, 2000.

Next chart. Enterprise-wide testing is critical. Testing individual systems is simply not enough to meet our goal of operational capability. We must ensure there is no window of vulnerability in U.S. defense on January 1, 2000. We must be prepared in advance to be able to deploy or respond on January 1. End-to-end testing in exercises will demonstrate our functional and real-world capability.

The Joint Staff and the CINCs are planning operational assessments to start this year and run through 1999. The services and agencies are planning end-to-end testing both in laboratories and on the ground. We are looking at stand-down periods to test functional capabilities, such as our pay and allowance systems.

Next chart. Contingency plans are a critical piece of our comprehensive Y2K strategy. DOD has about 2,800 mission-critical systems for which contingency plans are essential. Even compliant systems will run into unknown problems caused by internal or external nasty surprises, such as data contamination. So we are requiring all mission-critical systems to have backup operational contingency plans.

Next chart. Mr. Chairman, we are working on four major additional initiatives designed to accelerate our Y2K efforts. These will facilitate both the DOD Y2K efforts and our interaction with other Federal agencies.

First, we will convene a high-risk management board to review mission capability, assess risks, and shift resources from those key systems that are behind schedule. This will be in addition to our interface working groups that we already have. This will be composed of top CEO, CIO, and CFO leaders. This will start in late June.

Second, we will implement test and emergency response augmentation teams to support enterprise-wide testing, to provide a war-room capability, and provide for emergencies.

Third, we will institute a moratorium on modifying existing systems until they are implemented as Y2K compliant.

And, fourth, we will require contingency plans of all mission-critical systems and test the contingency plans.

Finally, to do this we must have the flexibility to internally reprogram the resources necessary to meet the Y2K time lines. I would ask the subcommittee to work with us to ensure that DOD has the flexibility we need to manage Y2K within the Department of Defense.

Thank you, Mr. Chairman, for the opportunity to appear before this committee today. I do share your concern and commitment to solving the problem. We all need to work together as this is a concern with global, national, and social implications. Thank you, sir.

Mr. HORN. We thank you. That is a very helpful statement.

[The prepared statement of Mr. Curtis follows:]

Good morning Mr. Chairman, I welcome your invitation to participate in this panel on the status of the Year 2000 (Y2K) problem. You and the entire Committee should be commended for your foresight in recognizing the significance of this global problem. I thank you all for helping to educate the public and focus the attention of the government leaders on the Y2K problem. I share your commitment and look forward to working closely with you, your committee, and the Congress as we grapple with this threat to our national and economic security.

DOD MISSION

Our job is clear in the Department of Defense -- to ensure our national security before, on, and after the Year 2000. Today we are here to report where we are, where we need to be, and what we are doing to get there.

THE YEAR 2000 PROBLEM IN DOD

Mr. Chairman, DoD needs to do a much better job in preparing for the Year 2000. We are making progress, but the leadership -- civilian and military -- fighting forces and support personnel -- cannot and will not be satisfied until we are confident that we can protect and defend our nation on January 1, 2000, and beyond.

In March of this year, the DoD Chief Information Officer assigned to me the responsibility as Special Assistant for Y2K Oversight and charged me to accelerate the Department's efforts in preparing for the Year 2000 rollover in our computer systems.

I am an engineer and a manager, and I understand the technical aspects of the Year 2000 problem and what it means to work on large, complex, interconnected information systems and manage a large scale endeavor.

I am a retired Army officer with combat experience. I understand profoundly what is at stake for our men and women who are charged with preserving our freedom. In my first action as Special Assistant, I reviewed your scoring of the Department's progress, the GAO reports, Office of Management and Budget Quarterly reports, DoD Inspector General reports, and the Defense Science Board recommendations. We fundamentally agree with the findings of these reports and studies.

The Department of Defense is fortunate to have the benefit of these painstaking studies. Your subcommittee's assessments have shown the critical need for a more comprehensive strategy for getting the mission critical systems in shape. The guidance from OMB has been essential in framing the critical mission and non-critical mission references and providing specific milestones by which to measure progress. All provide rich and meaningful insights into program status -- where we are and where we are not.

We are leveraging this information from these various reports to focus our efforts more precisely and to hone the direction of our program.

Deputy Secretary Hamre stated last week in his testimony to the Senate Armed Services Committee that the Department of Defense is at least four months behind schedule. We agree with the recent OMB evaluation that DoD is in the "Tier One" or red zone. We appreciate your recent upgrade of DoD from an "F" to a "D." I believe that your improved grade is based more on our recent management actions than on our actual results to date. This low score reflects the work that remains to be done in DoD.

When I was asked to assume oversight for DoD's Year 2000 efforts, the Department was lagging far behind where we needed to be, and the DoD Chief Information Officer recognized the need for change. The senior leadership of the Department has accepted the findings of this committee, the GAO, OMB, and the DoDIG. We recognize that the Year 2000 poses a real, mission problem. We have made significant changes at all levels of the Department in response.

We have redirected our efforts by keeping our eyes on our goal. The Department of Defense is focused on ensuring we have on January 1, 2000, a force that is able to execute the National Military Strategy, unaffected by a date-related failure of its computer systems.

As you know, the Year 2000 problem affects four aspects of computer systems: software, hardware, firmware, and embedded chips. The Department of Defense has approximately 25, 000 computer systems. About 2,800 are mission critical (11 percent). These include command and control systems, satellite systems, inventory management systems, transportation management systems, medical systems and equipment, and pay and personnel systems. The Year 2000 problem is an especially challenging for the Department of Defense because we are global, we engage in diverse activities, and we have a mix of new technologies and old legacy systems. However, we can't afford to fail. We must make sure the American people know that they are safe and that our potential adversaries know that that the Year 2000 does not pose a vulnerability that they can exploit. We must be prepared to provide humanitarian assistance where needed, and we must be prepared to respond to any attack that is predicated on the assumption that the Year 2000 presents a target of opportunity.

THE Y2K PROBLEM AS A GLOBAL PROBLEM

Senator Bennett stated recently that the Department of Defense is as interrelated as industry is today. Our suppliers are commercial industry, and our customers are our warfighters and peacekeepers as well as our Allies and Partners with whom we jointly work. The Department of Defense is dependent on its suppliers in commercial industry because DoD is also a just-in-time user of supplies and services, as is most of the world economy. We no longer have stockpiles of inventory in our warehouses and depots as in years past. Our infrastructure is also dependent on commercial industry. DoD operates

many military bases, which are really small cities, where the infrastructure can also be vulnerable to Year 2000 problems. Y2K failures in the commercial power grid and commercial communications could affect our military bases, both in the United States and around the world

DoD's plan is to work across boundaries and borders to surface, address and resolve critical Y2K issues, develop contingency plans, and lead efforts to orchestrate partnerships and alliances where appropriate.

OVERALL DOD STRATEGY

I would like to outline some strategies and actions we have implemented to gain better managerial control of our Year 2000 activities.

Since the beginning of its Year 2000 efforts, DoD has used a management strategy that combines centralized policy and oversight with decentralized execution. We divide our work on each system into five phases -- Awareness, Assessment, Renovation, Validation, and Implementation, which are defined by GAO and OMB in numerous reports. All military departments and defense agencies use these phases to track progress on Y2K compliance. While these phases are useful for determining progress on a system-by-system basis, we have gone beyond seeing the Year 2000 as an information technology problem to being an operations and readiness issue.

Organizing For Results

As this committee pointed out, a traditional organizational structure is not equipped to deal with a problem that cuts across all organizational levels and functions. To make the problem manageable, we have divided the DoD's activities into 20 functional areas. These functional areas slice across all military departments and defense agencies. This functional partitioning allows us to frame the challenge in a meaningful way. Some examples of functional areas are command and control, nuclear capabilities, weapon systems, logistics, finance, personnel and transportation.

DoD Organization

Mr. Chairman, we have set up several organizations to execute our Year 2000 strategy. We believe the Y2K problem warrants the attention and leadership of a CEO, not just a CIO. We have organized Y2K efforts in the DoD to provide the leadership we need. To that end, the Deputy Secretary of Defense chairs the DoD Y2K Steering Committee. This Committee reviews the progress of all DoD Components, serves as a forum for sharing information, surfaces management and resource issues, and identifies opportunities to accelerate progress on the Year 2000 problem. Senior representatives from all major DoD components participate in this forum.

The DoD CIO has overall responsibility for managing DoD's Year 2000 efforts. The Department of Defense Chief Information Officer function is assigned to the Senior Civilian Official of the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence is the DoD CIO. The DoD CIO sets Y2K policy, coordinates the efforts of the Services and Defense Agencies, and monitorsY2K progress on behalf of the Secretary of Defense.

As the DoD CIO's Special Assistant for Year 2000, I lead the DoD Year 2000 Oversight and Contingency Planning Office. Both the GAO report and the recent Defense Science Board Task Force report recommended assignment of a strong central leader. These recommendations were captured in the March 1998 blueprint for restructuring the Office of the ASD (C3I) and accepted by the Secretary of Defense. I was assigned roughly sixty days ago to lead the day-to-day Y2K efforts in DoD. My staff handles all multi-Component Y2K actions, such as developing DoD Y2K policy, management plans, consolidated reporting, interface assessments, contingency planning guidance and oversight, and testing oversight.

Each DoD Component Head is responsible for assuring all software and systems correctly process dates. The Military Departments' and Defense Agencies' Chief Information Officers have the responsibility for monitoring their progress and ensuring their systems are Y2K compliant before January 1, 2000, and for reporting status of their systems to the DoD CIO. Overall tracking is done through the new Y2K central database.

We have the commitment of all the CINC's in addressing the Year 2000 issue as an operations and readiness issue rather than as a computer problem. This awareness permeates the Department, throughout all commands and all mission areas.

DOD'S ENTERPRISE LEVEL STRATEGY

The DoD leadership has endorsed a broad attack on the Year 2000 problem. This attack is organized around three principal vectors:

- Report and Evaluation
- Programmatic Oversight and Coordination
- Test and Contingency Planning

REPORT AND EVALUATION VECTOR

DoD's strategy relies upon all DoD Components to provide accurate information on Y2K progress and lessons learned. DoD has established a Y2K central database on DoD's most important systems to expedite Y2K reporting. Each Component also has a Y2K database to provide detailed information on Y2K progress. The goal of this database structure is to meet the needs of DoD's senior leadership, OMB and Congress in managing Year 2000 efforts and ascertaining the impact on DoD's mission capabilities.

We began populating the Y2K database on June 1, 1998. The database is, as yet, incomplete on all specifics on all systems. We are working with the DoD Components to complete the database and to make sure the data is reported accurately. For instance, information in the database on projected completion of Year 2000 milestones should reflect the actual anticipated dates rather than the target dates. We need full and open reporting from our program managers so that DoD can make plans according to actual capabilities.

We are also creating the ability to access Year 2000 data with a new powerful analytical ability which will assist DoD in forecasting Year 2000 shortfalls and ensuring timely resolution of Year 2000 issues. The new ability will also help DoD in:

-- Streamlining the reporting process
-- Allowing quicker answers, and
-- Querying for more meaningful aggregations of information.

DoD is making the DoD Year 2000 data available to the GAO, OMB, DoDIG, and other Federal assessment and evaluation bodies. This will reduce time lags that could hinder their work. This should enable DoD to make necessary corrections faster and with a higher degree of precision.

PROGRAMMATIC OVERSIGHT AND COORDINATION VECTOR

Through oversight and coordination, the Department addresses enterprise analysis, identification of opportunities for improvement, lessons learned, candidate metrics and performance measures, organizational interfaces and resource tracking for Y2K efforts. One of the primary areas of progress in programmatic coordination has been in the acceleration of DoD's interface assessment workshops, so that every functional area will have completed three assessments by September 1998.

We are conducting workshops in each functional area every sixty days. We meet with the functional area leaders, who are responsible for ensuring that interfaced systems will be compliant and compatible. Assessment workshops identify common systems, action plans, and review implementation progress for each functional area. The assessment workshops include representatives of other Federal Agencies, DoD Allies and Partners, GAO, DoDIG and OMB.

Interface with Allies and Partners

DoD has initiated several efforts to coordinate with our Allies and Partners. The President made Y2K an agenda item at the last Group of Eight conference in the United Kingdom. The Secretary of Defense will discuss the Y2K problem at a NATO conference this week. Regional CINCs will sponsor follow-on workshops with Allies and US Security Assistance Officers. DoD seeks to establish ties to Allied defense ministries for critical defense systems, which are jointly operated. While our Allies are aware of the Y2K problem, there is concern that the level of attention is not as great as it

is in the U.S. For example, Europe is more focused on the equally complex and time-sensitive transition to the European monetary system than to the Year 2000 problem.

Verification Efforts

The DoD Inspector General (DoDIG), in conjunction with the audit entities for each of the Military Departments and Defense Agencies, assists in the independent data validation process. These audit efforts are crucial to verification of Y2K actions. The short time frame remaining for Y2K fixes requires further innovation in oversight processes that have already been streamlined by acquisition reform. In addition, the Services' audit agencies are part of DoD's verification process. For example, the Army Audit Agency, working as an internal management consultant for the Army CIO, is performing "Y2K readiness assessments" on critical systems and facilities and is also serving as an independent verifier of Y2K compliance certification documents.

Recent Progress

DoD is placing increased emphasis on Y2K compliance, from the Secretary of Defense to the individual system manager. DoD views Y2K compliance as an operational readiness issue. We have to be and we will be prepared to fight, if necessary, and to provide assistance, wherever called upon. The Department is addressing the findings and recommendations of the various assessments made on its Y2K program by the GAO and the DoDIG.

TEST AND CONTINGENCY PLANNING VECTOR

In FY 1999, DoD's primary focus will be the progress of testing and contingency planning . We will develop schema for Y2K tests, adopt best commercial practices, define testing strategies, and perform continuity planning for our most critical systems and functions. Contingency plans for both mission critical and non-mission critical systems will mature as well. Mission critical systems receive the highest priority in contingency planning.

DoD's contingency planning will come to the fore as the results of testing beyond the system level take place. DoD's operational tempo and complexity of interactions among systems require that testing take place across DoD functions and throughout an entire theater. DoD is establishing plans for including Y2K testing as part of special functional area tests and CINC-led Y2K operational evaluations, commencing as soon as possible and continuing through FY 1999. These should result in contingency planning refinement at departmental, functional, and theater levels.

Testing From Three Perspectives

DoD is using three approaches to test its Year 2000 compliance. Systems-centric testing addresses individual systems. Functional–centric testing assures both Y2K

compliant systems and functional effectiveness by end-to-end testing of DoD functional activities (accounting and finance, etc.). Mission-centric tests assure end-to-end performance of systems and interfaces to maintain the mission effectiveness of U.S. Forces.

System Level Testing

Systems-level testing is conducted by each Service, Agency, and Field Activity, under the oversight of a designated Y2K focal point or program office and is intended to ensure that individual systems are Y2K compliant and can perform as originally designed.

Functional Evaluations

Functional evaluations will be based on strategies and data collection from Interface Assessment Workshops. This includes a combination of interoperability and laboratory testing across Components, Departments, and where feasible, NATO and Allies. The nuclear community is a good example of collaboration to develop an end-to-end evaluation of the Nuclear C4I System of Systems. The process will demonstrate interoperability from sensor to shooter. Virtual and physical test methods will be needed to complete end-to-end testing as dictated by factors such as time, risk, cost, and resource availability. The single string approach facilitates fault isolation while maintaining readiness.

End-To-End Mission Level Evaluations

These will be used to demonstrate DoD's operational readiness in a Y2K scenario. Mission level operational evaluations will augment DoD's Y2K verification and testing efforts and are planned to be carried out in conjunction with Joint and CINC exercises. This testing requires defining specific Y2K objectives that address primary end-to-end operational capabilities, continuity of operations planning and risk areas.

Continuity of Operations

DoD Components are applying extraordinary efforts to meet the technical challenges of Y2K compliance. Despite these efforts, however, we know that all DoD systems will not be Year 2000 compliant by the immovable deadline of January 1, 2000. Some systems whose risks have been mitigated through renovation and testing may fail, and the failure of one system could disrupt many others. Other, lower priority systems will not be ready in time because of the limitations on available human resources to fix legacy software.

There are two areas of risk that must be considered in planning for Year 2000 disruptions:

– Known or suspected sources of disruption, and
– Unanticipated disruptions.

The Department has assessed virtually all of our systems and identified Y2K issues for corrective action. Renovation of systems is in progress, and schedules have been developed for testing each system. Resources are identified and available for accomplishing these actions.

Notwithstanding these efforts, contingency planning is critical to ensure continuity of operations. These plans must address:

-- Failure of the system
-- Disruptions at interfaces
-- Receipt of corrupt data
-- Failure of utilities and infrastructure

Specific workarounds will be addressed, including providing manual processes or non-automated tactics, to supplant systems that do not meet Year 2000 requirements.

The Department's Year 2000 Oversight and Contingency Planning Office is establishing and participating in working groups at all levels to interject Year 2000 threats, such as infrastructure failures, into existing contingency plans. The Department of Defense is expanding contingency plans at three major levels: System, Component, and Department. System level contingency plans are the primary management tools in preparing for unanticipated disruptions. Individual systems could have formal plans, or may rely on operating manuals, procedure guides, or other documents. These documents must address failure of the system. Components plan to test system level contingency plans to be sure they can be executed.

Contingency plans for each DoD Component will include a prioritized list of systems and major actions taken to minimize Y2K disruptions to the core missions of the Component. At the Department level, continuity of operations plans will be reviewed and Y2K scenarios will be incorporated.

DOD'S RECENT INNOVATIONS

We are instituting a High Risk Systems Board to meet with the CEO, CIO, and CFO responsible for each system in Y2K jeopardy. The board will review their progress every month and prioritize our efforts.

We are developing plans to field an independent enterprise-wide evaluation force of 250 individuals to support and independently validate the compliance of our most important systems, especially in functional testing, in mission testing and for emergency responses.

We are developing a proposal to place a moratorium on modifications to existing systems that are not Y2K compliant.

We will develop contingency plans for every mission critical system, and we will include testing of contingency plans in our validation process.

COMMITTEE REQUEST

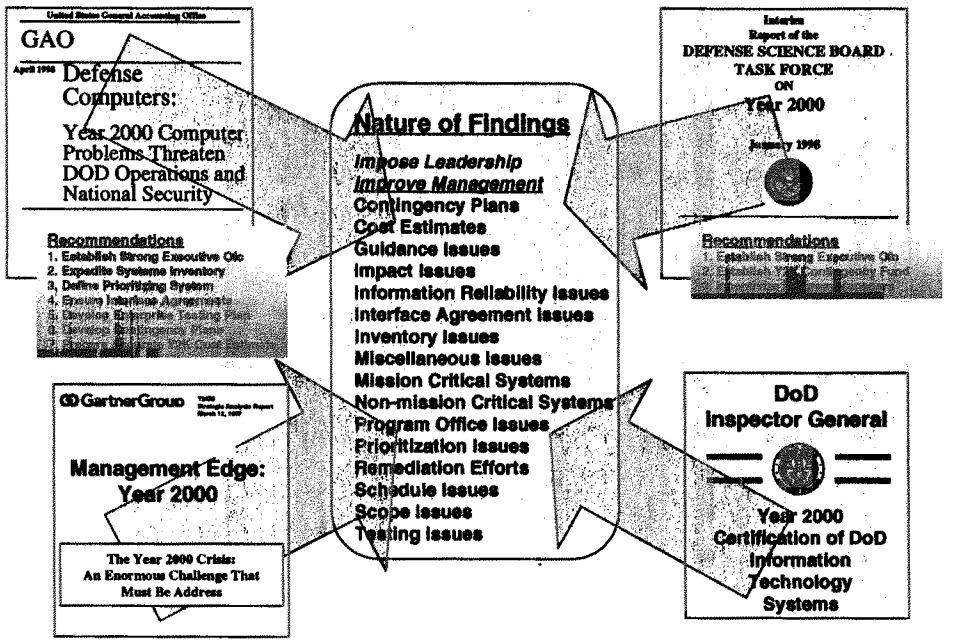
Mr. Chairman, your letter of invitation to today's hearing asked me what you could do to remove impediments to our efforts. There are two areas where this subcommittee and the Congress could assist us.

We ask that you resist helping us by legislating more reporting requirements or by legislating particular approaches to solving the Year 2000 problem. While well-meaning, such actions add administrative burdens that take resources away from fixing the problem or could even cause serious distortions in our contingency planning. For example, there are some legacy systems we should enhance to hedge against the potential failure of other systems that may fail. We are streamlining our reporting and data collection and will share our status data with you. We have also invited the GAO and OMB to attend all of our DoD interface assessment workshops and all meetings of the Year 2000 Steering Committee.

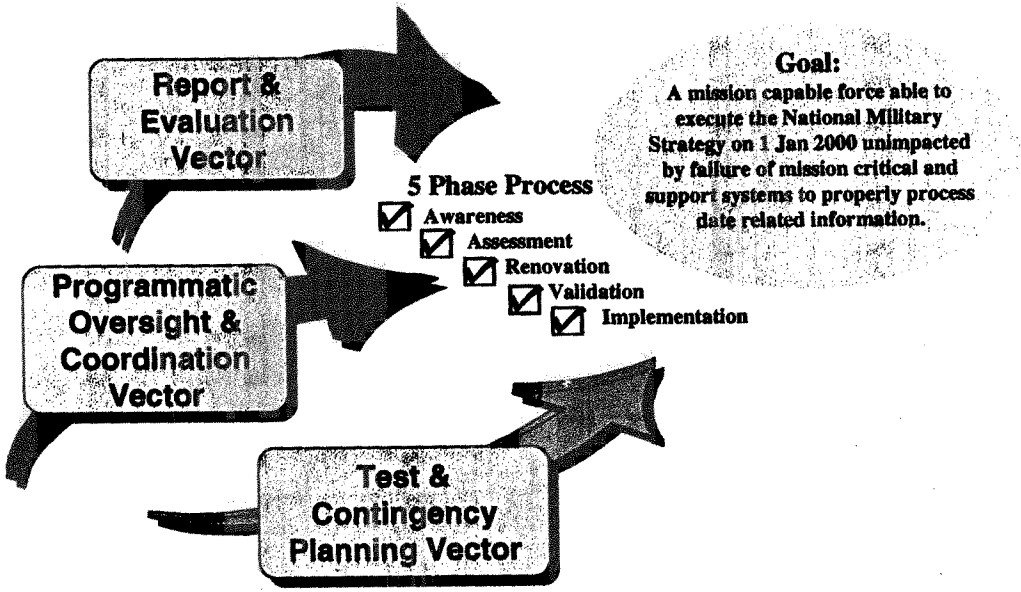
More importantly, we need flexibility in applying resources to this problem. DoD's senior leadership needs to be given the maximum flexibility and minimum red tape to assign resources -- be it money, people, or materiel -- to make sure that January 1, 2000, comes and goes without any degradation in DoD's mission capabilities.

Thank you again, Mr. Chairman, for your support in our efforts to meet the Year 2000 challenge.

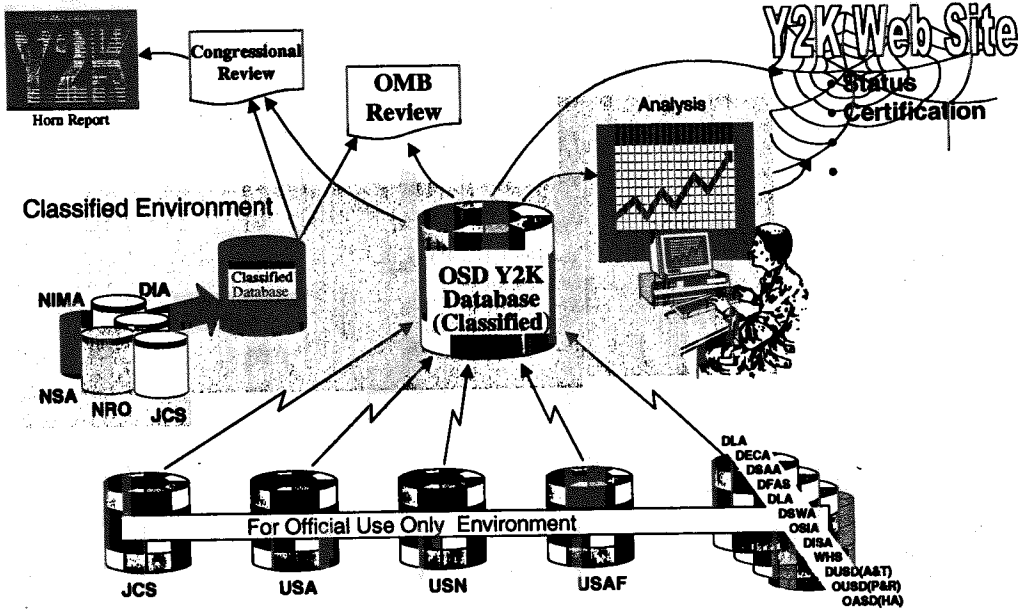
Ascertaining Y2K Reality



Strategic Thrusts



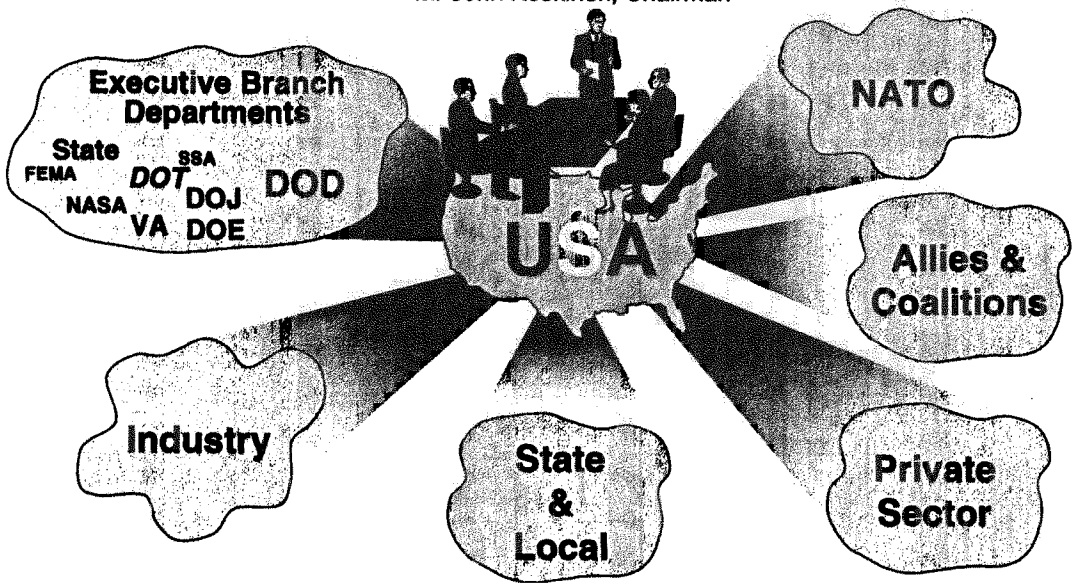
Concept for Y2K Reporting System



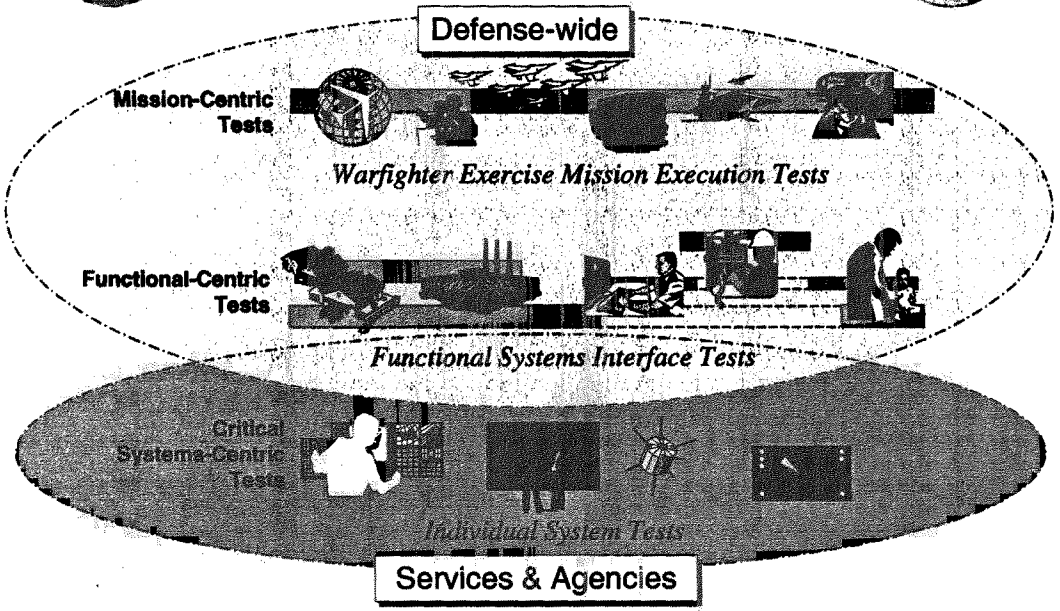
Cross-Organizational Interaction

The President's Year 2000 Conversion Council

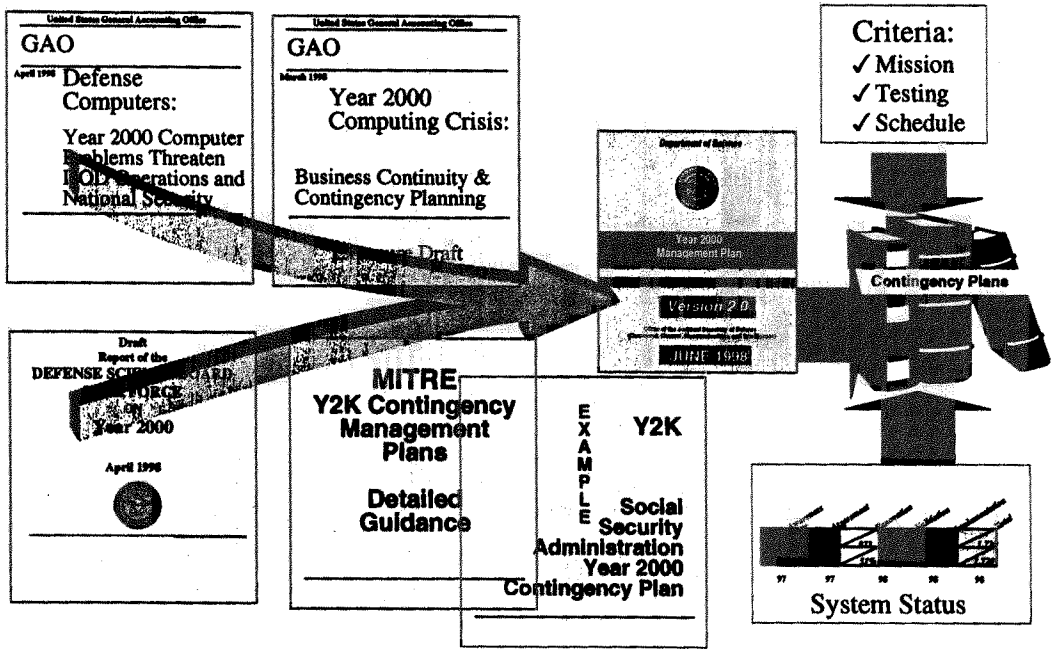
Mr John Koskinen, Chairman



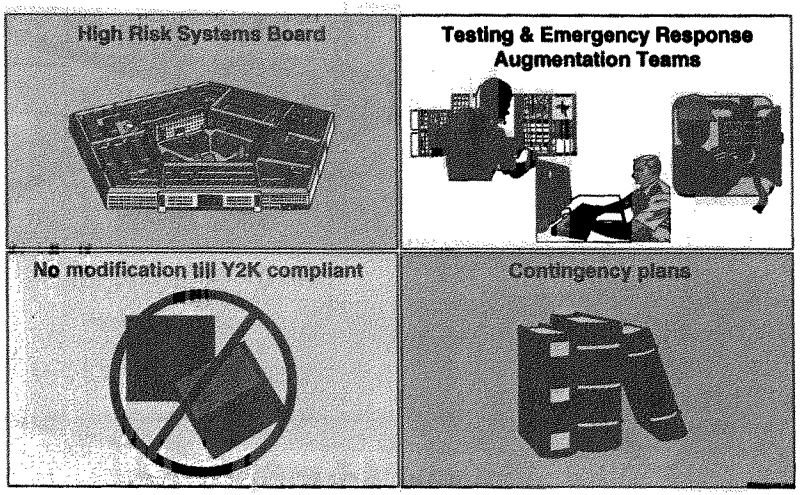
Enterprise Testing: Three Levels/Domain Focus



Contingency Plans



DoD Initiatives



Mr. HORN. Our last witness this morning is Mr. Howard Lewis, Jr., the acting Chief Information Officer of the Department of Energy. Thank you for coming.

STATEMENT OF HOWARD LEWIS, JR., ACTING CHIEF INFORMATION OFFICER, DEPARTMENT OF ENERGY

Mr. LEWIS. Chairman Horn, I appreciate the opportunity to appear before you today to provide a brief status of the Department's progress on year 2000 efforts. The Department is on track toward successful completion of all its year 2000 activities by March 1999, with the exception of six systems which will be completed no later than October 1999.

The year 2000 problem has a high priority within the Department, and it is being managed at the highest levels of the Department. The Deputy Secretary has the year 2000 challenge as a standing agenda item at the Executive Committee for Information Management, composed of senior Department managers; and the Secretary has discussed this at his staff meetings.

Additionally, each Assistant Secretary has assigned a senior manager to participate on the DOE Y2K Steering Committee chaired by the CIO. Importantly, results of an accelerated progress plan submitted by the Deputy Secretary to OMB in January of this year are becoming more visible.

The Department has a net total of 19 systems whose renovation phase has been completed ahead of schedule and a net total of six systems where the validation phase is also completed ahead of schedule. This demonstrates our plan is working.

Computer systems at the Department of Energy are a highly diverse and distributed resource, supporting the Department's four major strategic missions. Computer system activities take place where work is accomplished at departmental and contractor sites around the country and are not centrally managed. Such an environment requires a year 2000 approach that acknowledges the diversity of work throughout the agency. The Department's year 2000 team consists of over 100 individuals coordinating activities at over 50 sites across the country.

The current cost estimate for accomplishing year 2000 activities is $226 million. The Department will be using existing funds and is currently requesting no additional year 2000 funding.

The Department is using an implementation schedule that reflects concurrent efforts that are ongoing in various program offices and sites across the country. Departmental project management is accomplished by setting overall project milestones and monitoring information reported about each of the identified mission-critical systems requiring correction. Therefore, an evaluation of the Departmental progress using a straight-line approach does not accurately reflect the magnitude of Y2K activities that are taking place, nor does it appropriately measure the information technology systems that are managed, developed, and maintained in support of departmental missions.

Evaluate our progress against our schedule and grade us against established departmental milestones. Keep reporting requirements to a minimum, so we can concentrate our efforts on fixing these

problems. Each time we are asked to provide information on Y2K status we take away from the important task at hand.

We have 411 mission-critical systems. Of those, 40 percent are already compliant, 30 percent are being repaired, and 30 percent are being replaced. We are reporting monthly on the status of data exchanges, and currently over 50 percent are already compliant.

Y2K contingency plans are only required for systems that will miss a Departmental milestone, either for validation and/or implementation. Currently, only 6 of the Department's 411 mission-critical systems are scheduled to miss the March 1999 implementation milestone. However, the Department has required the development of contingency plans, continuity of operation plans, or business plans, if you will, since 1987, when it issued a directive to implement the requirements of the Computer Security Act of 1986 and the subsequent A130, appendix 3, for all unclassified mission-critical systems.

This requirement also applies to our contractors and continues to be a requirement today. This requirement calls for annual testing as a regular compliance review item when evaluating our sites and can be tailored and implemented in the case of year 2000 failure. We are requiring the development of Y2K specific plans for the six systems that will not meet the March 1999 deadline.

We continue to be on track for implementation of our repaired systems. We have systems that have completed the renovation and validation phases ahead of schedule. This should translate into accelerated implementations in the future.

I am confident that the efforts we are taking to repair, replace, and retire mission-critical computer systems will prepare the Department for the century date change. I am convinced that the Department of Energy is in much better shape than we have been given credit for.

Thank you, and I will be happy to answer any questions which you may have.

Mr. HORN. Well, thank you very much. We appreciate what you are doing there.

[The prepared statement of Mr. Lewis follows:]

STATEMENT OF
HOWARD E. LEWIS, JR., ACTING CHIEF INFORMATION OFFICER
U.S. DEPARTMENT OF ENERGY

YEAR 2000 COMPLIANCE

BEFORE THE
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY
COMMITTEE ON GOVERNMENT REFORM AND OVERSIGHT
U.S. HOUSE OF REPRESENTATIVES
JUNE 10, 1998

INTRODUCTION

Good morning. I am Howard Lewis, Acting Chief Information Officer (CIO) for the U.S. Department of Energy. I appreciate the opportunity to provide a description of the Year 2000 activities at the Department of Energy, and I thank you for your efforts to focus attention on a matter which urgently needs to be addressed. I am here today to assure you that the Department of Energy is addressing Year 2000 compliance and we are making every effort to ensure a successful transition to the Year 2000. The Department has established a baseline schedule for becoming Year 2000 compliant and is on schedule.

BACKGROUND

Computer systems at the Department of Energy are a highly diverse and distributed resource. Computer system activities take place where the work is accomplished at Governmental and contractor sites around the country. Our computer systems span a full range of application types:

from standard payroll, financial processing, manufacturing process control, high energy physics and weapons modeling, to basic tracking systems (correspondence tracking through nuclear incident tracking). This environment required a Year 2000 plan that distributes the work throughout the agency since computer activity is not controlled by a central site. While some compliance efforts have been ongoing throughout the Department of Energy community for some time, those efforts began to be coordinated and reported through the CIO's Year 2000 Project Office in April 1996. The Department's Chief Information Officer provides project oversight, coordination, and facilitation of ongoing efforts at solving Year 2000 issues in these diverse areas. The Department has required written certification to the CIO from each Program Secretarial Officer of progress towards Year 2000 compliance. A Departmental Year 2000 Project Management Plan was developed and includes formal reporting and tracking of progress toward implementation, including semimonthly reports to the Deputy Secretary.

APPROACH

The Department is focusing its efforts to correct the problem with its mission critical systems. The project team developed guidance on the definition of mission critical based on Title 36 of the Code of Federal Regulations, Chapter XII, Part 1236, MANAGEMENT OF VITAL RECORDS, and Office of Management and Budget Circular A-130, Management of Federal Information Resources. Besides these regulatory conditions, the following, simpler guidance was provided:

Any system should be considered mission critical if that system's failure comes to the attention of the Secretary or Departmental senior programmatic official because a mission of the Department is not being accomplished.

A Departmentwide team, led by the Chief Information Officer, has been organized with responsibility for ensuring that all mission critical systems successfully transition to the Year 2000. The Year 2000 Project Team is composed of information technology representatives (federal and contractors) from all parts of the Department. These representatives are responsible for directing and coordinating with the appropriate program office (funding organization) the development of comprehensive Year 2000 compliance plans. The appropriate program office must ensure that plans are developed and implemented. The process places accountability for Year 2000 compliancy directly on the program offices of the at-risk systems.

Departmental project management is accomplished by setting overall project milestones and by monitoring information reported about each mission critical system. Individual system status information is captured through an Internet-accessible Year 2000 Mission-Essential Status System. This information is used for tracking each system's progress as it achieves Year 2000 compliance and highlighting any area of concern requiring management's attention. Additionally, the status system is used for the semimonthly reports to the Deputy Secretary of Energy and providing information requested from the Department on its progress.

STATUS

Progress

DOE has identified 411 mission critical systems. Of these, 161 (approximately 40 percent) of the systems are already compliant or will be retired, 119 (approximately 30 percent) are being repaired to achieve compliance, and 131 (approximately 30 percent) are being replaced. Although the Department's schedule does not meet the straight-line projection adopted by the Office of Management and Budget (OMB), results of the Department's Accelerated Progress Plan submitted to OMB in January are positive. As of the May report to OMB, the Department has a net total of 19 systems where the renovation phase has been completed ahead of the baseline schedule. Also, there are a net total of six systems where the validation phase has been completed ahead of the baseline. This should translate into accelerated implementations in the future. The Department is eight systems ahead of its projected schedule for implementation of mission critical systems.

The Department has identified six mission critical systems that currently will not meet the March 1999 implementation milestone. Of these six systems, one is at Sandia National Laboratories and is a procurement/financial system which is being replaced by a commercial-off-the-shelf year2000-compliant product. Because it is a financial system, the plan calls for it to be implemented to coincide with the beginning of the fiscal year. The remaining five mission critical systems are at the Savannah River site. These systems are self-contained and interconnected and if any of these systems were to fail the worst that would happen is that a specific mission being performed at the site would stop. There would be no health, safety, or environmental impact at the site or to the

public if one or all of these systems were to fail because of a year 2000 problem. Westinghouse Savannah River Company recently had completed a second disinterested third-party assessment of the Year2000 plans for those five systems. The Department's Office of Environmental Management is currently reviewing results of those assessments.

Compliance Review Team

The CIO has developed a site compliance review process, and the Department's Inspector General is providing assistance with these reviews. The compliance review process: (1) ensures that Departmental policies and procedures related to Year 2000 compliance are being followed and (2) establishes a process for certifying the Year 2000 compliant implementation of each mission critical system. The reviews started in January 1998 and will be conducted at over 20 sites by September 1998. Additionally, sites are reporting that they are conducting their own self-assessment audits. As of May 29, 1998, five reviews covering eight Departmental sites have been completed or are ongoing.

Non-Mission Critical Activities

Team members have been notified that non-mission critical activities involving such things as non-mission critical systems, building systems (fire alarms, security systems, etc.), telecommunications (phones, LANs, routers, switches, etc.), biomedical equipment, and laboratory equipment are the responsibility of the owner and will be addressed at the local level by the March 31, 1999, milestone. The Chief Information Officer's Year 2000 compliance review teams have received presentations and high-level site plans documenting activities from sites reviewed and showing

that the sites are addressing Year 2000 implementation of non-mission critical systems. For the August 1998 OMB report, the Department will provide statistics on site progress on non-mission critical activities. Available information will include assessment status, implementation status, planned and actual implementation dates, and major areas of concern for each non-mission-critical activity.

Data Exchanges

The Department has a minimal number of data exchanges with state governments and all but one of these are compliant. Information on foreign exchanges was provided to the Department of State as requested. Of a total of 743 external exchanges to the Department, which includes federal, state, local and international organizations, 55 percent are compliant, and 58 percent of our internal exchanges between mission critical systems are already compliant. Activities related to all data exchanges are scheduled to be completed by March 1999.

Contingency Plans

The Department decided that contingency plans would be required only for those mission critical systems that miss or are scheduled to miss the Departmental milestones for either validation or implementation. This decision was made so that more resources would be spent on correcting these systems rather than spending a great deal of time developing contingency plans for systems that do not require them. However, contingency plans have been developed in many cases for mission critical systems in the Department's inventory. Contingency plans for systems that will miss or are scheduled to miss Departmental milestones are due to the CIO one month after a

system misses either milestone thus allowing time for implementation before the Year 2000. Contingency plans for six systems that are scheduled to miss the implementation milestone will be completed by December 1998. The creation of a business continuity plan for the Department has not been undertaken since established operating procedures already exist to maintain basic operations.

Cost

The current estimated cost to resolve Departmental Year 2000 problems is $226.2 million.

RECOMMENDATIONS

The Department's schedule does not meet the straight-line projection adopted by the Office of Management and Budget (OMB) for those mission critical systems being repaired and as a result appears as though the Department is behind schedule in meeting year 2000 compliance. The Department currently has 40 percent of all of its mission critical systems year 2000 compliant. If measured against the Department's Year 2000 Plan and corresponding schedules, DOE is making progress. Additionally, the Department is providing timely responses to information requests from the public, state and local governments, other federal agencies, and Congress. This demonstrates that the Department is prepared for dealing with century date change issues and that efforts are being made to successfully transition to the Year 2000.

We appreciate the need for the oversight, audit, and management responsibilities of Congress, the General Accounting Office, and the Office of Management and Budget (OMB), but our resources are continuously stretched responding to inquiries while still meeting critical implementation deadlines.

CONCLUSION

This concludes the description of the Department of Energy's Year 2000 activities. You have our firm assurance that we are addressing Year 2000 compliance and that every effort is being made to successfully transition to the Year 2000.

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

Howard E. Lewis, Jr.
Acting Chief Information Officer
U. S. Department of Energy

Howard E. Lewis, Jr., is a member of the Federal Chief Information Officer Council, the CIO Council Executive Board, and Co-Chair of their Capital Planning and Investment Committee. He is the Department of Energy representative to the Interagency Management Council.

Previously, he held the position of Director of Systems Engineering at DOE and had responsibility for managing the activities involving information architecture, technology assessment, and solutions engineering services.

He has held similar senior management positions at the Department of Energy, the Energy Research and Development Administration, the Atomic Energy Commission, and the U.S. Air Force. He has over 25 years of experience in the information resources management business and has worked in all facets of the computer and telecommunications fields. He received his B.S. in Mathematics from Mount Saint Mary's College.

Mr. HORN. Let me start on some of the questions now, first, I would like a response from all of the agencies. It was mentioned that reprogramming of DOD funds is the way you are going to solve the problem, Mr. Curtis; and we have agreed with that, with the Director of the Budget, Dr. Raines. I have not discussed it with the new director.

And in Energy, Mr. Lewis, you are telling us DOE will use existing funds.

Mr. LEWIS. Operating and maintenance funds, yes, sir.

Mr. HORN. What I need to know from the other agencies is do you have any problem with the reprogramming or have you sufficient authority in your annual budget to reprogram money in this area, should you need it?

Mr. Smith.

Mr. SMITH. We do have authority to do that, of course, with congressional approval. We are asking for, compared to my colleagues, what is a modest amount of money for the year 2000 in fiscal year 1999, but our initial request was for $4 million in 1999. We are now asking for a total of $12 million.

A large percentage of that will go to the validation and the end-to-end testing, and some of it will go to the outreach. Because we feel strongly that the biggest issue for us next year is really going to be the quality of the year 2000 compliance in the schools and colleges across the country.

Mr. HORN. How about HHS, Mr. Callahan, in terms of reprogramming authority? Do you need any more from the appropriations committees or the authorization committees?

Mr. CALLAHAN. No, we have the traditional reprogramming authority you referred to. We also have the 1 percent transfer authority that is given to us in our appropriations, and we have used that this year, and it is conceivable we would use that again next year at an early stage.

Mr. HORN. Let us start now with Mr. Willemssen on a number of things. In regard to the chart related to your testimony, tracking the compliance over time, have you done projections into the future based on this rate of progress? And, if so, what would they be?

Mr. WILLEMSSEN. We have not done a full projection, but what analysis we have done is we have tried to focus the analysis on what would need to take place in order to hit the March 1999 target. And in order to hit that, the rate of progress would need to be quadrupled from what it currently is. Again, this is one of the factors behind the pessimism we have, in terms of getting done in time.

Mr. HORN. So it is roughly three-quarters from now.

You mentioned several areas where Congress lacks sufficient information on the agencies in the year 2000 progress. Do you agree that the information Congress needs is the same as the information required by any manager trying to track progress within the agency?

Mr. WILLEMSSEN. In terms of the level of detail, I am not necessarily convinced that the Congress would need the same level of detail that an agency manager would need. I think what the departments and agencies need to look at, though, is the frequency with which they are reporting this.

And I think there was a comment made by one of the individuals who testified about the burden of reporting. I have to respectfully disagree with that. For any program that is being well managed, managers should already have those reports in summary form, in detailed form, so they understand what is going on. Additional requests for reports should be something along the lines of pulling it off the shelf or pulling it off your PC. There should not be a lot of work to putting reports together for those programs that are well managed.

Mr. HORN. Well, that is what I want to do, is just go down with the existing four agencies. You have defined the mission-critical systems; we have not. You are the ones that know whether they are mission critical; we really do not. That is why we depend on you.

Now what is the time period that you are getting weekly reports from the people that have to do the revisions, the revamping, whatever you want to call it? Mr. Callahan, do you get a weekly report?

Mr. CALLAHAN. It is twofold, Chairman Horn. I get a monthly report that is compiled from all the agencies. Actually, the agency CIOs, in many cases, get weekly reports.

Mr. HORN. In other words, in HHS—I realize it is big and the Pentagon is going to shrink compared to the HHS, I guess, although we might turn that around the other way—but you are saying you get a monthly report?

Mr. CALLAHAN. Right.

Mr. HORN. But who gets the weekly report?

Mr. CALLAHAN. The agency chief information officers. For example, in HCFA, the Chief Information Officer for HCFA is Mr. Gary Christoff, who comes to us from the Los Alamos National Laboratory. He is directly responsible for directing all their Y2K efforts. He receives a weekly report on the status of both their internal and their external systems.

Mr. HORN. Well, as we are getting down to the wire, I guess I do not understand. As a former executive, I would have wanted that weekly. Why are you not getting it weekly, to keep up with the work?

Mr. CALLAHAN. As I indicated in my statement earlier, Chairman Horn—and I appreciate your comments there—but I think at the departmental level what our job is—and I illustrated six areas that we were having our attention focused toward. One is to get them the funding. We move very quickly, because, in addition to being Chief Information Officer, I am also the Assistant Secretary for Management and Budget, to get HCFA the additional money for their external contractors.

Personnel authority. We were the first ones to work with OPM to get them the personnel authority to hire additional resources.

So our job, at least at the Department level, in addition to things you are concerned about, is to mobilize money, resources, make sure we are working with them in terms of outreach and contingency. We are not necessarily down there at an operational basis looking over their shoulder on a weekly basis to see that they get their systems done. That is their direct responsibility, and then we work with them on a longer time basis.

Mr. HORN. So you get it only on a monthly basis——

Mr. CALLAHAN. That is correct.

Mr. HORN [continuing]. As to how many critical mission systems have been revamped?

Mr. CALLAHAN. Both mission-critical and non-mission-critical.

Mr. HORN. By that time you have lost a lot of time. Do you ever get the bad news laid on your desk from somebody when they are on a monthly report and you say, how do we ever catch up? What is the matter? Do you need more resources? Do I need to devote more people from the agency over to help you to catch up?

Mr. CALLAHAN. Certainly in cases where the agencies' Chief Information Officers feel that they need direct help from the Department, whether it be in funding, personnel, or the other areas that we do mobilize our resources at the Department to give them that information and that support directly. We feel that that is an appropriate role.

Mr. HORN. Well, you are playing one role. Of course, I think it is completely wrong for an agency to have the assistant secretary for management, administration, by whatever name, to also be the Chief Information Officer. This is what I saw in Budget, when the head of OIRA is also running the year 2000 problem. They already have an 18-hour day. Why give them another 18-hour day, since there are not that many hours in a day? Seems to me a Chief Information Officer should be doing a lot of that.

That is what bothered me when I saw it at Treasury 3 years ago, which was a disaster area, and I might add, they should have had a full-time Chief Information Officer. But I take it you do not agree with that, or the Secretary does not agree with it or something?

Mr. CALLAHAN. I think the issue here, Chairman Horn, as you have correctly suggested, is that we have to meet our milestones. The proof is in the pudding. We, right now, as you know, are at approximately, in the reclassification of our systems, about 34 percent compliant. We have already added another 10 or 15 systems. We are now up to 38 percent compliant.

You can be assured that from the Secretary, the Deputy Secretary, myself, and all the individual Chief Information Officers that are the front-line soldiers on the year 2000 effort in their agencies, that we will give you our full and complete attention. I cannot do much more than that, sir.

Mr. HORN. Well, I noted in passing, you just repeated it, that you were 44 percent compliant; and now you have worked and cleaned up some more systems and you are 38 percent compliant. Does that tell me something?

Mr. CALLAHAN. Chairman Horn, we went back and, as is indicated in our formal testimony, we looked at all our systems again in terms of mission criticality, whether that is business continuity, whether that is payment concerns, et cetera, and made a renewed determination of what was mission critical. In fact, as a result of that, our "compliance level" dropped.

If we had used our old system, our compliance levels would have been higher. So, in essence, we did not—to be perfectly frank, we did not try to game the system. We tried to look very closely at mission-critical systems. That review was done. On the new basis, our progress in the last several weeks has also improved. We have

added additional mission-critical compliant systems, and we will continue to do that throughout.

Mr. HORN. Mr. Smith, do you get a weekly report as to what is happening or do you get a monthly report?

Mr. SMITH. I get a weekly report, Mr. Chairman.

Mr. HORN. Weekly report.

Mr. Curtis.

Mr. CURTIS. Mr. Chairman, could I have my slide on the data base?

Sir, as you know, the GAO did not like what we were doing on the reporting. We redesigned our whole reporting capability. As this slide will show, what we are doing is building a real-time capability, which we have approximately 4,000 records in already. Each one of the services and agencies down at the bottom have their own Y2K only reporting data base.

In the Department of Defense we were trying to do a number of things in terms of modernization and everything else. That became too complex, too hard to do, and got in the way of Y2K. So now we have a total system as depicted on that chart. That data is real-time delivered to a more summary activity at the top. That is loaded out on our secret network for all of our CINCs, so they can see real time what is going on with each system.

The Secretary, Dr. Hamre, has directed that he will get monthly reports. We have these reports coming in so that, as we work the 20 assessment workshops, at every workshop we can get the data that is right there today. We will also be doing that for our senior level.

I think we are trying to get prepared, obviously, to deal with a faster and faster cycle that we are going to absolutely need as we get down to the wire. We are going to need to know how we are doing. We have also put in dates for forecasting the movement of every system through every phase. Not only do we want to know what historically was reported, we want to know what the program managers are saying when they are going to move that data, to what phase, and if they are not making that, we can start making the decisions to cut those systems off, move money, or work a contingency plan.

Mr. HORN. OK. So am I correct if I said the Department of Defense at your level, and perhaps any senior level, you could know right now, today, as for a particular critical-mission systems, how far along they are in conversion?

Mr. CURTIS. Yes, sir.

Mr. HORN. Is that correct?

Mr. CURTIS. Yes, sir.

Mr. HORN. This assumes the people, the contractor, the team, the center, whatever you are going to call it, updates every day?

Mr. CURTIS. Sir, what we are doing in terms of the updates when something changes on the system at the program management level. Of course, we have the 2,800 mission critical, plus we also have some that are called mission essential that are in our data base, another 2,000 to 4,000. We are working to get that cleaned up. We expect the program managers to change that data on that record when the status changes. So when the status changes, that is available.

Mr. HORN. If you are moving from one half percent complete to 1 percent complete, what kind of instructions do they have as to when you change the little guidepost in the computer program?

Mr. CURTIS. We are looking for when they move through a phase. That's when a specific program moves from one phase to the next phase.

Mr. HORN. Give me an example. Take one critical-mission system and tell me what is phase one and what is the second one they would update on.

Mr. CURTIS. We are using the same 5-phase system. So we have 789 systems right now in renovation. So if one moves out of renovation until validation, the record would be updated.

Mr. HORN. Just on that point, what would be the typical time elapsed between stage one to stage two in an attempt to update and convert a particular mission critical system? Are we talking about a week, 2 weeks, a quarter, or two quarters when you move to validation and so forth?

Mr. CURTIS. Sir, I think that depends on each one of the systems.

Mr. HORN. But an eyeball.

Mr. CURTIS. I don't have an answer to the question.

Mr. HORN. We have a vote on the floor, but let me finish this question.

Mr. Lewis, what is your process here? Is it a weekly report, a monthly report, what?

Mr. LEWIS. Chairman Horn, I have access to our database and can get that information daily. I am informed by my Y2K project manager of what the status is on a biweekly basis. When we go to the Deputy Secretary with that same information, I have access on a daily basis for status.

What I have done with that biweekly information, besides making it available to the Deputy Secretary, is I meet with the Assistant Secretaries. That $226 million that we are taking out of operating and maintenance, that comes out of the program Assistant Secretaries' budgets. I meet with those people, identify which systems are behind the schedules, and work with them on getting their systems to the point of being back on schedule.

Mr. HORN. Well, that is very helpful.

I would just say as we get closer and closer to the time where we have to have not just testing but real, operational testing in a real-world environment, not simply a laboratory—we have seen FAA go back to the drawing boards when they thought they had it cleaned up with the radar situation, which is a paramount—so I would think you would all want to, since the Secretaries of your respective departments are holding you responsible to get the job done. If I were the Secretary, I would want to know, "hey, folks, are we on the right track?" One Secretary I know does ask every week what is going on in his particular agency.

Let me ask this question, before I leave to recess and vote. My understanding of the DOD is that it has improved the honesty of its compliance percentages, is what I am told; but I will further indicate that the Department of Defense's inspector general just released a report that was rather critical of compliance honesty. What is the relationship there? Have you had a chance to look at

that before? I haven't seen it, but I thought I would ask the question, as long as I have you here.

Mr. CURTIS. Yes, Mr. Chairman. We have looked at that IG report. It is very recent. We do concur with their findings.

Part of what we were looking at when I came on board was to try to make sure that people were not reporting the OMB or DOD target dates. What we wanted was the real—when are you going to pass this, that borderline; and we also wanted people to have the freedom to move systems back into awareness assessment or renovation if they found they really weren't up to a validation or implementation area.

I think if we are really going to manage this problem, we have got to have the most accurate data. We need to know when the systems really work, and we can't be shooting the messenger. You know, some of that was going on, and we tried to take that out of the process.

We have accelerated our workshops, so I am running about three a week these days. And in those workshops, we are trying to get really where we are. And sometimes the people don't know where they are, or they think they are in one place or another. We have to get them to the right place so we can make the tough decisions on which systems are going to make it and which aren't.

Mr. HORN. We have another expert in our midst here, Jack Brock, the Director of Government-wide and Defense Information Issues for the General Accounting Office. Do you have a view on this recent report of the inspector general at DOD?

Mr. BROCK. Yes, Mr. Chairman. That is a recent report. We were very concerned in a report we had done earlier that DOD was not getting accurate information and, as a result, it would be hindered in making decisions. And that was not only true at the OSD level, but also true in the service levels. The IG pulled a sample of systems that were reported as being compliant in November, in the November report; and for roughly 75 percent of those systems, they could find no documentation that they had been certified as compliant, even though they had been reported as compliant. Of course, this increases the risk that some of these systems that had been reported as compliant would, in fact, not work properly at the millennium change.

Mr. HORN. Well, I thought we were past the days of the Vietnamese body counts, but it sounds like we had a few over there, at least in the computer area. As I said, I haven't read that report yet, but I will look at it.

Let me suggest, ladies and gentlemen, we take a recess for lunch, because we have lots of questions afterwards. And may I suggest that we reassemble here at roughly 1:05 because, by the time I get to the floor, people will hold me up there; and there is no use keeping you waiting. You might as well do it for the useful purpose of eating lunch and storing up your energy.

We are in recess.

[Whereupon, at 12:10 p.m., the subcommittee recessed, to reconvene at 1:05 p.m., the same day.]

Mr. HORN. The subcommittee will reconvene for its afternoon session.

Where we left off this morning, we were on reprogramming and did you have sufficient authority; and the answer seemed to be yes. So we don't have to worry about that one.

Then the question is, how do you assure that what is reported to you is accurate?

Now, Mr. Willemssen, you mentioned Canada has had national year 2000 priorities for over a year now. Is Canada also reallocating resources from agency to agency based on those priorities? And, if so, how does the system work?

Mr. WILLEMSSEN. Mr. Chairman, we haven't, at this point, done a detailed review of Canada. We have had some discussions with their program director and the CIO. They went to a priority-setting process because of their concern several months ago that they were not going to get all of their systems deemed mission critical done in time. So it wasn't to say to each of their agencies, we don't want you to do this, but our top priority is going to be focused on these 44 functions. I don't have the data at hand at this point as to what kind of reallocations have occurred to date.

Mr. HORN. Let's file it for the record, and we will insert it without objection in the record at this point.

[The information referred to follows:]

Question: GAO mentioned that Canada has had national Year 2000 priorities for over a year now. Is Canada also reallocating resources for agency to agency based on those priorities? And, if so, how does the system work?

GAO Response: According to Canada's Year 2000 program director, Canada has not begun to divert resources to its highest priority functions. The program director stated that, at this time, Canada does not believe that such diversions will be necessary. However, he added that Canada is prepared to divert resources if needed.

Mr. HORN. In your April recommendation to the President's Council on the Year 2000 Conversion, apparently some of your ideas weren't accepted. I count seven in your testimony, of which only three were accepted: and priority setting was not accepted; end-to-end testing was not accepted; central reporting issues were not accepted; contingency planning was accepted; independent verification was accepted; work force issues were accepted, and the Nation's year 2000 status in priority setting was not accepted. Is that an accurate statement?

Mr. WILLEMSSEN. I would say, generally speaking, with one exception on the reporting issue, I would consider that more mixed.

Among our recommendations was to get reports from additional key organizations; and OMB did implement that recommendation and has asked, as you know, for reports from 41 additional organizations. So I would not say that was totally not accepted.

Mr. HORN. OK. We have heard a lot about the five working groups that have been organized by the Assistant to the President on this matter, and that has been established for Federal agencies to reach out to the rest of the American economy through them—that makes a lot of sense—in terms of regulatory—the so-called quasi-legislative, quasi-administrative, quasi-judicial regulatory groups. And do we know from GAO's standpoint anything about how those regulatory agencies are doing in relation to their client in population?

Mr. WILLEMSSEN. Point one is we would agree with the establishment of those groups. It looks to us like they are focusing on the

right topics, such as telecommunications, energy, and work force. So I, one, think the establishment of the groups is a good step.

Two, we recognize that they have just recently started and had initial discussions. And I think it is an appropriate time to begin asking the questions beyond just talking on the issues, what kind of data is being exchanged regarding these key economic sectors, and when are we going to get past the talking and discussion phase and really get down to where we stand on these key sectors, from a risk perspective and understanding, what we have to do to minimize that risk.

Mr. HORN. I have talked to a number of consultants; and, as you know, consultants become experts rather rapidly in this particular area because it is so different from what they have generally dealt with. What I am being told is that more information should exist for the private sector corporations than is available. That is partly because the lawyers of the general counsels in the private corporations don't want them to share that information because they are fearful of increasing their liability, since we know there are a lot of hungry people in the tort bar that are moving from tobacco into the year 2000 area.

What insight do you have here in terms of a degree to which the clientele, in this case, American corporations, fear dealing with Securities and Exchange or FCC and those regulatory bodies, where they are fearful about saying where they are now, that that will be used against them in a court case?

Mr. WILLEMSSEN. If I can preface my remarks by acknowledging that I clearly am not an attorney but just giving a layperson's view on this, clearly, there are a number of issues that have been raised about the legal liability situation as it pertains to year 2000. In fact, there are a number of conferences that are held over and over again just on Y2K liability, so this is a very hot topic, one that is attracting quite a bit of attention.

It just would appear to a layperson that if a company has a product that ends up being Y2K defective, from a due diligence perspective it would seem that they would probably want to err on the side of informing their customers in advance, as opposed to not sharing that information. And what we see is several major computer companies starting to move in that direction and sharing information on the compliance status of their products.

Again, from a layperson's standpoint, not a legal perspective, that makes sense to me, so that you know up front what this company is telling you about the compliance status, rather than holding that information. Then if indeed the product is found defective, it would seem that the risk may be greater in the case where information was not shared.

Mr. HORN. Mr. Brock, do you want to add anything to any of this?

Mr. BROCK. I think that is a real issue.

I would like to add something to Mr. Willemssen's remarks earlier. One of the private sectors, where a great deal more information is known, is in the banking industry, in the financial institutions, where the regulators have, for some time, in the safety and soundness examinations, been doing more detailed assessments of individual institutions. And I think, as a result of those examina-

tions, the banking industry is generally believed to be ahead of the other industries in where they are, in large part, I think, because of the active role the Federal Government has played in providing some oversight and direction.

Mr. HORN. Well, I agree with you, and I certainly do when it comes to the Federal Reserve and what they have done. Do we have any feel for what the Comptroller of the Currency, the FDIC, and several other regulatory bodies that have a sort of foot in the door in terms of what goes on at the State level, do we know anything about what they are doing?

Mr. BROCK. Yes. All of the regulatory bodies use a common examination guide that was developed among them all. So they share an assessment guide. They have all gone through fairly rigorous training.

The primary concern we have had, when we have done individual reviews of each of the regulators, is they started too late. They are just like everyone else. They started too late; and, as a result, some of the guidance that went to the financial institutions, particularly the smaller ones, was getting to them later in the cycle than what we would like to have seen.

But there is now, unlike other sectors, a great deal of information that is now being made available about individual institutions. You generally don't have that kind of information about other individual business entities within the U.S. economy.

Mr. HORN. Well, I thank you for those comments. I think they are very helpful; and, I must say, they are reassuring. You are telling me these four or five agencies are sort of marching to the same tune in terms of the guidebook and the further use of human resources, which all of them collectively can make quite a contribution, one of them individually might not.

Mr. Callahan, I haven't forgotten you as Chief Information Officer of Health and Human Services. You expect to receive a complete set of contingency plans by June 15 from your operating divisions. Are these sort of real-business-type continuity plans or are they simple system plans? In other words, do they cutoff beyond the system as to how you might solve the problem, should it just go blank?

Mr. CALLAHAN. It is my understanding that they will be business contingency plans, and we will look at those very carefully. We will, obviously, work with the subcommittee in terms of analyzing these plans as well.

Mr. HORN. Are they connected with every mission critical system or just several of the mission critical systems that might be the most critical?

Mr. CALLAHAN. It is my understanding it is every mission-critical system, sir.

Mr. HORN. Now, you mentioned the situation at the Health Care Financing Administration and that there are 900 million payments annually. That is over 17 million per week. Does that mean if the year 2000 causes even a 3-week processing delay—and, of course, they aren't processing the checks; the Financial Management Service of the Department of the Treasury is doing the benefit checks? Are they also doing the actual reimbursement checks?

Mr. CALLAHAN. To the providers?

Mr. HORN. To the providers, yes.

Mr. CALLAHAN. It is my understanding—and I talked with the people at HCFA this morning, in this regard—is that, actually, each one of the contractors, our principal contractors, will draw money from the Treasury and then they will make—through an affiliated bank that is connected with each contractor—the provider payments to the medical providers.

So, clearly, one of the things that you mentioned, in terms of making sure that there are not cash-flow problems or what have you, one of the contingency plans that may well be brought forth is if we cannot assure you that an individual contractor system will be year 2000 compliant, whether in calendar year 1999 or the first quarter of fiscal year 2000, whether we would put into place some prospective payment system to provide the medical providers with cash for the first part of the calendar year 2000. Then we would, in essence, have to come back behind that and make sure we did the appropriate audits, which we would do. So it would be a novel way of doing business, in addition to also the other standard thing of going back to manual processing and paper claims.

Mr. HORN. Has the Health Care Financing Administration and the Department looked at the relationship of the contractors or intermediaries between HCFA and the hospitals and different types of health care facilities and doctors and so forth? Have they looked at that relationship, which exists, I guess, from the 1965 law, and to what degree do they feel that should be changed?

Mr. CALLAHAN. I am not sure I get the last part of your question, Chairman Horn. They are looking—they are in the process, in terms of outreach, of working with their providers, whether that is the hospitals, the doctors, et cetera, to alert them of the need to have year 2000 compliant systems.

However, we anticipate that we would be able to receive data from those providers through electronic bridging systems, somewhat similar to what we are doing in CDC, so we would be able to take in the information, presuming the contractor systems are compliant.

The problem may then rest with individual medical service providers—doctors, home health agencies or whatever—if their systems go down. So we are trying to alert them to get their systems compliant; but, in any case, we are prepared to take their data and make it 2000 compliant within our own system.

Mr. HORN. I am really thinking of the intermediaries between the hospitals and the doctors that file their expense bills and are as you say, drawing from the trust fund to make those payments, if they are in accord with law. And I guess my curiosity is, since those are not governmental intermediaries, can the government require them to become 2000 compliant?

Mr. CALLAHAN. Well, that is a point that we raised in the legislation that we sent up to the Congress on May 18th. We put in an additional provision in our contract reform legislation to enable the Secretary to require the contractors, in this case, the intermediaries, to be year 2000 compliant, so that the Secretary could have that authority in terms of working with them. That legislation is pending before the Congress.

Mr. HORN. It is pending before, I assume, the Ways and Means Committee on our side and Senate Finance on the other side?

Mr. CALLAHAN. That is correct, sir.

Mr. HORN. And that has the full support of the Secretary, I take it?

Mr. CALLAHAN. The Secretary, the President, and the administration.

Mr. HORN. Does it look like it is going anywhere?

Mr. CALLAHAN. We certainly hope so.

Mr. HORN. I agree with you.

Mr. CALLAHAN. We will make the push for it. I know it is a crowded legislative schedule. But, clearly, hopefully, your efforts and others and your colleague on the other side, Senator Bennett, will help us push this legislation. I know Senator Thompson in a hearing that he held was receptive to this as well.

Mr. HORN. Yes, I think you have a real point there. Let's see if we can't get something out of the respective finance committees.

Now, when I asked the General Accounting Office about Mr. Koskinen and sector outreach groups in general, could you please describe the two for which HHS has the lead role? I hear it is the health care center and the human services sector. How are we organized to get some accomplishments out of that?

Mr. CALLAHAN. First, on the Year 2000 Conversion Council, our Deputy Secretary, Mr. Kevin Thurm, sits on this council. We have been providing Mr. Koskinen and the Conversion Council information from our side about the types of outreach that we would make to all of our partners in both of those areas. But as the General Accounting Office has mentioned, these efforts will be combined with other agencies as well. There is a meeting tomorrow of the Year 2000 Conversion Council at which this matter will be discussed, and I presume that the time lines will be set forth, and specific policies for outreach will be set forth, and we will report back to the subcommittee in those efforts.

Mr. HORN. Well, I thank you. That is really all the questions I have right now. We might have a dialog on some general ones, but let me turn to Mr. Smith, the Acting Deputy Secretary in Education.

As I understand your paper and what we know about Education, there are 14 mission-critical systems and 25 mission-important systems. I am not quite clear of the difference between mission critical and mission important. Give me an example, if you could, in each category, so I understand this.

Mr. SMITH. The examples in the first category are largely drawn from student financial aid and the delivery of student financial aid to 10 million students around the country, about $45 billion worth.

Another mission-critical system is our finance system, which provides resources, connections to States, colleges, and so on across the country.

A mission-important system would be a system that operated within one of our principal operating components that might, from the perspective of that particular component, carry out a very important function, but not a function that is critical to the overall functioning of the agency. So that it is really a matter of scope. I mean, you make a decision and you draw a line. But our line is

pretty bright because the systems, the 14 systems that we have, are qualitatively very different from the systems we have as mission-important systems.

Mr. HORN. Well, are we putting all of our resources now in education in the 14 mission-critical ones or are we sort of also doing the 14 mission-critical ones and the 25 mission-important ones?

Mr. SMITH. And the third category of systems, too. We are putting our efforts into all three. And, in some ways, these efforts get divided up among different groups of people, in the same way that in HHS there are different groups of people working in HCFA than working in NIH, presumably. So we are able to—I am able to concentrate largely on mission-critical systems.

But, I have in the last week, just gone over in detail and looked at the time lines for each of the other systems and then said, "I think they are too long," and we are pushing them back. A lot are simple replacements of software, and we should be able to do that very, very quickly and just wipe them off the books.

Mr. HORN. Now, I note—and I will quote you on this—failure of any of our mission-important systems could cause mid- to long-term failure of Department business functions, unquote. Now, if their failure causes failure of business functions, doesn't that make them mission critical?

Mr. SMITH. Perhaps that is an exaggeration in the language, Mr. Chairman. If on January 1 of the year 2000 one of those systems failed, it would not create any major problems for any of our customers. If by June we hadn't corrected it, and since we are going to have contingency plans for the mission-important systems, if we hadn't been able to put those plans into place we might have a problem of delivering grants, let's say, that particular year. But, from my perspective, that is a relatively unlikely problem.

Mr. HORN. Do you have a figure on the percent of, say, the 25 mission-important systems, how far along are they as a group in terms of becoming compliant?

Mr. SMITH. Hang on, let me just check on that.

Mr. HORN. You don't have to give an exact percent.

Mr. SMITH. About 45 percent of the mission-important systems are compliant.

Mr. HORN. Now, the other 55 percent are in various stages, I take it?

Mr. SMITH. I am actively trying to get rid of a lot of them, actually, and that is difficult sometimes.

Mr. HORN. This is a great excuse to clean house, get it down to one system or something.

Mr. SMITH. That is exactly right. But it is not always easy. You have to have a hearing, in effect, about it and have the discussion and so on before you actually do it.

Mr. HORN. You can say Congress and your conscience made you do it, right? We are good people to beat up with the bureaucracy. The wise administrator uses us for that purpose.

Now, you mentioned, in several letters, large volumes of 15,000 school districts, is it, nationwide?

Mr. SMITH. It is. Right.

Mr. HORN. Do you know how these schools are doing and do you get reports from colleges? How are we doing in that area?

Mr. SMITH. Well, we are now clearing some surveys through Congress for the colleges and universities.

Mr. HORN. Through the Congress or through the OMB?

Mr. SMITH. Through the OMB. One hurdle or another, they all get mixed up together. Yes, we are clearing the survey through. We have our nine responses from our preliminary survey, which is what we are entitled to do under the law.

If you look at those—and just from anecdotal work, because we have people out working with direct lending schools, for example, on a daily basis, there is a great mixture out there, as I am sure you know. You have been talking with people, and it ranges from institutions that did exactly what the Social Security Service did—and they started a long time ago, and they are up to date—to places that haven't heard of it, God knows why. But it just has not entered into their consciousness. They don't have a plan. They don't have an idea about what they need to do. Largely, those are in schools and universities that don't have the resources to do very much, and that is a real difficulty. So we are trying to get a real handle on that and a set of strategies for working with it.

Mr. HORN. In terms of updating their systems, are the big-city urban schools——

Mr. SMITH. I was actually just talking about the colleges and universities at that point.

To move over to the school systems, we have gotten some information about large school systems, a sample of about 25. We just looked at it yesterday, and it is very distressing. Everybody says they are going to make it, but the dates are lined up in such a way that you—and we have it against their systems—their accounting system, their tracking student system, their payment and so on, a whole variety of systems. And they put down the dates these systems are going to be compliant, and for a number of them, every date is exactly the same, February 1999. In others, it is exactly the same, and it is October 1999, which begins to get a little worrisome.

But just the notion they haven't differentiated among the systems, which means they either haven't paid attention to answering a survey, which is possible, or they haven't paid attention to the problem in the depth we would like to see it paid attention to.

The survey itself, of course, can generate some interest. It says, gosh, they are interested in what we are doing. But I think there is a very significant problem out there.

Let me give you another anecdote. Let's say this is a hypothetical district, actually. Two years ago, the district discovered there was a year 2000 problem; and the CIO and the district put together a plan which said, for $8 million, we can fix it. For $10 million, we can put in this wonderful new system where the bells and whistles will work wonders for us and bring us into the 21st century. And the CIO recommended the $10 million system, and the school board sat on the decision for a year and a half. And they are just now waking up to the fact that now it is not only going to cost $8 million, it is going to cost far more than $8 million. And they are also waking up to the fact they are probably not going to make it. I wouldn't be surprised if that were the case in a number of different places.

Mr. HORN. You mentioned, in the Department of Education, one of your solutions is—and I imagine it is with the personal computers—to just turn in the old models, which might be several generations behind, and get the new model. What are you going to do to make sure they are 2000 compliant? Are you going to test them? Is GSA going to test them?

I have been through this with the Agency for International Development way back in 1996 when they said, you don't have to worry about us; we are getting all new computing. They didn't test for it, and the result is they bought a screwy system that didn't work, and they are still in the F stage. Whereas they were getting A's just for saying we are going to replace it.

Mr. SMITH. It is a very good question. We are buying systems that others have tested, so we are buying basically models that have gone through tests and are deemed compliant by the industry, and we are also going to test them ourselves.

Mr. HORN. Well, I thank you for that; and it looks like you are keeping on top of it.

Let me move to Mr. Curtis, who is the new Department of Defense czar for 2000 conversion. Tell me, what is your reporting relationship in the Department of Defense? To whom do you report?

Mr. CURTIS. Right now, I am a special assistant to Mr. Money, who is the senior civilian official for command, control, communications and intelligence.

Mr. HORN. Have they filled General Paige's job? He was the Assistant Secretary in that area.

Mr. CURTIS. Mr. Money is acting in that capacity. He has not been confirmed yet.

Mr. HORN. I see. Because what bothered me is I remember, when General Paige retired, I thought the Deputy Assistant Secretary also had retired and two Directors over there also had retired. Roughly three levels of management disappeared into early retirement. Did they just know that there was a problem here, and there was no use wrecking the rest of my life or what? And how did they get you to cheerfully take over?

Mr. CURTIS. I am not so sure how they all left. I actually worked for Secretary Paige way back when we were both in the military wearing a uniform. I don't know if I should say this, but I volunteered for this job, Mr. Chairman. I think, in my career, every time no one else wanted the job, you know, I took it.

Mr. HORN. You are a wise man. Challenges?

Mr. CURTIS. I love challenges, sir, and I do feel that those of us working this can make a difference. That is why I am here.

Mr. HORN. Well, I will tell you, one thing we have been fascinated by—obviously, you have hundreds of thousands of embedded chips—somebody told me a few months ago, you were going to try to decentralize all of this operation down to the base. I don't know if you meant commands by that. You weren't around when this happened. I am just curious, when you relate to these commands and they, in turn, relate to the facilities, be it a ship or a fort or contracting or whatever it is, what are we doing? Because that is going to take extensive training.

I mean, if I was the colonel in charge of a base and I get a letter from the Secretary signed by one Bill Curtis, I would say, where

do I start hunting to find one of those imbedded chips now? And if I find one, what do I do about it?

How are we handling that? It seems to me like a massive problem.

Mr. CURTIS. Mr. Chairman, I think you are absolutely right. And the Department of Defense has probably everything the rest of the Federal Government has. We feed people. We have towns. We have things that are afloat. That is why we are on 18 of the 32 sectors.

What we tried to do is organize the infrastructure as one of the 20 functional areas. If I step back for a minute, if you look at the 20 sectors, functional areas like procurement, nuclear, command and control, weapon systems facilities. Then, we look at some defense agencies. We see different ones at each assessment workshop. So we have a huge matrix you are trying to work with. You would like to get everybody in the room at one time, if possible, at the Department of Defense level. You want to cut across a functional area all at once so that the lessons learned in one area can be passed down the other. So we have gone through our facilities assessment workshop, No. 1. No. 2 is coming up in July. So, at the top level, we are looking at that.

Now what we tried to do with getting down to all of the base—post, camps, and stations and bases—and tried to make sure that the commander, the base commander in that place, understood that he or she was responsible for the Y2K problem. We have tried to move this from a CIO to a CEO issue. Don't pass it off to your computer guys like Curtis. Get on with it—you must make that base work. All of our bases today are power projection platforms for anything that we need to do, so they need to work.

That has helped. That has got that kind of focus. In July, I will be able to give you a better indication of where I think we are with that.

We also are working our embedded chip issue in two areas. In the weapons systems, the embedded chips are part of the system review. So if you own the Tomahawk, you own the embedded chip problem or the software problem. But if you are on a post camp and station, and the infrastructure chips include all of our PC computers, LANs, our routers, and all of that kind of stuff, plus the lights on your base. In our infrastructure review, we found one of the biggest problems was the security mechanisms. For many of those devices, we don't know how they are really going to operate. Are they going to allow people to open up buildings or not? So we are looking at that. That seems to be one of the key areas.

They also found out that the Corps of Engineer dams need to be checked, because all of the devices that monitor our dams all over this country are also full of those chips. So, as we work all the different areas and we try to pass along the information. Obviously, we have web sites and things like that to do this. Fundamentally, we try to bring this back up to the CEO leadership in each area.

Mr. HORN. I thought I could make it through and not have to keep you gentlemen here, but we are going to have to recess. We have two votes on the floor, so we are going to be in recess, essentially, until 2 o'clock. So I am sorry to hold you here like that, but I have a couple key questions for the last two gentlemen and maybe some for all of you, so we are in recess until 2 o'clock.

[Recess.]

Mr. HORN. I understand you have some time constraints?

Mr. SMITH. I have a meeting over at the State Department. Secretary Riley is leaving for Portugal this afternoon, and we are going to connect by phone at least while he is still in the country.

Mr. HORN. We are going to go about 20 more minutes.

Mr. SMITH. That is great.

Mr. HORN. Sorry about those votes. That is why the taxpayers sent us here, but it does wreck business, doesn't it? But that is our business, so we go.

We will have some questions to followup on this, because we couldn't get to everything. But it has been very helpful to hear your answers, and I appreciate that.

What I wanted to do is get to NATO in terms of the interactions of our computers and their computers How many situations like that do we have besides NATO, where you have got foreign commands that are going outside the American military? Is that a problem, and is NATO working on it? Because I am about to go to a meeting of the Interparliamentary Delegation between the U.S. House and the European Parliament, and we discuss these in use with them also, every 6 months. Of course, NATO is a separate entity in Europe, so we just wonder how they are doing.

Mr. CURTIS. Mr. Chairman, we are concerned about NATO and our allies and the coalitions. We don't sense, necessarily, they have the same thrust as we have in getting this problem done. As you know, they are occupied with getting onto the Eurodollar, but I think there is an awareness there.

The President brought this up at the G–8 meeting recently. And the Secretary of Defense, at the end of this week—I believe that is the correct date—when the Defense Ministers meet, he has put Y2K on the agenda and plans on speaking on that. At the end of the month, my counterpart in the United Kingdom and I will be sitting down and talking about what we are doing there.

Mr. HORN. I might add that the delegation from the House of Lords and Commons has come over here to visit with us. I think they saw Mr. Koskinen and they might have seen others of you. Go ahead.

Mr. CURTIS. So we will be putting increased emphasis on that.

And I know our STRATCOM people are working just this week on this kind of thing, especially with the coalition partners. Secretary Hamre spoke to the Senate about the fact that we are concerned about the fact that everybody can see that no missiles are flying during this timeframe. We don't want any screens to go blank or have any miscalculations, so we are working that. I think you will see a lot more emphasis across that whole arena.

Recently, my counterpart from Australia asked if we could come down and give them an assessment of their Y2K environment. I don't know if we can do all that, but we will certainly work with them.

Mr. HORN. One of the things we have never been clear on and we just haven't asked the question is on the critical mission systems. How many of those are exclusively related to weapons systems, as opposed to command systems of normal defense discourse to the various commands and other sorts of subordinate groups? In

other words, I am not asking do you have it on Cruise missiles or Stingers. What I am asking is; is this a problem and to what degree and at what level are we dealing with it?

Mr. CURTIS. Again, I don't know if I quite understood your question.

Mr. HORN. Are they on the list of your total number of mission-critical systems?

Mr. CURTIS. The weapon systems are all mission-critical systems, every one of them. And I will take that for the record, Mr. Chairman, and get you better data on that, if you don't have it. We are looking at all weapons systems as mission critical. And then you have the command and control and the other systems that are involved.

[The information referred to follows:]

Yes, weapon systems are included in DoD's total list of mission-critical systems.

Mr. HORN. To what extent do they depend on maintenance of particular equipment that you might have? And are those mission-critical systems? When you are looking at maintenance schedules and so forth, those would kick over into the zero zero before most?

Mr. CURTIS. Correct. The first thing with the weapons systems is to make sure they will work. You also have test equipment, maintenance equipment, support equipment, around them. I am not prepared to tell you how we are looking at that between mission- and non-mission critical. But we definitely have all of these issues about the weapon systems. For instance, the chips, the software, the hardware, the whole thing belongs to a program manager to get that entire system across the line.

Mr. HORN. Are we planning any war games where the year 2000 problems come into effect and the systems just break down on the field? What are they going to do about it and is there a contingency plan and so forth?

Mr. CURTIS. Mr. Chairman, absolutely.

One of the things, when I came on board, we were doing system-level testing, listening to industry. Secretary Hamre has a large number of industries that came to him and explained to him the problem if you don't do real, open, end-to-end testing.

I sat with the Director of the Joint Staff the other day; and we are going to do exercises, operation capability exercises, where you take the CINC exercises and you change all the computers they are working on, everything they are working on, and make them run that across the date line. The vice chairman is putting out a message to the CINCs to get a set of exercises in by the 30th of June where we can start doing this.

I have indicated a realistic number of exercises. We do about 270 joint exercises a year. Potentially about 10 percent or around 25 of those would be our target, as a minimum, to actually do this. The Director of the Joint Staff would like to get that started, even this year, and then run them all through 1999.

I think that is the only way we are going to be able to demonstrate to the American people, we really can defend this country. I don't believe any amount of rhetoric is going to convince people that we can defend this country. I think we need to demonstrate to our adversaries that we are ready and that there is no oppor-

tunity for them to take advantage of us, either by doing anything with us, with our friends and allies.

Another issue we are very concerned about is the whole cyberspace war, the confusion that would be in place. We have problems. People might think it would be a Y2K problem, may not actually be a Y2K problem, but actually, an attack on our systems.

Mr. HORN. Do the joint chiefs have a unit on this?

Mr. CURTIS. The Joint Chiefs of Staff have a Y2K office. They have done a lot of work to bring the CINC representatives together. A few weeks ago, they identified the top 20 C4&I systems. This is not the weapon systems, but the companion control systems and intelligence systems. They are a big help, and they are going to take the major lead in the operational exercises for the CINCs.

Mr. HORN. Getting to resources and when they are identified and available for accomplishing various critical missions that might be more critical than some other critical missions. To whom do you have to turn in order for the authority on those resources to be moved to solve a defense-wide problem?

Mr. CURTIS. Well, sir, I haven't done that yet in the first 60 days. But in that 60 days, I have briefed the Secretary of Defense three times. I have been with Dr. Hamre on a number of occasions. I see Mr. Money, and we would take recommendations to Dr. Hamre for execution. I think that is pretty high up in the Defense Department. I think we can get it done there.

Mr. HORN. So there is no problem in moving the resources, as long as they are within the regular reprogramming rules?

Mr. CURTIS. Yes, that is true, sir. And what we are looking at, though, is what are the flexibilities? We are concerned as we go down through the year, we are in 1999 and it is an election year, how much reprograming flexibility will we have between the major committees and so forth. So I would like to get back to you on that for the record on what I think might be able to be done.

[The information referred to follows:]

Yes, it is true that DoD has no problem with resource availability for Year 2000 (Y2K) efforts when these requests are within the reprogramming rules that are already in place. The Deputy Secretary of Defense has directed the DoD Components will fund Year Y2K systems remediation efforts to the fullest extent possible within existing total funding. In addition, appropriation for DoD in FY 1999 includes emergency supplemental funding to address Y2K-related requirements. Both of these enable flexibility in funding for Y2K-related requirements.

Mr. HORN. We have been accused of wanting too much paperwork out of the administration. Well, all we want is a couple of simple figures, and I think that is all that Mr. Koskinen would want.

Can we get the clerk to move this chart on my right, over here? Just move it so you can see it. Bring it up so I can see it. Because, apparently, staff has not provided a draft for us. But we have used this chart for 2 weeks. Here we go. I can actually see it from there.

What we are asking for is recommended monthly reporting. You have mission-critical systems, second-tier systems—and we could do a better job at defining that—and contingency plans, telecommunications, embedded systems, external data exchanges.

Now it would simply be, how many have you got? Are they now compliant? What percent has been assessed? What percent is com-

pliant? That is all you need to tell us. We are just getting down to the basics of, have you done it or haven't you?

And then we took an example, and we used DOD as an example because we thought it was a very good example. Even if you are lagging behind on the lagger's panel, but that is OK. That is good experience.

May 15, we have mission-critical systems, 2,803 second-tier systems—10 times that, really—and contingency plans, we don't know yet. I don't know if you have them yet. I mean, do we go back to the cavalry; what do we do when things go kaplunk? I mean, are the services developing the contingency plans or is it your office doing it?

Mr. CURTIS. Mr. Chairman, in all honesty, we have been focused on fixing the systems. Not a great deal has been done on contingency plans. We are looking at the rest of 1998 and 1999 to get those contingency plans done. We have said that anybody that falls behind on a system in any of the dates that are posted, you have to start working on them.

I am very concerned about this. As an automater, people think that another automation contingency plan will do it. It won't. If the system doesn't work one place, it is not going to work in another. So we must get the operators involved with the contingency plans, and they must be able to deal with this without the computers. So that is what we will be focusing on.

In my new staff, I have people who are doing that. I have put contractual work on that. Those will, however, be developed at posts, camps, and stations at program levels. It has got to be a decentralized execution, because we are looking at at least 2,800 of those. We are going to have to deal with a large number of the second-tier systems, which will feed data in.

Mr. HORN. How about the rest of the agencies here? Have you developed any contingency plan? Because there are one or two crucial systems that you just don't seem to be making progress on. Where are we on that? Just to start down the line.

Mr. CALLAHAN. As I indicated to you earlier, Chairman Horn, we will receive all those contingency plans for all our mission-critical systems on June 15th.

Mr. HORN. For all systems, you are asking. Very good.

Mr. CALLAHAN. The mission-critical systems.

Mr. HORN. Education?

Mr. SMITH. We are reviewing plans for all mission-critical systems right now, and we will have contingency plans for some of the key other systems below the mission-critical.

Mr. HORN. And Defense would be all mission-critical or just some?

Mr. CURTIS. All the mission-critical systems.

Mr. HORN. How about Energy?

Mr. LEWIS. As I stated before, we had a requirement there from our Computer Security Act requirement; and a good percentage of ours, I think in the neighborhood of about 45 percent of the mission-critical, are in good shape. We have the requirement or the plans coming in for the six systems that are not going to make the date also.

Mr. HORN. Well, you mentioned in your report to OMB and also to us that new systems will replace 131 current mission-critical systems on time. I guess we wondered about that, because there are few, if any, big, mission-critical systems that are ever installed on time. That has been my experience with computers.

In fact, the other day I happened to be catching some of the C–SPAN coverage of that Center for Strategic International Affairs; and Peter D. Jaeger, a consultant in the field, asked the CEOs in the audience, have you ever received a work product that had to do with information technology on time? If so, please put your hand up. Not one hand went up.

That has certainly been my experience. It's always overpromised. Oh, yes, this wonderful world of technology. It will happen. It doesn't happen, and there are probably some 20 percent that never see the light of day, if you gave them 5 years.

So with that bit of cynicism, I am curious, are you pretty confident on this, on the 131 before March of next year?

Mr. LEWIS. Yes, and may I explain why?

Mr. HORN. Sure.

Mr. LEWIS. The reason I say that is, basically, we recognize that, in the testing and things like that it is not something that you can say that you are going to stay in that category. When you have changes that affect you from the outside and things like that, that could shift and you could have a mission-critical system, as far as you are concerned, that has been compliant. It is exterior effects that you are going to have to go back and respond.

That is where the priority comes, as far as I am concerned. This whole thing is a priority issue, from my standpoint.

I told you the money was coming from the operating and maintenance. We have to be able to get to program people and the people who are responsible for the mission-critical systems, ensuring priority can be given for continuous integration testing, not just end-to-end testing. I don't think end-to-end testing is going to do it. If we don't have continuous integration testing, every time the system is touched, from the time we declare it to be compliant, we could have problems, and that is how we are looking at this.

Mr. HORN. And you are doing it in relation to some of the people you interact with?

Mr. LEWIS. Yes. I have the IG assisting me in this, and I have the Office of Oversight within the Department providing assistance. I also have a compliance team that goes out to the various sites. We have visited five sites so far and hit eight of the installations that we have. And what we are doing is looking and ensuring that the people have documentation.

I will not tell you right now that everything is beautiful from that standpoint, but we are identifying problem areas. We are pointing these out, and we are getting improvements made on the spot and coming back and giving an update on where we stand there.

Mr. HORN. Are you optimistic that the private utilities with which the Department interacts will have this problem under control by the year 2000? Because that is what people are worried about. Members of Congress come up to me every day saying, well, what about our grid system? Well, we have about 10 of them out

there, haven't we, 10 major ones? And what do you see? Are things happening under the direction of these particular either public or private utilities?

Mr. LEWIS. Yes, our Deputy Secretary, who is on Mr. John Koskinen's Year 2000 Conversion Project, has a working group under that conversion group that is looking at how that needs to be addressed. She is going to be reporting to the special Senate committee on Friday. They are addressing this. They are getting the right people involved. They are getting the people that are doing the job right now.

The people who need to be involved in this, Chairman Horn, are the people who are making things work right now. Year 2000 is just one of the contingencies that can happen with the grid. You can just think back a number of years ago about problems that have occurred, and we are responding to those problems, and those people need to be in a position to respond in the year 2000.

Mr. HORN. I well remember the New York situation and the northern California, U.S. situation. If those grids go, you can just count on an increased population 9 months later, apparently, is what I learned from the two experiences.

Now, Savannah River, we understand they are behind. But their systems will be fail safe or OK, is that sort of your conclusion?

Mr. LEWIS. That is our current assessment. I just had a conversation before I came over here this morning with the environmental management senior management here at headquarters. What we did at Savannah River was, we brought in an outside contractor to verify the process, to verify the schedule, and to verify where we are going with that project.

That project is a very integrated project. We are doing contingency planning on that project on a continuous basis, because we have to do it in order to make the operation safe. So now we are looking at what needs to be done in order to accomplish the year 2000 along with the operation and maintenance activities for that particular site. We do not feel that, at this particular time, that there is any problem that is going to be impending with respect to health, safety, or anything outside the site if there would be a failure there.

Mr. HORN. Moving from that, there are more questions we could pursue on the toxic nature and what goes on and so forth, but let me move to some of the Department practices, program level managers handling embedded systems problems. The responsibility for building security systems, for telecommunications, routers, for biomedical equipment rests with the local level managers. Now how would a local program level manager recognize a telecommunications router if he saw it? How would he find the embedded chips and what would we do when he did? I mean, what kind of training is going on in Energy to deal with that kind of thing or are there specialized teams that are looking at each of these?

Mr. LEWIS. Energy is somewhat unique. The majority of the Energy sites are managed by contractors, operating and maintenance contractors, management and incentive contractors.

We happen to be fortunate in most situations. You did not hear me respond negatively to the need for manpower. When we have a site set up, that site is completely covered from an operations and

maintenance standpoint; and we are having those people—and, again, I defend—those are the right people, the people at the site, to be looking at that. They do know what facilities are there. They do know where the information is for finding out about where embedded systems are going to be impacting their operation.

Again, they have to know that in order to make the particular facility operate to support our missions. It is tied in with the mission accomplishment of those particular sites. So we are collecting the information at headquarters, and I feel those are the best people that can respond.

We can respond with special expertise in some areas, but I will give you an example. As we get closer and closer, some of the information that is needed on special embedded chips and things like that are only available at the site. Not that I can't supplement that expertise from outside, but if I don't have the expertise at that site, I am going to be very, very unfortunate from the standpoint of having the time to respond to what needs to be done. So we are using the expertise where it is, and we are fortunate to have that expertise.

Mr. HORN. Well, you raise an interesting question. Obviously, they should be at the site, because that is where things go on, as you suggest.

I guess I would ask this: if part of the site was affected by a terrorist or just an accident, where do we have a duplicate set of plans? Do we have them in the Washington office on all these sites so one could go out and pick up what is left and see what is where, part of it might still be potentially operational? Where do we keep duplicate sets of those plans?

Mr. LEWIS. I would have to research the specifics on that particular question. I would be happy to provide it for the record.

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

[The information referred to follows:]

The Department keeps emergency management plans within the various organizations responsible for actually carrying out the plans. Emergency Management, DOE Order 151.1, Comprehensive Emergency Management System, issued September 25, 1995, describes the Department of Energy (DOE) Emergency Management System (EMS). The Order establishes policy; assigns roles and responsibilities; and provides the framework for the development, coordination, control, and direction of the DOE EMS. The Order establishes requirements for emergency planning, preparedness, response, recovery, and readiness assurance activities. The plan describes the approach for effectively integrating these activities under a comprehensive, all-emergency concept. DOE facilities/sites or activities, Operations/Field Offices, and DOE Headquarters offices are required to develop emergency management programs as elements of an integrated and comprehensive EMS. Together, these elements ensure that the DOE EMS is prepared to respond promptly, efficiently, and effectively to any emergency involving DOE facilities/sites, activities, or operations to protect workers, the public, the environment, and national security. The DOE EMS is a three-tiered organizational approach to forming an integrated Departmental emergency response organization structure. Responsibility begins at the facility or event scene level and rises through the cognizant Operations/Field Office to the Headquarters Emergency Management Team. At each tier, there is a designated organization responsible for responding to and

minimizing or mitigating the effects of Operational Emergencies.

As required by DOE O 151.1, Chapter IV, Section 3.b(8), each facility must have "an alternate location if the primary command center is not available." To function as command centers for emergency response, these alternate locations must have copies of the emergency plan. Furthermore, DOE O 151.1, Chapter XI, Section 6, "Emergency Operating Records Protection Program," requires that "vital records, regardless of media, essential to the continued functioning or reconstitution of an organization during and after an emergency, are available, per 36 CFR 1236." DOE's guidance for implementation of these emergency management requirements, contained in the Emergency Management Guide DOE G 151.1-1, issued September 21, 1997, further elaborates the requirements by recommending that "A formal transmittal, distribution, and filing system should be established to ensure that copies of emergency plans, implementing procedures, agreements, and associated documents are up to date and accessible at locations where they may be needed during an emergency for use by appropriate personnel within DOE, contractor organizations, and Federal, state, tribal, and local governments." Because of the tiered approach to emergency management with the Department, emergency plans are available at multiple locations at and near the site, as well as at the cognizant DOE Operations/Field Office. Copies of emergency plans are also forwarded to the DOE Headquarters Office of Emergency Management, within the Office of Nonproliferation and National Security, and used for reference in the Headquarters Emergency Operations Center during an emergency. Additionally, DOE Headquarters Program Offices typically have copies of emergency plans for sites/facilities under their purview. Emergency plans for DOE facilities are also typically maintained at State and municipal emergency response organizations.

Mr. HORN. I have mentioned the utility grid, and I think we pursued that enough. But let me ask you a few other things. Monthly reporting, as has been suggested by some, is this what you need and could provide to OMB and Congress? Or should, as we get down to the wire, it be less than monthly reporting?

Mr. LEWIS. From my standpoint, I need more than monthly reporting; and I am getting more than monthly reporting. I have an on-line data base that I have daily access to. What I am attempting to do is to provide that information to my program managers, the senior people who have funding responsibilities so programming decisions can be made.

The biggest thing in getting the job accomplished, when I am looking at trying to take it out of operating and maintenance dollars, is to put proper priority on accomplishing the year 2000 challenges we have. So it is a prioritization issue, and I believe I am providing that information to the right people to make those prioritization decisions. It is decentralized in the Department, but we do have funding authority centralized and have the Assistant Secretaries in the program organizations working with me to obtain priority, when priority is needed.

Mr. HORN. Does the Nuclear Regulatory Commission have any role in what the Department of Energy is doing on this? Have they asked any questions about it or have they dealt with, say, the people that are part of the grid? And what role have they, if any, played in this?

Mr. LEWIS. We are coordinating with the Nuclear Regulatory Commission as part of the John Koskinen and Year 2000 Conversion Project.

I am also working with both the Nuclear Regulatory Commission and the Federal Energy Regulatory Commission with respect to interfacing with their CIOs and knowing what needs to be provided from an information and interaction standpoint. We are able to basically interact and provide information, and put the right people in contact with who needs to be informed in addressing problems.

Mr. HORN. Well, let me ask GAO, before we break this up, any questions we should have raised that we didn't?

Mr. WILLEMSSEN. I think you have hit the most appropriate topics.

Among the remaining critical issues are testing, business continuity planning, independent verification, and validation. Those are among the most paramount issues, and I have heard those discussed here today. If we were sitting here 6 months ago, I don't think you would have gotten the same kind of responses from the agency representatives that you did today, so I think we have to acknowledge that there is——

Mr. HORN. Are you going to walk out of this room feeling better or are you saying, "Hey, we are not going to make it?"

Mr. WILLEMSSEN. We stick to what we said up front. What I see is more of an acknowledgment on the part of agencies on the massive magnitude of this challenge and that, as they have gotten into it more, they are beginning to recognize that, and we are at least hearing the right things. But that is why, for example, IV&V are so critical. All of these representatives must know more than ever now that they need some independent organizations to come in and

help them, to check on what is being reported to make sure it's indeed reality.

Mr. HORN. Any questions we should have asked as far as some of you feel we didn't ask, and you think are important questions? Personnel limitations, staff reminds me. A couple of you mentioned it. As I understand it, OPM has been pretty flexible in bringing retirees out of retirement.

Mr. CALLAHAN. I would offer one quick comment on that, Chairman Horn. I think governmentwide, as we approach, as each day passes, it certainly would make good common sense inside the government for there to be some sharing of critical computer personnel. So that as an agency or any part of the government completes their task to their satisfaction of the executive branch and the Congress, we have some ability to move those critical personnel.

Mr. HORN. I think that is an excellent suggestion. A friend of mine who is at the top level of one agency, has noted that he created a center to do a lot of this work; and other departments, States, nonprofits, and corporations are buying off his employees every week. They get them out of retirement, they bring them up to speed, and they are doing good things, and then they are disappearing. I don't know how many of you have had these raiding parties on your staffs. I am curious. Are you losing many people, Mr. Lewis?

Mr. LEWIS. Yes, sir.

Mr. HORN. How many a week to other jobs, before you have done yours?

Mr. LEWIS. I lost my boss to another agency just a month ago. But within our organization, we are basically—in the last 3 years, probably reduced our work force by 33 percent. And many of those people went to industry. Obviously, a number of them retired. But there are critical resources in the government that are very valuable to industry.

Mr. HORN. Well, are these people being hired for the purpose of year 2000 conversion?

Mr. LEWIS. I don't know.

Mr. HORN. You don't know that.

Any feeling, Mr. Curtis, on this? I mentioned the group that disappeared under Assistant Secretary Paige, including Assistant Secretary Paige.

Mr. CURTIS. Yes, sir, and I know a number of them are working in the information business. I don't know if they are working with Y2K. It has been very helpful. They allow us to bring back people. I know the Air Force in their systems center has hired a number of people back. But, of course, we are also faced with the downsizing that is taking place in our military department, especially among our civilians. So we have two things working against each other, but I don't have a strong handle on the numbers of people.

Mr. HORN. Do you have a center, Mr. Smith? Can you tell us how many of yours might be going elsewhere?

Mr. SMITH. We don't have a good sense for that number, but I would throw in another factor. A number of our contractors are losing people. And, again, I don't know the absolute magnitude, but

I do know they come in and they say, well, we are trying to get this thing done, but we have just lost two or three of our key programmers or analysts.

Mr. HORN. Well, Cobol is in again. I thought when I learned that in the 1960's, that would be the last I would see of it, and I am almost right, but I don't have a contingency plan.

Anyway, Jack, do you have anything—Mr. Brock.

Mr. BROCK. Yes, sir. One final thing.

I think today, whether you liked all of the information or were displeased with it, you saw a window that was opened into what the Federal Government is doing; and I think, unfortunately, there is not a similar window that can be opened, for the most part, into the private sector. I think it is very easy to come up with all sorts of scenarios for the health and well-being, safety, financial status, et cetera, of Americans, individuals and businesses, both, they are likely to be affected by this. And, unfortunately, we don't have a very good understanding of what is going on in that arena, and you would have a very difficult time of having a hearing where you were able to come up with the same kind of information you were able to develop today.

Mr. HORN. Well, I thank you. You have all made good suggestions, and I appreciate you coming here. I am sorry for the fact we have had to break up a hearing that I thought I could go from 11 to 1 and would be over, but voting prevented that. So thank you very much for coming.

Let me read the staff list and thank the people that have been involved. Let's see. I am told it's in my book. OK.

We thank, for setting up this hearing, J. Russell George, who is the staff director and chief counsel; Dr. Alloway, to my left, professional staff member, deeply involved with this hearing; Matthew Ebert, the clerk; Mason Alinger, staff assistant; and interns: Betsy Damus, Mark Urciuolo, David Graff.

Then for the minority: Faith Weiss, counsel; Earley Green, staff assistant.

Pam Garland and Katrina Wright, court reporters; and Julie Moses.

OK. With that, this hearing is adjourned. Thank you very much.

[Whereupon, at 2:40 p.m., the subcommittee was adjourned.]